January 2020

SUMMARY OF "FAIR and OPEN USE Act"

The Information Accountability Foundation ("IAF") is a global policy think tank dedicated to facilitating information-driven innovation while protecting individuals' rights to privacy and autonomy. IAF believes that accountability-based information governance is central to achieving this outcome.

To help policymakers understand how the concept of accountability can support a legal and enforceable privacy framework, IAF published model privacy legislation titled the "Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical Act" or the "FAIR and OPEN USE Act" or the "Model Legislation." The core principles of the Model Legislation are derived from the IAF's Fair Processing Principles to Facilitate Privacy, Prosperity and Progress or the "Fair Processing Principles." Although published on January 1, 2019, the Fair Processing Principles reflect many years of work and consultations with hundreds of thought leaders from across the globe.

Some preliminary insights about the Model Legislation may be helpful. First, IAF attempted to draft a bill with 2030 in mind, rather than focus on what many believe are the greatest challenges today. Accordingly, a "black list" of prohibited practices or a "white list" of approved practices will not be found in the Model Legislation. The Model Legislation generally rejects the U.S. sectoral approach to privacy, as the distinctions become more meaningless each year. The concept of risk is central to the Model Legislation, liberally borrowing from the successful and ongoing work at the National Institute of Standards and Technology and elements of the General Data Protection Regulation ("GDPR"). The absence of "black lists" and emphasis on risk management necessarily means that organizations will be required to make judgments.

Several words many would expect to find in a proposed legislative framework are intentionally omitted: privacy, harm, rights and advertising. Although some of the vocabulary in the Model Legislation may be new, most of the concepts are not. IAF looked to a wide range of bills introduced by members of Congress as well as legislative proposals from diverse U.S. stakeholders, including the Center for Democracy and Technology, Intel, the U.S. Department of Commerce and the California State Legislature.

Finally, in an effort to develop a framework that will be interoperable with legal regimes around the world, IAF looked to principles published by non-governmental organizations

such as the OECD and APEC, as well as legal frameworks in the EU, Canada, Australia and Asia. Many concepts have been ported from GDPR, including the definitions of personal data and processing.

IAF, a 501(c)(3) "think tank," is not advocating for legislation or supporting a particular bill. Its goal is to provoke a thoughtful discussion about privacy legislation in the U.S. and to inject new ideas about accountability and risk assessment into the conversation. IAF published the Model Legislation in response to statements from policymakers that while they understood "accountability," they did not understand how it could be the foundation of an enforceable legal framework. The Model Legislation is an educational tool illustrating just that, how an accountability framework can protect individuals and promote innovation.

PURPOSE

The FAIR and OPEN USE Act's stated purpose is to:

- Preserve America's innovation engine;
- Protect individuals' interests in the fair, ethical, transparent, and responsible processing of their personal data;
- Mitigate risks of adverse impacts from the processing of personal data; and
- Promote the benefits of the 21st century information age through an agile regulatory framework.

Section 102, "Findings and Purpose," provides a more detailed discussion of the intent behind the Model Legislation and its novel approach. There are two foundational principles:

- The benefits of the information age belong to everyone; and
- In today's data-driven economy, organizations must be responsible stewards of personal data and be accountable for their actions.

In addition, we live in a complex, data-driven world with diverse business models and infinite possibilities for innovation. IAF believes that this reality requires an equally complex, nuanced, innovative, and agile policy and regulatory response. Difficult digital challenges that evolve in real time cannot be solved with a short, simple legislative solution. We must embrace complexity, not run from it.

WHO AND WHAT ARE COVERED?

Organizations covered by the Model Legislation include commercial actors subject to Federal Trade Commission ("FTC") jurisdiction, as well as common carriers and non-profits. Non-profit entities are not subject to the civil penalty provisions of the FAIR and OPEN USE Act. Although there is no carve out for "small business," certain small businesses (and small non-profits) are not subject to the enforcement provisions of the FAIR and OPEN USE Act. In addition, the requirements of the FAIR and OPEN USE Act can be applied and adapted to entities of any size or scale.

The requirements apply to "personal data" as defined in GDPR. The bill identifies four categories of personal data: provided data, third-party provided data; observed data; and inferred data. Personal data in the context of employment is excluded.

The Model Legislation does not define "sensitive data," as that concept will evolve over time and varies by jurisdiction. It is addressed through comprehensive risk assessments. In addition, there is no definition of "de-identified data." Again, identifiability or linkability of data goes to the level of risk created by the processing activity, not the applicability of the Model Legislation.

Although the term "harm" is not used, the Model Legislation defines a broad concept of "adverse processing impact," meaning the "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." The definition includes a non-exhaustive list of examples. Adverse processing impact should not be confused with litigation issues around proving "injury" for standing in Federal court or articulating a cognizable harm or damages for a proper claim for relief.

