December 19, 2018

The Information Accountability Foundation ("IAF") is a non-profit organization whose charitable purpose is research and education on balanced policies to achieve both innovation and fair processing of data. The IAF respectfully requests the opportunity to testify on accountability at the Federal Trade Commission hearings on privacy on February 12-13. The IAF is also pleased to respond to most of the questions asked in the hearing notice.

IAF's testimony would be based on the its work since 2009 with the Global Accountability Dialogue ("Dialogue"), a project at the Centre for Information Policy Leadership. The Dialogue was a multi-stakeholder endeavor that included Federal Trade Commission staff participation. The Dialogue's objective was to define the accountability principle in the Organization for Economic Cooperation and Development ("OECD") Privacy Framework in a manner in which it could be put into effect by data users and overseen by regulators. The output of the Dialogue shaped global regulatory guidance, and the essential elements of accountability are reflected in the European Union General Data Protection Regulation ("GDPR"). It is also reflected in regulatory guidance and laws in Asia and North and South America.

Over the past five years, the IAF has conducted research in numerous jurisdictions on how fair processing may be achieved when data are used beyond the common understanding of individuals to whom that data pertains. The initial document in that research series is the "Unified Ethical Frame for Big Data Analysis." Follow-up work has been conducted in the United States, Canada, Europe and Asia. IAF's most recent work was commissioned by the Privacy Commissioner for Personal Data in Hong Kong China and focused on ethical data stewardship for the legitimacy of data processing. The Hong Kong work provides guidance to assure advanced data processing activities are ethical and fair to all stakeholders, including individuals and organizations.

In response to the passage of the California Consumer Privacy Act of 2018, the IAF has a developed a set of principles to guide development of new legal frameworks for privacy. In the IAF's view, the United States is in need of an updated privacy framework that maintains the ability for organizations to think and learn from data while also protecting individuals in a highly observational digital ecosystem. These principles are material to the means and strategy the FTC would deploy to protect American consumers.

These comments were prepared by IAF strategists, including Martin Abrams, Stanley Crosley, Peter Cullen, Lynn Goldstein and Barbara Lawler. They do not necessarily reflect the views of the IAF board of trustees or financial supporters.

Data use is necessary for a safe, productive America,but still needs guardrails

Data pertaining to individuals are used to make cars smarter, improve healthcare outcomes, make cyber safer, improve education, create new products, keep us from getting lost, predict new trends, and prevent suicides. The privacy debate in the United States often focuses on advertising, marketing and social network uses. However, as the United States considers new privacy regulations, it is important to factor in how important data have become to our everyday lives. We often take the tangible improvements in our lives from using data for granted and feel spooked by the negative uses. There are few of us that literally want to be lost in an information age because data were over regulated. However, we also do not want to be harmed, shamed, disadvantaged, or made to feel little. This dilemma, and the FTC's role in resolving it, are the challenges for the February hearing.

What do we mean by privacy

Privacy in the United States encompasses both rights and interests related to individual autonomy, seclusion and fair processing. The Fourth Amendment to the United States Constitution expresses societal values related to seclusion and interests in autonomy, as does the U.S. Privacy Act. Fair processing has been defined by sector specific laws, with the Fair Credit Reporting Act being the oldest. This combination of autonomy and fair processing in the same legal regime is not uncommon. One sees it in laws in the United States' closest trading partners, Canada and Mexico. It is also reflected in the FTC general privacy authority emanating from section 5 of the Federal Trade Commission Act of 1914 (the "FTC Act"), which prohibits unfair and deceptive practices. Deception tracks to autonomy through the concept of telling the consumer what one is going to do with data and sticking to those disclosed uses. Unfairness tracks to fair processing. Yet unfairness creates a very stern test that often requires empirical evidence of harm. This proof level makes unfairness a very tough test for regulators when anticipating future negative consequences.

