November 15, 2022

The Information Accountability Foundation (IAF) is a U.S.-based non-profit engaged in research and education on the accountable and fair processing of data pertaining to people. The IAF continues the groundbreaking work of the Global Accountability Dialog,[1] which defined the essential elements of accountability, which in turn formed the basis for data protection laws and regulations in Europe, the Americas, and Asia. The IAF's core beliefs are that:

- Progress, both negative and positive, comes from using data to create knowledge and then applying that knowledge as action. Therefore, It is critical that organizations engage in knowledge discovery (the use of data to create new insights) and knowledge application (the application of those insights to make decisions that often impact people) in order to achieve a trusted global ecosystem.
- To be trusted, organizations must be accountable, responsible and answerable, and be prepared to demonstrate their accountability.
- Frameworks based on risk assessments and effective data governance enable beneficial, data-driven innovation while protecting individuals and society from the potential harms that may arise from data processing in the digital age.

These comments were prepared by the IAF staff and do not necessarily reflect the views of the IAF board or membership.

These comments bundle the answers to numerous questions being addressed by the ANPR and list the questions being addressed. Some general comments are made prior to the answers to the group of questions.

An Unfair Processing Rule Is Needed

The IAF congratulates the FTC on initiating a rulemaking proceeding to address data protection, privacy and information security and appreciates the opportunity to provide the FTC with comments based on years of research and experience in these vital areas. The IAF believes that comprehensive federal guidance regarding the commercial processing of information about people, particularly the observation of individuals and their actions online, is long overdue. Concerns about the application of new digital technologies that observe people's activities date back to the dawn of the commercial Internet in the 1990s. Unfortunately, three decades ago, policymakers punted on the question of whether third party cookies were an intrusion into an individual's private space, leading to an unregulated Internet where personalization based on passive observation is the default.[2] Since the initial uses of third party cookies

[1] The Global Accountability Dialog was an independent project under the Centre for Information Policy Leadership in 2009. The project ran from 2009 until 2014 when the last meeting was held in London, England. The IAF was the result of the incorporation of that project.

[2] E.g., Beyond Cookies: Privacy Lessons for Online Advertising

and similar digital tracking technologies in the 1990's, passive observation has enabled the creation of a wide range of beneficial, innovative products and services, but those also cause adverse processing impacts that range from minor inconvenience to serious harms impacting the physical and mental health, safety, finances, identity, reputation and autonomy of American consumers of all ages.

Recognizing the potential for consumer injury in the late 1990's, the FTC encouraged websites to voluntarily adopt fair information practices to protect the privacy of consumers.[3] Beginning in 2000, the FTC recognized that self-regulation alone did not adequately protect consumer online privacy and recommended legislation to guarantee basic consumer protections.[4] The FTC's strong and vocal support for privacy and data security legislation continues until today.[5] The FTC's flexible "unfairness authority" provides a solid foundation for such a legal framework. The logical and adaptable application of unfairness to evolving commercial practices dates back to at least 1980 when the FTC issued a Policy Statement on Unfairness, and Congress effectively codified the unfairness doctrine in 1994 amendments to the FTC Act.[6]

The unfairness doctrine is applicable particularly to those situations where harms and benefits arising from the application of rapidly evolving technology need balancing. An act or practice may be unfair if it: (1) "causes or is likely to cause substantial injury to consumers;" (2) the injury "is not reasonably avoidable by consumers themselves," and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition."[7] The flexibility of the unfairness doctrine, however, produces a lack of clarity and uncertainty regarding what conduct would be designed as unfair, leading commentators to complain about the lack of rules, policy statements or guidelines explaining what conduct is actionable under the unfairness doctrine.[8] The IAF suggests that the pervasiveness of observation in today's digital world, which produces both beneficial outcomes and harm, requires the FTC to enact a transparent unfair processing rule with clear guideposts. Such a rule must identify the types of adverse processing impacts that may meet the FTC's test for "substantial injury" and thus support an enforcement action. The IAF has drafted a comprehensive list of "adverse processing impacts" that it respectfully suggests the FTC should consider when drafting the rule and soliciting stakeholder feedback..