The Model Legislation covers "processing," borrowing the definition from GDPR, and then more narrowly defines "processing action" and "processing activity."

LAWFUL PROCESSING: LEGITIMATE USES AND RESPECT FOR CONTEXT

In general, processing is allowed when it is for a legitimate use or when the processing is consistent with the context of the relationship between the organization and the individual. There are eight defined legitimate uses: (1) compliance with legal obligations; (2) information security; (3) ongoing business processes; (4) protection of property rights; (5) public safety and health; (6) informed consent; (7) knowledge discovery (research); and (8) defined and documented benefits. The last three—informed consent, knowledge discovery and defined and documented benefits—are defined and have limitations and obligations.

Respect for context is defined as processing "within the reasonable expectation of similarly situated individuals." Section 201(c) identifies the factors to be considered when evaluating reasonable expectations.

The Model Legislation introduces the concept of "beneficial processing" and includes restrictions on processing personal data if individuals do not derive a benefit or value from the activity. This provision attempts to codify a fundamental belief of IAF that data should not just serve the interests of the organization that collected the data.

ACCOUNTABLE PROCESSING MANAGEMENT PROGRAM
(equivalent to a privacy or data protection program.

A covered entity must maintain an accountable processing management program, taking into account the covered entity's size and complexity, activities, and legal requirements. The program should be designed to:

- Ensure compliance with the FAIR and OPEN USE Act, other applicable legal or regulatory requirements, and industry best practices;
- Promote effective management and oversight of processing;
- Manage risk, including processing risk, on an ongoing basis;
- Evaluate both adverse and beneficial impacts of processing; and
- Demonstrate the covered entity's ongoing commitment to fair processing.

The program must include: strong leadership; collaboration across the covered entity; appropriate resources, staff, polices and procedures; data governance; a program to ensure ethical and trustworthy design (privacy by design); employee training and awareness; an independent and objective internal review, audit and assurance program; and Internal Data Processing Review Boards for high risk processing.

MANAGING RISK

The Model Legislation relies on a simple, straightforward concept: not all processing creates the same level of risk to individuals and society. The greater the risk created by a processing activity, the greater the restrictions and obligations.

To operationalize risk assessment, Article V requires a covered entity to establish a risk management program to identify, assess, mitigate and monitor processing risk on an ongoing basis. "Processing risk" is defined as the level of "adverse processing impact" potentially created by processing, assessed as a function of—

- The likelihood that adverse processing impact will occur as a result of processing; and
- The degree, magnitude, or potential severity of the adverse processing impact, should it occur.

When assessing the potential severity and likelihood of adverse processing impact, the Model Legislation requires a covered entity to consider context, including the purpose for the processing, sensitivity of the personal data, linkability and identifiability of data, the sources of information, and other factors.

The Model Legislation creates five distinct levels of processing risk: minimal; low; moderate; high; and extreme. Section 5.03 provides a limited set of rebuttable presumptions to illustrate how a covered entity should categorize risk in different contexts. Covered entities will be required to make informed decisions, exercise judgment and be accountable for their actions. There are no bright line tests and the assessment of risk in a given context can be challenging. In light of these challenges, a covered entity cannot be held liable solely for incorrectly categorizing the level of risk for a particular processing activity.

Processing impact assessments are required when the processing of personal data is:

- Reasonably likely to create a moderate or greater level of processing risk;
- Involves new or novel methods of automated processing; and
- Other identified circumstances.

As part of the processing impact assessment, covered entities are required to develop procedures to accept residual risk and authorize processing.

IMPLEMENTATION OF THE FAIR INFORMATION PRACTICE PRINCIPLES

Notice and Transparency—Covered entities must publish two notices: (1) a comprehensive statement for regulators and others interested in the details around processing and (2) a summary statement for individuals. The comprehensive public statement must include an organization's "guiding principles for accountability and data responsibility," a new concept to promote both transparency and accountability. In addition, explicit notice is required before using an individual's personal data for high risk processing.

Individual Control and Choice—The level of control is tied to risk.
- Individuals can opt out of the use of their personal data.
- Informed consent is suggested, but not required, for high risk processing
- Extreme risk has a separate standard
- Individuals must be able to withdraw consent.
- Individuals can opt out of the sharing of personal data with third parties

Data Quality and Accuracy—A covered entity must ensure that personal data is reasonably accurate, complete, and current, taking into account the use of the personal data and the level of processing risk.

Data Minimization—A covered entity may not maintain personal data in identifiable form once the personal data is no longer necessary for a legitimate use. "Identifiable form" is not defined.