European Union law links autonomy and data protection to different constitutionally recognized rights as enshrined in the Charter of Fundamental Human Rights of the European Union. Privacy tracks to Article 7, Respect for Private and Family Life, and data protection tracks to Article 8, Protection of Personal Data, which requires consent or some other legal basis to process. The GDPR takes a very broad view of Article 8 and interprets it to include the full range of human rights, interests and freedoms. By extension, data protection as interpreted in the GDPR requires organizations to process personal data in a fair fashion, rather than prohibiting unfair practices.

The IAF is not suggesting a shift to a GDPR type approach. The GDPR, as it is being interpreted, creates impediments to thinking and learning with data, which has been the cornerstone of data driven innovation. Thinking with data involves new insights, which go beyond experience and intuition, and come instead from correlations with data sets that are discovered. Learning with data is where these insights are put into effect.

As society has seen a progression in communications and information technologies from mainframe computers through numerous technological and operational developments to the world we live in today, the ability of individuals to understand and grasp the risks and rewards of data being processed and controlling that processing has become more problematic. That progression of technology changes includes:

- relational databases;
- application of statistical analysis against large data sets;
- consumer web browsers;
- open networks;
- common programming modules;
- the cloud;
- big data;
- the Internet of Things;
- and now artificial intelligence and machine learning

The technology progression has made individual control more challenging just as individuals are more compelled to participate in a digital ecosystem to receive the benefits of an information age. Thus, the balance between autonomy and fair processing must naturally shift from individual control to more fair processing by organizations in order to achieve both protection and innovation.

To the IAF, an essential question for the February hearings is how does the United States shift from a regime focused on prohibiting deception and enforcing against unfair practices to one that actively encourages fair practices without sacrificing unexpected innovation that might be hindered by ex-ante oversight? To the IAF, privacy is more and more about achieving accountable fair processing and an evolved set of individual rights.

Responding to specific FTC questions

The FTC notice included 25 specific questions. IAF's response begins with those questions related to legal frameworks and is followed by answers for most of the more general questions. One note, the IAF response discusses individuals, their interests and rights, which is reflective of its work. The FTC authority relates to consumer protection and therefore individuals as consumers. The IAF recognizes the difference in scope. This difference, particularly in responding to the FTC questions, relates to marketplace versus non-marketplace harms.

**Questions About Legal Frameworks**

What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?

> *The IAF has proposed a framework that is based on the work it has conducted in the United States and globally. The regime in the United States has facilitated data driven innovation from credit prescreens to watches that act as health sensors. Organizations are fairly free to observe, think and learn with data without needing to establish a permission for such activities. This ability to freely think and learn with data has generated significant benefits for consumers and competition. This engine for innovation is a benefit that any framework should preserve. However, the potential consequences associated with artificial intelligence and advanced analytics demand a more formal discipline associated with accountability requirements.*
>
> *Globally, regulatory structures have attempted to address this dilemma. For example, the Canadian regime is based on two very strong OECD pillars, consent and accountability. This structure has led Canadian regulators to see consent as a gating mechanism and accountability as the means to achieve fair processing. Canadian regulatory guidance has encouraged*

*comprehensive privacy programs that include privacy assessments. The IAF has conducted research in Canada, funded in part by the Office of the Privacy Commissioner, on assessments based on accountability, to determine whether uses are legitimate and in context. However, the nature of evolving technologies that merge the digital with the physical and biological (also known as the Fourth Industrial Revolution) have placed great stress on consent as an effective gating mechanism in Canada.*

*The GDPR has created flexibility about what might be considered legitimate processing. The GDPR also requires organizations to understand all their own processing as well as the processing of their partners and vendors and to conduct assessments to understand the risks they create for others. But, the GDPR has published guidance on advanced analytics and automated decision making that hampers thinking and learning from data. Almost every other regime achieves transparency through individual rights to see most of the data that organizations have that pertains to them. In the United States, the lack of access as a generalized right has facilitated secret data collection, creation and processing. This secrecy in turn exacerbates the trust deficit that exists in the United States – individuals do not trust organizations to collect and then use the data they have about them in a responsible manner.*

*The IAF framework captures the controls that come from other regimes, evolves them for today's more complex data world, and merges them with the flexibility that has fostered innovation in the United States. The IAF framework contains four individual rights principles and eight accountability principles. The accountability principles create a road map for responsible and answerable processing of data beyond common understanding. They also create a means for thinking and learning with data that facilitates next generation innovation.*

What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?