Comparing a rule based on the FTC's unfairness authority with privacy laws in other jurisdictions demonstrates why such an approach is important, effective, and practical. The European Union General Data Protection Regulation (GDPR) requires that the processing of personal data be fair. This vague "fair" standard triggers other requirements such as the completion of Data Protection Impact Assessments to determine whether a given processing action is fair. Canadian privacy law, both at the provincial and federal levels, requires that processing must be reasonable from the perspective of the reasonable consumer, even if the individual provides consent. Unfairness is different, requiring that the specific processing activity causes or is likely to cause harm to consumers (injury or adverse processing

[3] FTC 1998 Report to Congress on Privacy Online; FTC 1999 Report to Congress on Self-Regulation and Privacy Online
[4] FTC 2000 Report to Congress, Privacy Online: Fair Information Practices in the Electronic Marketplace
[5] FTC 2021 Report to Congress on Privacy and Security
[6] Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691 (1994) (codified at 15 U.S.C. § 45(n)).
[7] 15 U.S.C. § 45(n
[8] E.g., The Unfairness Doctrine: Has the Commission Gone Too Far?

outcomes) and that the consumers are unable to avoid or correct for such harm. In addition, the application of unfairness balances that harm against benefits to consumers and competition.[9]

This more nuanced and detailed analysis is more appropriate than applying a vague "fairness" test since the FTC is an enforcement agency with robust authority rather than a privacy regulator.

IAF's comments to specific questions expand on this discussion.

Defining The Scope of Unfair and Deceptive Commercial Activities

The ANPR defines the acts or practices to be regulated as "commercial surveillance," which refers to,

> *the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide – say, when they affirmatively register for a service or make a purchase – as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first.*

"Commercial surveillance" appears to be related to the term "surveillance capitalism," coined by Professor Shoshana Zuboff. Wikipedia defines surveillance capitalism in the following manner:

> *Surveillance capitalism is an economic system centered around the capture and commodification of personal data for the core purpose of profit-making.*

Importantly, Wikipedia's concise definition adds a purpose, "profit-making."

At the request of the OECD, the IAF published a paper in 2014 that identified four categories of data, "The Origins of Personal Data and its Implications for Governance" . One of the four categories is "observed" data, which is explained as follows:

> ***Observed data** is simply what is observed and recorded. The emergence of the Internet as an interactive consumer medium has made it possible to observe and digitalize data in a more robust manner. On the Internet, one may observe where the individual came from, what he or she looks at, how often he or she look at it, and even the length of pauses. Facial recognition and the Internet of Things is making observation in a digital manner possible in the physical world.*

Following this straightforward explanation, the paper then divided observed data into three sub-categories based on an individual's level of awareness of the processing.

> ***Engaged.** Engaged observed data includes data that originates from online cookies, loyalty cards, and other instances in which the individual is made aware of the observation at some point in time. While the individual may forget that the data is being created, there is a general awareness that it is taking place. In some cases, the individual can object to or abort the creation. For example, a person may disable the Wi-Fi on their mobile device*

[9] A proactive requirement that processing must be fair most likely would require legislation. The Federal Fair Credit Reporting Act is a law that requires organizations be proactively fair.

if they don't want to be observed. Regulation and industry practice have implications on which sub-classification a type of data might fit. For example, cookies are included in engaged because various regulations and industry codes have made transparency a growing norm.

