For Circulation January 1, 2019

Fair Processing Principles to Facilitate Privacy, Prosperity and Progress

The information ecosystem in the United States is the world's most innovative. It has not just driven economic growth, it has facilitated positive changes in all sectors. At the same time, high levels of observation along with advanced analytics have increased angst in individuals and a sense that they may be harmed by the misuse of information from them or about them. To further the discussion about a U.S. privacy regime, the Information Accountability Foundation ("IAF") puts forth these principles for a U.S. privacy framework. The framework is intended to:

- *preserve America's innovation engine,*
- *be interoperable with other new and emerging privacy regimes,*
- *protect individuals' interests in privacy, and*
- *protect all the benefits of the 21st century information age.*

While interoperable with other regimes, this framework is American in its vision and structure and is divided into two parts. The first part describes the rights necessary for individuals to function with confidence in our data driven world. The second part is focused on the obligations that organizations must honor to process and use data in a legitimate and responsible manner. While the framework outlines principles, in some cases it *includes means and outcomes to better illustrate a particular principle.*

Individual Rights

1. **Transparency** Individuals have the right to be free from secret processing of data that pertains to or will have an impact on them. Organizations should provide understandable statements about their data collection, creation, use and disclosure practices and about their policies and governance. While these statements may be directed at enforcement agencies, they should also be publicly available. To augment this level of transparency, Organizations should also provide summaries and other means that make their data collection, creation, use and disclosure practices understandable to individuals.
2. **Access and Redress** Individuals have the right to request access to and information on the data they provided, to understand what data is observed by the organization that

pertains to them, and to be told what types of data are inferred by analytical algorithms. They also have the right to request changes to data to ensure accuracy, provide feedback, and receive relevant explanations on data use. Individuals have the right to object if they believe that the data about them is inaccurate or being used out of context, is not being undertaken in an accountable manner, or if they believe that uses of data are not legitimate. The right to object to processing does not pertain where data processing and use are permitted by law. Because intellectual property rights may prevent individuals from having full access or disclosure of inferences made by the organization, and where inferences such as scores potentially have negative consequences for individuals, organizations should provide relevant explanations about their processing, appropriate opportunities for feedback, and the ability for individuals to dispute such processing.

3. **Engagement and Appropriate Control** Individuals have the right to control data uses that are highly consequential to them. This should be facilitated through an appropriate level and contextual application of consent where possible. Where consent isn't possible or less impactful, they have the right to know that accountability processes assure the data uses are fair and responsible. Individuals also have the right to know that data is disclosed to third-parties beyond the context of the relationship or the legitimate purpose of the data use and to request such disclosure not take place, with the exception of data shared to assure security or for public purposes required by law. Where highly consequential uses, such as health, financial standing, employment, housing and education, are governed by specific laws, those laws take priority.

4. **Beneficial Purposes** Individuals have the right to expect that organizations will process data that pertains to them in a manner that creates benefits for the individual or for a broader community of people. In cases where the organizations receive most of the benefit, a demonstrable vetting process should determine there is minimal risk or impact to an individual. All data processing including for beneficial purposes should be part of understandable summaries required under the Transparency Principle. Where there are benefits and the potential for negative consequences to individuals, individuals should expect an explanation of the results and the ability to dispute the findings, as provided in the Access and Redress Principle.

Accountable Data Stewardship

5. **Assessed and Mitigated Impacts** All collection, creating, use and disclosure of data should be compliant with all applicable laws, industry codes, and internal policies and practices, and should be subject to privacy, security and fair processing by design. Employees should receive appropriate training for their specified roles, and accountable employees should be identified to oversee privacy, security and fair processing obligations. Specifically, fair processing assessments should identify individuals and groups of individuals who are impacted, both negatively and positively, by the processing, and should guard against identifiable negative consequences. Where

there are negative consequences, organizations should mitigate those consequences to the degree possible. If unacceptable consequences still persist for some individuals or groups, the organization should document why the benefits to other individuals, groups and companies are not outweighed by the unacceptable consequences.

6. **Secure** Data should be kept secure at a level that is appropriate for the data.

7. **In Context** Data should be collected, created, used and disclosed within the context of the relationship between the individuals to whom the data pertains and the organization, based on the reasonable expectations of individuals as a group. Public safety, security and fraud prevention are considered within context.

8. **Legitimate Uses** Data should be processed only for legitimate uses that have been disclosed, would be expected or are consistent with those uses. When the data is no longer necessary for the legitimate use, it should not be retained in an identifiable manner.

   Legitimate uses include the following:

   a. Where individuals have provided informed consent.

   b. Ongoing business processes such as fraud prevention, accounting and product improvement that would be expected of an enterprise.

   c. Freely thinking and learning with data by organizations that demonstrate effective accountability, including mitigating risks to individuals, consistent with the societal objective of encouraging data driven innovation, and that honor the Onward Responsibility Principle.

   d. Uses that create definable benefits for individuals, groups, organizations and society that are not counterbalanced by negative consequences to others, and that are based on assessments established by external criteria.

   e. Designated public purposes, including public safety and in response to an appropriate legal request.

   f. Organizations that stand ready to demonstrate why they believe other uses that are based on assessments established by external criteria are legitimate.

   g. Where permitted by law.

9. **Accurate** Data should be accurate and appropriate for all legitimate uses and that level of accuracy should be maintained throughout the life of the data.

10. **Onward Responsibility** Organizations that originate data should be responsible for assuring the obligations initially associated with the data are maintained within the accountability chain. As the data chain expands the previous data originator bears responsibility for the accountability chain. When data leaves the accountability chain, for example when requested by the government, the party providing the data to the government is only accountable for assuring the government has a legal right to request that data and disclosure is as limited as possible.

11. **Oversight** Organizations should monitor all uses of data to ascertain that the uses are legitimate, the data is processed fairly, the data is accurately used within the context of the relationship with those to whom the data pertains, and processes that support individual rights and accountable data stewardship are effective and tested. The oversight process, whether conducted by an internal body or an external agent, should be separate from and independent of those persons associated with the processing.

12. **Remediation** Organizations should stand ready to demonstrate the effectiveness of policies, practices and internal oversight to those that have external authority for oversight. Organizations should consider rectifying negative consequences where they reach a level of significant impact to individuals.