*Ex ante privacy regulation, that requires behaviors such as fair processing by design, is very useful in encouraging appropriate due diligence before data are used. However, ex ante regulation that requires prior approval to process data is a speed bump that adds minimal value and creates real opportunity costs. Certifications, a form of ex ante co-regulation, fit somewhere in the middle. Ex post enforcement is necessary with or without ex ante processes so that individuals and regulators will trust organizations to use the personal data collected and created by them in a responsible way.*

The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct? Why or why not?

*The Fair Credit Reporting Act, as amended, is arguably a successful privacy law in establishing both a set of consumer rights and organizational obligations while maintaining its effectiveness over time. Other laws, such as the Drivers Privacy Protection Act, have established guideposts around data consumers are required to provide. Laws related to healthcare have been effective*

*in creating guideposts for organizations delivering healthcare but have restricted value added research and thus may have inhibited innovation. However, it is not clear the laws enacted in the United States are fully effective when sensor technology-based applications augment traditional medicine. The lessons from those laws are that where individuals must provide data, and there are established norms around the provision of that data, sector specific laws are very sensible. However, when specific harms have not yet been identified, where business practices are evolving quickly, and when there are emerging individual interests, comprehensive laws are more appropriate. The IAF believes that a comprehensive privacy law is needed in the United States.*

Other than explicit statutory exemptions, are there limitations to the FTC's authority to protect consumers' privacy? If so, should they be removed? Why or why not? Should more limitations be implemented? Why or why not?

*The IAF has defined privacy in fair processing terms. If processing goes beyond an individual's ability to commonly understand how data might be used, then enforcement based on deception is less effective as a policing mechanism. The unfairness test requires the FTC to either enforce after the harm has already occurred or to have a concrete understanding about the nature of the potential risk of harm. Creating empirical evidence of future harms for an application that does not yet exist is a very hard test, especially when one is attempting to encourage fair processing. As an example, less than twenty years ago, facial recognition did not seem to be a viable mass technology. Now faces are used as passwords. Discussions on discriminatory scoring based on mood as reflected in faces would have been science fiction. These examples demonstrate why the IAF believes the future enforcement model in the United States should be "fairness". Taking this approach will require rethinking the basis for enforcement.*

*On the other hand, the IAF believes open ended power to limit processing may lead to reticence risk, as it has in other jurisdictions. Reticence risk simply means data are not being fully used because the decision drivers are unclear. The IAF sees examples of reticence risk as a result of guidance from European regulators. For example, reticence risk can limit the innovation potential of data because the European guidance on profiling and automated decision making is broader than the language in the GDPR. Instead a model is needed where accountability is encouraged and oversight is based not on second guessing decisions but rather on determining if they were made with integrity and competence.*

If the U.S. were to enact federal privacy legislation, what should such legislation look like? Should it be based on Fair Information Practice Principles? How might a comprehensive law based on Fair Information Practice Principles account for differences in uses of data and sensitivity of data?

*Fair Information Practice Principles ("FIPPs") were formulated in the early 1970's when data and systems were one and the same. In that era, they were first designed in a linear fashion where data were mostly collected directly from people. Those individuals were informed about the purposes for which the data were collected, and they agreed, or did not object, to those uses. The conundrum of how to differentiate data provided by the individual and the observations of organizations was never really resolved. However, FIPPs are the backbone of the OECD Privacy Framework and are well understood across the world.*

*Today, in contrast, the ecosystem is based more on observed and created data than the collection of provided data. Observation is necessary for many technologies to work. The*

*challenge is how one applies the FIPPs to this less direct world. The IAF believes one does so by thinking about the FIPPs in a less linear manner and about how all the principles in their entirety provide guidance and protection. One applies the principles based on the context of use. For example, in machine learning, the accuracy gained from robust data use should have greater emphasis than the requirement for data minimization.*