Not Anticipated. *Not anticipated data creation are instances in which individuals are aware that there are sensors but have little sense that the sensors are creating data that may pertain to the individual. For example, a person may be aware that there are sensors in the tires on the car and in the oil pan in the engine, but the person might not be aware that the manner in which he or she maintains the car is a data element that might pertain to them. This sub-classification would be appropriate for many of the applications related to the Internet of Things. Typical individuals would have limited awareness of this type of data.*

Passive. *The last sub-category is passively created observational data. An example is CCTV in public places when combined with facial recognition. It is also applicable to any situation in which it would be very difficult for individuals to be aware that they are being observed and data pertaining to the observation is being created.*

This analysis recognizes that not all "observed data" presents the same level of risks to consumers. In addition, this more granular approach makes a distinction between observation and surveillance. The difference is that surveillance requires a target. Thus, not all observation is surveillance, but all surveillance is observation. Targets need not be clearly identified, but a person, object or place must have been selected as the target. Of course, the substance of any rule is far more important than definitions, but terminology is important. The IAF respectfully suggests a more precise definition for corporate surveillance would improve the proposed rule. The term "observation" should be used for commercial acts or practices that are not targeted for operational purposes and thus present less risk. In contrast, the term "surveillance" should be limited to targeted monitoring, collection, or processing for the purpose of influencing, persuading, or manipulating (either in the near term or over time). Applying this distinction will focus on those acts or practices likely to cause harm, thereby effectively putting industry on notice of those practices that cross the line.

The FTC's definition of "commercial surveillance" appears to cover the processing of any data pertaining to persons in a commercial setting without taking into consideration the method of collection, source of the data, consumers' expectations, purpose for the processing or potential secondary uses. The IAF believes that the FTC does not intend to sweep in legitimate, beneficial uses of data by commercial entities that have ongoing and transparent relationships with consumers. For example, a mobile phone operator observing location to provide uninterrupted service is a legitimate use. The same location data used to engage in fraudulent activity or manipulate a consumer is not a legitimate use. Inappropriate origin or use of observed data is an appropriate target for an unfairness rule. For that rule to be successful, it needs to differentiate between surveillance for misuse and observation for operational success.

ANPR Question #2 asks *Which practices do companies use to protect consumer data? Documentation and implementation of a comprehensive, organization-wide accountability program is the starting point for* most responsible organizations that process data about people. Recent laws require organizations to

identify, document and mitigate risk created by processing data.[10] Organizations must therefore understand the potential harm created by a given processing activity and the likelihood such harm will occur before deciding if the risk can be mitigated adequately. These obligations are described in the essential elements of accountability developed in 2009 with the participation of FTC staff, and further described in regulatory guidance from Canada, Hong Kong, Colombia, Australia, Singapore and most recently Bermuda. Without a comprehensive privacy law in the United States, accountability is voluntary and risk assessments are haphazard and inconsistent, which is bad for consumers, businesses, and enforcement agencies.

ANPR Questions #4, #5, #6, #7 request information about harms related to surveillance. The IAF's inventory of potential "adverse processing impacts" that may arise from processing data about people was created through a multi-year iterative process and informed by the extensive work of NIST and the FTC's Bureau of Consumer Protection. Throughout the process, IAF staff reviewed legal frameworks from multiple jurisdictions, state and federal legislative proposals, international standards and best practices, FTC reports and enforcement actions, and academic studies that catalogue potential "privacy harms." This inventory of potential harms does not address the severity of harm or suggest what standard should trigger potential liability in an enforcement regime. Rather, it's an inventory of potential adverse outcomes that should be considered when assessing risk created by a processing activity. The criteria for assessing risk should be included in any proposed rulemaking. A model for assessing risk can be found in the FAIR and OPEN USE Act, which presents a comprehensive list of over 30 questions that will help determine the potential severity of harm and the likelihood that such harm will occur. There is no quick and easy path to assess risk; it's context dependent.

Adverse Processing Impacts

The term "Adverse Processing Impact" means detrimental, deleterious, or disadvantageous consequences to an Individual arising from the Processing of that Individual's Personal Data or to society from the Processing of Personal Data, including—

1. direct or indirect financial loss or economic harm;
2. physical harm, harassment, or threat to an Individual or property;
3. psychological harm, including anxiety, embarrassment, fear, and other mental trauma;
4. inconvenience or expenditure of time;
5. a negative outcome or decision with respect to an Individual's eligibility for a right, privilege, or benefit related to—
    a. employment, including hiring, firing, promotion, demotion, reassignment, or compensation;
    b. credit and insurance, including denial of an application, obtaining less favorable terms, cancellation, or an unfavorable change in terms of coverage;
    c. housing;
    d. education admissions;
    e. financial aid;
    f. professional certification;
    g. issuance of a license; or

[10] E.g., Virginia Consumer Data Protection Act, Colorado Privacy Act, and Connecticut Personal Data Privacy and Online Monitoring Act

h. the provision of health care and related services.

