IAF

Information Accountability Foundation

**California Privacy Protection Agency Stakeholder Sessions, May 6, 2022**
**Risk Assessments** (for Covered Businesses and others such as Service Providers)

Thank you to the CPPA for holding these Stakeholder Sessions providing the opportunity for a wide range of stakeholders to give feedback about the rulemaking for the CPRA. Hello, I am Barbara Lawler, COO and Senior Strategist of the Information Accountability Foundation.

The IAF is a non-profit research and educational information policy think tank. Our mission is to foster effective organizational accountability that facilitates a trusted digital ecosystem, and the ability for organizations to use data to create real value for people.

- We believe that to be trusted, organizations must be accountable, responsible and answerable, and be prepared to demonstrate their accountability.
- We believe that frameworks based on risk assessment 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.

As the interests of multiple stakeholders increase and the expectations that organization be accountable for the processing of data about people, risk assessments are a critical and necessary lynchpin of operational integrity for evaluating the risk to consumers' privacy and security.

Since 2014, the IAF has led multistakeholder research projects that describe ethics-based assessment frameworks for complex and potentially risky processing. Deciding to process data is in itself a risk-based action. This work includes global forums, as well as specific projects in the U.S., Bermuda, Canada, Singapore, Hong Kong China and Europe. Risk Assessment frameworks function as a governance model for organizations of all sizes, and should be encouraged regardless of the type of data processing activity or in anticipation of "significant risk" level, a regular and ongoing process as envisioned in California Sec. 1798.185(a)(15).

Accountability-based risk assessments are responsive to both aspects of accountability – being both responsible and answerable. The objective for the risk assessment is to demonstrate (be answerable) that data processing is responsible and that impacts to stakeholders are considered. Fundamentally, the question of who is impacted – people -- and how, and whether others – as in other people, larger groups or the public -- are part of a risk assessment that is demonstrable.

The risk assessment process creates the risk documents that provide a sustainable mechanism for the organization to be answerable and to demonstrate that it is acting responsibly.

To determine the risk of what and to whom, a measurable, vetted framework is needed to describe the impacts to people. That is, a framework of negatives to isolate and then manage and measure against. The IAF created such a framework as part of our model legislation, The FAIR and OPEN USE Act – which we've called "Adverse Processing Impacts", and is derived from the already vetted NIST Privacy Framework.

Incorporating Adverse Processing Impacts into risk assessments serve broader purposes. It creates mechanisms for PbD, points to controls that should be implemented and validated, informs usable and fair designs for consumers, and creates a strong linkage with security risk assessments based on NIST or similar frameworks such as SOC and ISO. It provides measurability for the organization. And equally important, as a means to measure and enhance the capability to oversee and review risk assessments by the Agency.

Although technical compliance is important, if that is the only focus, organizations will miss the bigger picture (strategic) issues and considerations related to the processing of data about people. Therefore accountability-based risk assessments should become the norm for structuring and implementing risk assessments and the broader privacy and security governance for all types organizations – Covered Business and Service Providers.

Thank you. Detailed resources can be found on our website, informationaccountability.org and are linked in the written submission of our comments (found on the next page, p3). We look forward to future discussions with the Agency on this and related topics.

Regards,

Barbara Lawler

IAF

Barbara Lawler
COO & Sr. Strategist
[redacted]
www.informationaccountability.org

Resources:
Adverse Processing Impact and Risk to individuals 2021-22

Expansive Impact Assessments and AI (Global) 2021

Bermuda Report on Information Accountability 2020
Bermuda Commissioner Comments on Information Accountability 2020

Singapore Checklist and Assessment for Legitimate Interests 2019-2020

Ethical Data Impact Assessments (Global) 2019

Data Stewardship Accountability and Impact Assessment (HK) 2018

Canadian Assessment Framework 2017
Canadian Assessment Oversight 2017

Legitimate Interests Risk Assessments (EU) 2017

Risk-Benefit Analysis for Data Intensive Initiatives (US) 2016

Big Data Assessment Framework and Worksheet (Global) 2014-15
Big Data Contextual Assessment for Marketing (Global) 2014-15
Enforcing Big Data Assessment Processes (Global) 2015