*The IAF, however, does not totally reject the FIPPs. Instead, transparency, data quality and integrity, and security are building blocks for the Essential Elements of Accountability. The IAF believes the Essential Elements of Accountability are more effective in defining next generation guideposts for organizational behavior. Those concepts are the basis for the IAF Framework.*

Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

*The IAF believes that the global communications and information ecosystem is not bound by state lines. Therefore, it is hard to see how state laws will be effective in overseeing either national or global markets. In addition, the likelihood of inconsistent and even conflicting State laws will add to the complexity, not only for businesses and consumers inside the United States, but also for the global ecosystem and the many consumers that take part in it.*

Short of a comprehensive law, are there other more specific laws that should be enacted? Should the FTC have additional tools, such as the authority to seek civil penalties?

*The IAF believes that a comprehensive law is preferable and that penalties should be within the scope of the comprehensive law. While there is a place for laws specific to a well-defined sector, eco systems are so integrated it has become very difficult to even define sectors todays. This is already seen in smart watches that may conduct EKGs. Which sector would regulate those watches? Would that change based on how people use the devices? Would that change on the way new apps are developed? Focusing on a specific use, such as qualifying individuals based on data aggregated for that specific purpose, may be possible. The Fair Credit Reporting Act is such a law, but that is a very piecemeal approach.*

How should First Amendment norms be weighed against privacy values when developing a legal framework?

*The Unites States data culture is based on freedom for individuals and organizations to observe what is in the public domain and to robustly use information technology to assist in thinking with and learning from data. Organizations also feel free to create new data as the product of processing what is observed. Such an entrepreneurial spirit does not mean that guideposts are not needed. Norms are set by laws such as the Equal Credit Opportunity Act. The problem in the United States does not lie in encouraging expression through thinking and learning with data but rather with the expansion of the public commons that has taken place over the last generation. Sensors observe, and observation is necessary for everything from smart cars to advertising supported content. In the physical world, we understood that what went on in our front yard was part of the public commons but that what went on in our houses was not. The public commons became less clear when the Internet expanded observation, and the challenge has only grown with mobile computing and the Internet of Things. Business models have been built based on observation. Rather than stifle the innovation that comes with expression, the IAF framework is designed to preserve the benefits of the freedom to think and learn with data by*

*placing requirements on organizations to be accountable. This approach means privacy and ethics by design and requires assessments that take into consideration the interests of all impacted parties.*

**General Questions**

What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to realize these benefits?

*Every time a person is protected by collision avoidance braking or has their heart rhythm restored by an embedded defibrillator, they are receiving the benefits of an information age technology that is dependent on society's ability to think with and then innovate with data. So, every individual is likely to receive benefits from data flows in almost every role they play, even if there are also risks. Organizations in the United States have a greater ability to use data to innovate because few of the laws here address the processing of data. Instead they address the application of data. From a competition perspective, former Federal Reserve Chairman Alan Greenspan was reported to have said the best explanation of the difference in growth rates between the United States and Europe was the greater application of information and communications technologies in the United States. The early benefits of this information era began with a national credit reporting system which facilitated a national consumer credit system rather than a local one. This development facilitated the expansion of the consumer economy in the United States. It is also why the World Bank encourages third party credit reporting as part of the necessary infrastructure for growth. That advantage continues today because of the ability to use data to discover new insights. The ability to use data for innovation makes it possible for new players to increase competition. However, the IAF believes it is now time to mandate some overarching guardrails just as the Fair Credit Reporting Act did for substantive decision making and the Safeguards Rule provided for security.*

What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?

*The objective of almost every analytics system is to transform data into knowledge and then make use of that knowledge. Knowledge almost always advantages some and disadvantages others. Those results are one of the reasons why the IAF strongly encourages fair processing approaches that emphasize data stewardship. Competition typically benefits from the free flow of data and is hindered by data being held by a narrow group of players. Yet controls are often more easily applied if data are held by a narrower group of players. To mitigate that risk, the IAF believes fair processing requires that obligations move with the data for which they are associated. This approach permits new players to emerge and the proper alignment of responsibility.*

*A downside of the more flexible regime in the United States is that it encourages broader data use and more experimentation. There is no question that more data from more touch points reduce the ability for individuals to function in an unobserved manner. Yet new technologies need to be observant to work. This result is a dilemma that has led to more discussions related*

*to digital ethics and therefore stewardship. The IAF framework is reflective of the desire to encourage innovation while also more broadly protecting against both hard and soft risks.*

The use of "big data" in automated decision-making has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer rather than a human?