6. stigmatization or reputational injury;
7. disruption and intrusion from unwanted commercial communications or contacts;
8. discrimination in violation of Federal antidiscrimination laws or antidiscrimination laws of any State or political subdivision thereof;
9. loss of autonomy [11]through acts or practices that are not reasonably foreseeable by an Individual and that are intended to materially—
    i. alter that Individual's experiences;
    ii. limit that Individual's choices;
    iii. influence that Individual's responses; or
    iv. predetermine results or outcomes for that Individual; or[12]
10. other detrimental or negative consequences that affect an Individual's private life, privacy affairs, private family matters or similar concerns, including actions and communications within an Individual's home or similar physical, online, or digital location, where an Individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

Harms Related to Adverse Processing Versus the Benefits from Robust Processing

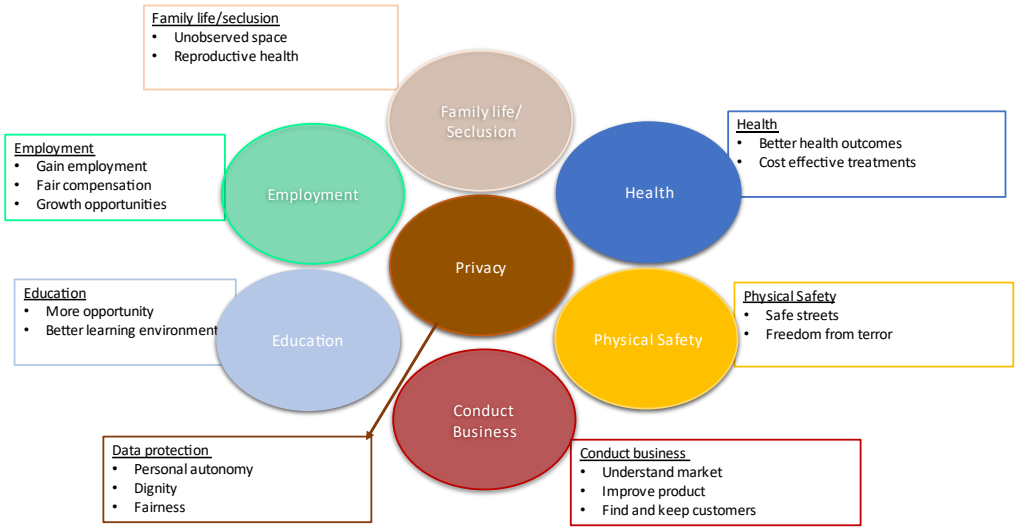
In ANPR Questions #24 through #29, the FTC asks how costs and benefits should be balanced. The IAF has conducted substantial work across different sectors of the economy to help responsible organizations identify the range of stakeholders impacted by processing data about people, both negatively and positively, and whether the risks of harm and benefits are asymmetrical. The IAF addressed this issue directly in its April 2022 paper "The Risk of What," which built on IAF's multi-year risk assessment project. The project is based on the proposition that those parties processing data pertaining to people need to identify (1) stakeholders impacted by a given processing activity as well as (2) stakeholders impacted by an entity's decision to forego processing for any number of reasons.

Below is a chart that illustrates the range of fundamental interests that may be impacted by an entity's decision to process or not process data in a given context.

[11] The concept of "loss of autonomy" is widely recognized in many bills and frameworks including the NIST Privacy Framework, which provides that, "[l]oss of autonomy includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement." Catalog of Problematic Data Actions and Problems.