Access, Data Portability, Correction and Deletion—A covered entity must provide individuals with access to their personal data, but the scope of access depends on the category of personal data: provided data; third party provided data; observed data; and inferred data. The level of processing risk also informs the scope of information that must be made available to an individual. In limited circumstances, when processing creates no more than a moderate risk, a covered entity may provide a statement of accountability in lieu of access, subject to penalties for abusing this provision.

Individuals must be able to:
- Dispute and resolve the accuracy or completeness of personal data;
- Delete their data, to the extent practicable; and
- Transmit or transfer personal data or otherwise download data.

Information Security—Covered entities must maintain a comprehensive information security program that includes administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of personal data.

Exceptions—The requirements in Article III are subject to specific, limited exceptions depending on the context, use of data and risk.

SPECIAL REQUIREMENTS FOR AUTOMATED PROCESSING

The Model Legislation includes additional requirements for "automated processing," defined as processing through a machine-based system that can, for a given set of objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Automated processing includes techniques such as machine learning, artificial intelligence, deep learning, analytics, or the use of algorithms.

Section 3.01(d) addresses transparency and explainability, requiring notices to make individuals aware of automated processing and to help them understand both the purpose and outcome of such processing.

Section 3.06(c) provides individuals with the ability to challenge the outcome of automated processing in certain circumstances.

Section 4.03 requires, among other things, a covered entity to:

- Understand the reasoning behind automated decisions or recommendations;
- Decide whether to accept the decision or recommendation;
- Implement safeguards and take steps to mitigate bias; and
- Ensure that data is labeled or traceable to enable analysis of the outcome or decision.

Finally, when automated processing is reasonably likely to create a moderate or greater level of processing risk, a covered entity must conduct an enhanced processing impact assessment to analyze the unique risks raised by automated processing.

SERVICE PROVIDERS AND THIRD PARTIES

When retaining service providers, covered entities must:

- Conduct appropriate due diligence before selecting a service provider;
- Contractually require implementation of appropriate measures;
- Contractually limit the use of data and processing; and
- Exercise reasonable oversight.

With respect to third parties:

- A covered entity may not transfer personal data to a third party unless that third party is contractually bound to meet the same processing and security obligations.
- Upon request, a covered entity must provide an individual with a list identifying the specific category or categories of third parties with whom the covered entity shares the individual's personal data.

- An individual can request that a covered entity discontinue the sharing of personal data with third parties.

ENFORCEMENT

The FTC will enforce the proposed framework. The FTC is granted full independent litigating authority and may seek the full range of equitable relief available in the Federal judicial system. In order to carry out its obligations under the Act, the FTC is granted additional resources, including up to 500 new personnel.

Civil Penalty Authority

The FTC may seek civil penalties for specified violations of the FAIR and OPEN USE Act. Civil penalties phase in over time, and the Model Legislation includes a civil penalty cap per violation. The cap does not apply to a handful of provisions that are explicitly identified as "separate independent violations." These include: Section 2.01(d), which prohibits relying on a legitimate use without having a reasonable basis; Section 2.03, which creates a separate violation for the reckless disregard of risk; Section 4.04(c), which prohibits knowingly providing substantial assistance or support to an entity that violates the FAIR and OPEN USE Act on an ongoing basis; and Section 5.06, which prohibits certain misrepresentations about impact assessments.

An individual may be liable for civil penalties if the individual knowingly violates the FAIR and OPEN USE Act, creates a high or extreme level of risk and cause significant adverse processing harm. That is a very high burden of proof and unlikely to be used in the vast majority of cases. Finally, the FTC may not seek civil penalties against a non-profit.

Oversight

Section 7.04 grants the FTC new authority to conduct limited reviews of covered entities for compliance with the FAIR and OPEN USE Act.

Safe Harbor

A covered entity that is in compliance with an approved code of conduct may not be subject to civil penalties or oversight reviews authorized by Section 7.04

State Enforcement

State Attorneys General may also enforce the FAIR and OPEN USE Act. There is no private right of action.

Federal Preemption

State laws are preempted "to the degree they are focused on the reduction of processing risk through the regulation of personal data processing activities." In sum, state privacy laws intended to prevent consumer harm related to the collection and use of personally identifiable information would be preempted. Certain state laws are excluded from the preemption provision.

LIMITED APA RULEMAKING AUTHORITY

The FTC is required to promulgate three narrow rules:

- Section 3.08(d), to modify or add additional exceptions and limitations to the requirements in Article III regarding accountable organizations
- Section 5.07, to provide additional clarification with respect to assessment and categorization of processing risk
- Section 7.03(a), to identify procedures for codes of conduct

In addition, the FTC is granted "restricted" APA rulemaking authority. If the FTC chooses to promulgate rules in addition to the mandatory rulemakings, the FTC must consider the potential benefits and costs to individuals and covered entities. In addition, any regulations must be technology neutral.