*The IAF first published the "Unified Ethical Frame for Big Data Analysis" in 2014 which provided a vision for how predictive sciences could be used to create value for individuals, groups of individuals, society and organizations in a fashion that is ethical. As that work has evolved, the IAF has worked with organizations and regulators to evolve fair processing frameworks that include ethics by design, assessments of risks and benefits, and auditable controls. It is this mixture of ethical design, assessments and controls that facilitate these technologies being used in a beneficial manner while mitigating unfair consequences. This combination is the essence of fair processing in our present data driven ecosystems.*

Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

*While it may be desirable to define some data as being more sensitive than other data, it is important to recognize that it is more often than not the context in which data are used that creates real risks of inappropriate consequences. In many ways, this concept is already recognized in United States law. For example, under the Fair Credit Reporting Act, the risk of consequences when using consumer reports for employment decisions is different than when using the same report for credit purposes. Therefore, different protections are built into the employment report process. New data uses evolve so quickly that society cannot possibly create sector specific laws for each and every business process. That is one of the reasons why the IAF is suggesting fair processing solutions that make use of ethics by design, assessments, and auditable controls.*

Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?

*Dashboards and controls that allow individuals to express their preferences and create their own communities are always a good thing. However, data are increasingly used in a manner that goes well beyond common understanding. In those instances, fair processing by organizations based on sound external criteria, as discussed, is more effective in respecting the full range of individual, societal and organizational interests.*

Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers' finances in a directly measurable way. Alternatively, a "non-market" injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?

*The FTC was created by Congress to protect consumers. As discussed earlier, the difference between individuals and consumers is why the IAF focuses on individuals and not just their role as a consumer of goods and services. Based on its current legal mandate, it is appropriate for the FTC to focus on market harms. There are times where risk to reputation impacts the ability for individuals to participate in the market, and from that perspective, those harms are within the FTC's current scope. However, a privacy regulator typically has a broader mandate to protect individuals in almost all their roles. That would almost surely include non-market harms. From an interoperability perspective, it would be useful for the privacy regulator in the United States to have similar jurisdiction over both market- and non-market-based injuries. When data practices were more linear, harm may have been more objectively measured and therefore more appropriately limited to market-based injuries. In today's complex information ecosystem, harms may not be direct, and the privacy regulator's jurisdiction should not be limited to market-based harms. The FTC's mandate creates a dilemma when looking beyond market harms.*

In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?

*Effective data governance operates at every stage in the data lifecycle. At every point in collecting, creating, thinking, learning and acting with data, the accountable organization makes a decision that collecting or creating the data is appropriate or not, or the organization makes a decision that data use is value creating for stakeholders and that the risks to those stakeholders is low or can be mitigated. It is rare that data use is either all good or all bad. It is the use context that guides how to balance the interests of all stakeholders. The use context in turn makes bright line rules very difficult to develop. There is no magic bullet. Context and accountability matter. That is why the IAF has encouraged data stewardship as part of a governance process. Data stewardship is different from being a data custodian. A data custodian follows the rules. A data steward has a responsibility to understand the impact of processing on all stakeholders and act appropriately. A data steward uses ethics by design, assessments and auditable controls. Data governance with stewardship is the appropriate approach.*

Should policymakers and other stakeholders attempt to improve accountability for privacy issues within organizations? Why or why not? If so, how? Should privacy risk assessments be mandated for certain companies? Should minimum standards in privacy protections be required?