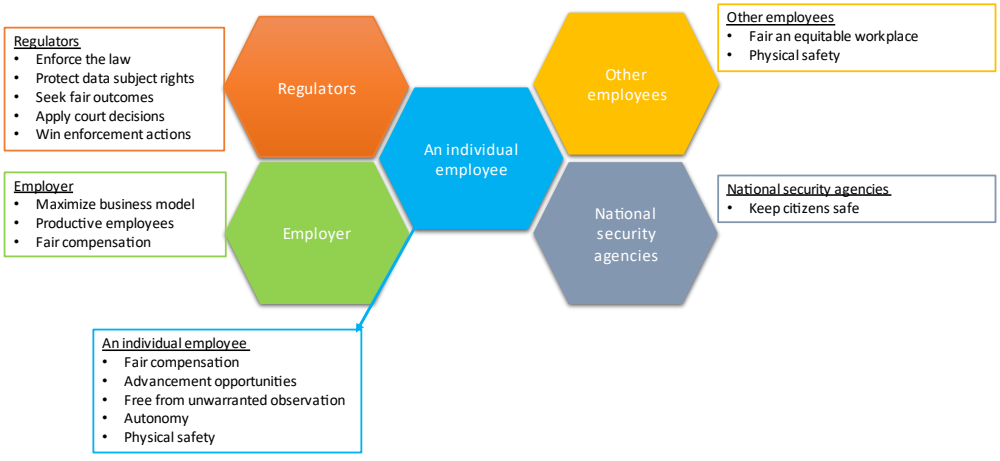
[12] The IAF Model applies the well accepted drafting convention that "or" means "either or both", or if there is a series of items, "anyone item or combination of items".

Fundamental Interests



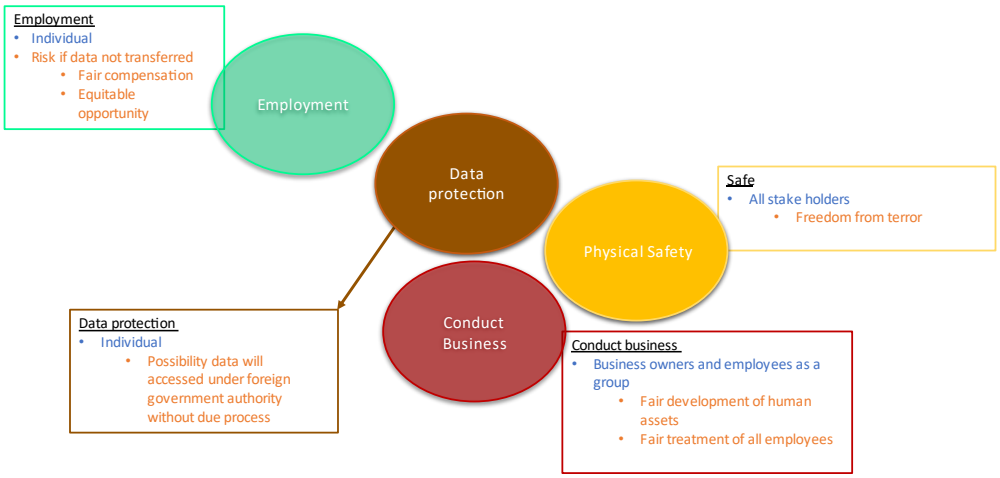
The IAF has conducted research on the transferring of human resource data to the United States from Europe. The next chart shows the parties that have an interest in those transfers.