*As mentioned earlier in these comments, the IAF was founded as the Global Accountability Dialogue. The IAF's mission is the development of accountable processes. Beginning in 2015, the IAF conducted work and published assessment frameworks. Some of this work has been conducted under grants from privacy commissioners in Canada and Hong Kong. In Europe, the IAF work on legitimate interest assessments included participation by European regulators. Assessments come with various levels of rigor. For example, traditional privacy impact assessments ("PIAs") look at the legal issues related to particular processing. Legitimate interest assessments in Europe add the balancing of individual interests versus those of the organization. Ethical assessments, as developed by the IAF, require a cataloguing of stakeholders and evaluating the positive and negative impacts to those players. In many ways, Canada has been a laboratory for moving up the maturity curve for assessments. Canada's private sector privacy law*

*requires organizations to be accountable. The Canadian accountability principle has been interpreted to require PIAs. IAF Canadian work suggests that PIAs should be augmented with ethical questions when organizations are using data beyond common understanding. That approach would include almost every big data or artificial intelligence project. Canadian organizations that have moved to comprehensive assessments have found that such assessments not only accommodate good privacy, but that they also reduce impediments to using data wisely. So ethical assessments have been used by Canadian enterprises to reduce internal barriers to using data by creating greater certainty about what might be right and wrong.*

How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?

*An essential part of any accountability program is to share data in a manner where obligations associated with data are maintained. When these obligations are maintained, organizations must conduct due diligence, contractually bind data partners, and enforce contracts. Essentially, organizations are responsible for creating an accountability chain.*

What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?

*Privacy interventions are part of an overall data governance strategy. They are tactics used to mitigate negative consequences. None of the strategies mentioned above are perfect, but when used as part of an overall strategy, they help to effectively mitigate risk.*

Do firms incur opportunity costs as a result of increased investments in privacy tools? If so, what are the tradeoffs between functionality, innovation, and security and privacy protections at the design level?

*A Canadian company that was part of the ethical assessment project in Canada recently informed the IAF that the strategy that they built based on the framework developed in the project saved them a million Canadian dollars each year. There are costs associated with any governance process. However, those costs may be offset by greater clarity in how data may be used to create value for external stakeholders as well as the company.*

If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker? What is the best way to strike that balance and assess its efficacy?

*The IAF believes transparency is very important. There should be no secret data systems. Transparency also adds to the ability for the market and regulators to govern fair behavior. The IAF published a paper on Effective Data Protection Governance that discussed transparency for individuals and regulators being two different communications devices. The IAF staff does not believe choice based on privacy notices is effective in governing complex processes beyond common understanding. Moreover, given today's complex information ecosystem, the IAF does not believe that all of the responsibility for managing information use should be put on the individual. The best way to strike a good balance is where the use of the data is beyond the common understanding of the individual, the organization should be required to implement accountability mechanisms that balance the interests of all stakeholders to determine whether the processing of data is fair.*

To what extent do companies compete on privacy? How do they compete? To what extent are these competitive dynamics dictated or influenced by consumer preferences, regulatory requirements, or other factors?

*This question goes beyond IAF research*.

Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?

*This question goes beyond IAF research.*

Given rapidly evolving technology and risks, can concrete, regulated technological requirements – such as data de-identification – help sustainably manage risks to consumers? When is data de-identified? Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable? If not, are there alternatives?

*This question goes beyond IAF research.*

What should the role of the Commission be in the privacy area? What would define successful Commission intervention? How can the Commission measure success?

*The Safeguards Rule is an example of a regulation that sets expectations while leaving the compliance details to organizations. It is also a regulation that is interoperable with similar regimes in other regions. The IAF believes the transition from governing privacy by enforcing against deception and unfairness to governing by fair processing could be handled in a similar fashion. Canadian privacy enforcement agencies set the table for such a system when they published "Getting Accountability Right with a Privacy Management Program." Canadian companies and agencies have built their programs based on that guidance, and enforcement strategies have been established on reviewing programs based on that guidance. Currently, the FTC often requires this type of accountability as part of consent orders. The IAF believes this type of guidance would be useful beyond consent decrees.*

The IAF appreciates the opportunity to participate in this hearing preparation. Please direct your questions to Martin Abrams, Executive Director, (mabrams@informationaccountability.org 972.781.6667).