Stakeholders related to the transfer of HR data for employment review



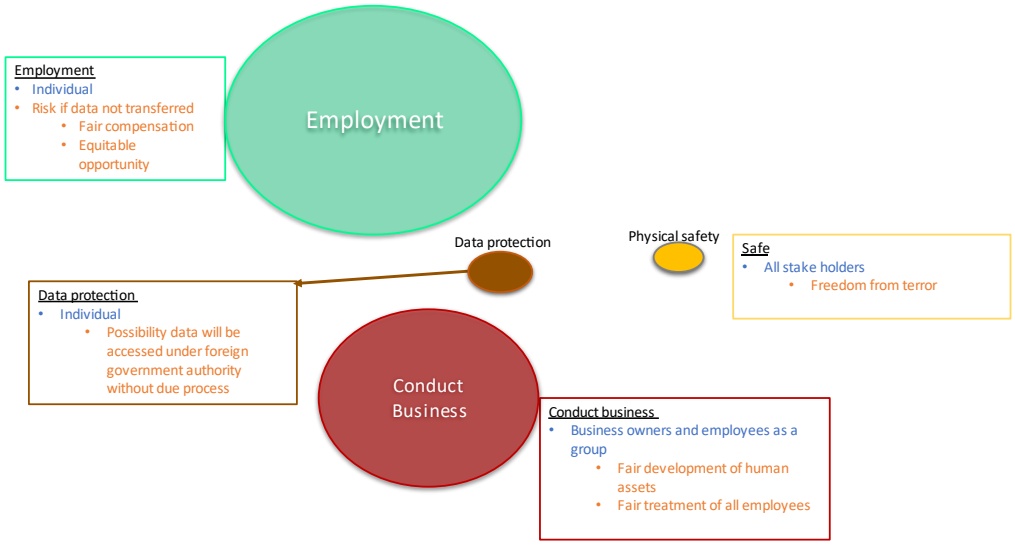
The next chart shows the fundamental interests to be considered.

Fundamental Rights Related to HR Transfers



The next chart shows how the fundamental interests might be weighted.

Fundamental Rights Related to HR Transfers- Weighted



Costs and benefits can be identified and weighted against each other, enabling an organization to determine when it would be unreasonable to go forward with a particular processing activity (act or practice). The analysis necessarily is dependant on context and may be subjective. Thus, it is important

for the FTC in a proposed rulemaking to explain clearly to regulated entities the criteria the Commission will use to assess risk and how the Commission will weigh costs and benefits. This explanation will provide regulated entities with the ability to engage in lawful data processing that does not violate the FTC Act's prohibition on unfair acts or practices or any proposed rule based on that authority.

Data Minimization

ANPR Questions #43 through #50 relate to the long established OECD privacy guidelines related to data minimization. Data collection and use should be limited to meet the objectives of legitimate processing with a stated purpose, and future processing should be consistent with stated purposes. This principle requires a balancing between effectively and fully achieving the previoulsy disclosed legitimate purpose of a given processing activity and restricting the collection of data to that which is strictly necessary to enable the purpose to be achieved, even if not at the optimal level from the entity's perspective. Complicating this principle is the fact that in the digital age processing may, and often does, create new data. For example, the credit prescreen process permitted by the federal Fair Credit Reporting Act (FCRA) allowes for calculations based on the underlying credit tradeline data. Those calculations are derived data. The derived data, which may be very substantial, also is covered by the principle.

Advanced analytics, including the experimental phase of AI processing, is about creating the knowledge that is then applied to either guide decision-making or, in an automated fashion, make decisions. There is less risk of adverse processing outcomes in this experimental stage than there is when data actually is used to makes decisions. There are risks, such as incomplete knowledge and insecure systems, and those risks need to be assessed and mitigated. One of the ways that the risk of incomplete knowledge may be mitigated is by using all the data necessary for knowledge to be accurate. The Centre for Information Privacy Leadership published a 2013 paper entitled "Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance." The paper discusses the risk differential between the discovery phase and the application phase in big data processing. Those findings have been the basis for guidance in numerous jurisdictions. The bottom-line is, to achieve accurate outcomes, the minimal amount of data necessary for knowledge discovery is anything but minimal. As a result, certain safeguards may be mandated as part of an unfairness rule. The data necessary for accurate application and the minimal amount of data necessary to achieve legitimate objectives typically are less than what was needed for knowledge discovery.

ANPR Question #48 asks specifically whether data minimization requirements or purpose limitation would unduly hamper algorithmic decision-making or learning-based processes. Knowledge discovery and knowledge application are different. The GDPR provides that research always is a compatible purpose, yet that statement is not always interpreted as written. The draft Canadian federal privacy law, C-27, allows (with conditions) for data to be used for research and analysis without obtaining consent. Pure data driven research indeed may be a repurposing of data. However, that repurposing serves other legitimate interests for the consumer, other consumers, and competition. The knowledge discovery should be evaluated to make sure that the objectives for the processing are sound and not illegal, unfair, or unjust (prohibited discrimination), but a bright-line rule that prohibits repurposing, the IAF submits, is inappropriate.

Algorithmic Error and Assessments

ANPR Questions #53 through #59 explore issues related to algorithmic error. The first application of probability to large data sets to enhance decision-making was the first credit scores in the 1980's. The scores were based on the probability that a person with a particular credit history was likely to default on a loan. That likelihood did not mean that any specific individual would default but rather that a certain number of a hundred consumers with similar histories would default. To safeguard consumers, scores were subject to the Equal Credit Opportunity Act, lenders needed to disclose their use of scoring and the risk factors that linked to an adverse outcome needed to be disclosed. These requirements benefited consumers by facilitating a national credit market that increased competition.

Credit scoring and the lending based on those scores have been regulated in part since the data used for scoring is covered by the FCRA. The FCRA covers consumer reporting in general, not just credit. The FTC has brought cases against tenant and employment screening services.[13] A key is defining the parameters for a substantive decision that impacts a consumer in a considerable fashion. Not all decisions pertaining to a consumer have a substantive impact on a consumer. A decision not to target an ad to an individual might not be substantive, while a decision to not allow an individual to purchase a good or service might be substantive.

The FCRA also provides guidance on how to determine whether an algorithm is biased. The FCRA allows financial institutions to obtain prescreened consumer lists if they intend to extend a firm offer of credit to each consumer on the list. Once the prescreened individuals have been identified for inclusion on a consumer list, the consumer reporting agency may provide the financial institution only with limited information about each individual. Firm offers of credit that satisfy the FCRA also must comply with other federal and state laws, such as the prohibition against unfair acts or practices and discriminatory acts. In order to determine whether a prescreen mailing was discriminatory, the financial institution obtains a full consumer report from the consumer reporting agency. If there was discrimination, the financial institution must adjust its process accordingly. The same approach could be used with respect to AI algorithms – after the algorithmic processing has occurred, sensitive personal data could be used to check the algorithm to make sure that it did not have a discriminatory impact, and if it did, the algorithm should be adjusted accordingly.

When considering an unfairness rule, the FTC might want to consider whether the Commission has achieved maximum milage from the FCRA. If new rules are necessary to protect people's privacy and information, they should be crafted carefully and in line with fifty years of learning from the FCRA.

As stated earlier in these comments, the IAF believes that accountability is a principle that is applicable to the fair processing of data pertaining to people. When using probabilistic processing, organizations should document the stakeholders that will be impacted by the processing, and what those adverse consequences might be.

Consumer Consent

ANPR Questions 73 through 82 pertain to the effectiveness of consent to govern consumer surveillance and data security practices. The FTC's specific questions suggest that consent is ineffective in governing personal data within complex observational ecosystems. The IAF concurs with that sentiment.

[13] E.g., U.S.A. v. AppFolio, Inc.; U.S.A. v. HireRight Solutions, Inc.

Consumers often do not understand how complex processing helps make products work. Yet consent globally, and notice and choice in the United States, is the proffered governance methodology.

Consent is most easily traced to the OECD Privacy Principles, specifically the "Use Limitation" principle that says data only should be used consistent with the consent given by an individual or by the authority of law. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the private sector privacy law, and the international law that tracks most closely to the OECD principles, requires that data users receive consent from individuals before data is used. PIPEDA does permit implied consent where that implied consent would be considered reasonable by a reasonable individual. Guidance from the Office of the Canadian Privacy Commissioner has pushed back on implied consent. Singapore's law, heavily modeled on PIPEDA, adopted consent as the primary mechanism for data governance, with a laundry list of exceptions. The regulators in both countries have issued guidance[14] on the accountability principle that requires data be used in a responsible fashion even if consent would allow less than fair treatment of data. Singapore recently amended its national law[15] to allow for more exemptions and allow for flexibility where there is demonstrable accountability. Canada's draft private sector privacy law, C-27, also would grant greater flexibility. However, C-27 does not allow personal information to be collected or used without consent for the purpose of "influencing" the consumer.

The GDPR often is characterized as being consent based. Consent is one of six legal bases to process personal data under the GDPR, yet it is the one most used by commercial organizations. Data processing in Europe must be lawful and fair, even if consent is granted by the individual. So, consent does not create a license to use data in a manner that causes inappropriate adverse consequences.

In past policy papers,[16] the IAF has suggested that consent should be reserved for instances where consent will be effective fully, and the complex ecosystems discussed in the ANPR are not limited to cases where consent is effective. In cases where consent is ineffective, commercial entities should be obligated to use the data in an appropriate and fair fashion and should demonstrate that their practices meet that standard.

The lesson from other countries is that even where consent is the first pillar for governance, consent is inadequate in highly observational systems. Instead, those countries are looking to organizational accountability with demonstrable sound processes including assessments. Consent should not be used as a means to get around behavior the FTC has deemed unfair.

Transparency

ANPR Questions #83 through #93 are on notice, transparency, and disclosure. Trust does not exist without transparency, yet clear and complete transparency has become an oxymoron. This generational issue began with consumer browsers that made possible the consumer Internet. Understanding that history is important in considering new policy answers.

With the rapid expansion of the consumer Internet, the Clinton Administration and the FTC encouraged organizations to adopt online privacy notices. The FTC conducted surveys to quantify the percentage of websites with privacy notices. From the very beginning, those notices were expected to be both

[14] Getting Accountability Right with a Privacy Management Program; Accountability Within an Organization
[15] 2021 Personal Data Protection Regulations
[16] The IAF publications page includes at least eighteen papers on assessment driven governance.

accurate and easily readable by consumers. One-page notices soon grew to several pages and then even longer and longer. They were written by lawyers to limit legal liability, and readability was a casualty. Sector specific laws, such as GLBA and HIPAA, required greater transparency. When GLBA required a privacy notice be mailed to every consumer from every financial services company annually even though consumers did not read them, the demand for short-form notices led to projects such as the one at the Centre for Information Policy Leadership[17] in 2001 that developed a short form notice based on food labels. Some critics said the short form notices were deceptive because of the detail that was not included in the short form notice. The FTC held a 2002 workshop on improving privacy notices and participated in a project with other financial services regulators to develop a standardized GLBA notification. The OECD published a report on multi-layered notices in 2008.[18].

Organizations responded with food label notices, layered notices, dashboards, and many other devices. Yet, as data systems become more complex, communicating complex processing still is a challenge. For example, regulators have questioned whether advanced analytics can ever be understood well enough to satisfy data subject information requests. After a generation, policy governing transparency still is inadequate.

The IAF for a long time has suggested that transparency should serve three main purposes:

- Be a detailed description of an organization's data practices that would be available to regulators so they can fulfill their regulatory responsibilities. These documents would be available to the public, but the public would not be the targeted audience.
- Inform individuals so that they may exercise their rights.
- Provide a snapshot for busy people so that they have a sense about how data that pertains to them is being used.

It is unlikely that one approach will serve all three purposes. So, the IAF believes that the obligation should be that organizations have different means for satisfying all three objectives, rather than requiring one specific notification satisfy all three purposes. The approach will be different based on the purpose. For example, the approach for satisfying the snapshot requirement might be a video or a comic book. While organizations should make a good faith effort to be consistent, differences in approaches are not deception, unless the purpose of the document was to obscure an adverse processing impact.

Conclusion

IAF staff appreciate the opportunity to contribute to the ANPR. If there are questions, please direct them to Martin Abrams at mabrams@informationaccountability.org or 972.955.5654.

[17] Martin Abrams, an IAF officer, led the CIPL short form notices project.
[18] Martin Abrams was the principal author of the OECD report.