Information Accountability Foundation

RISK OF WHAT?

Setting Risk Priorities for Data Protection and Privacy

APRIL 2, 2022

FROM THE IAF POLICY SUMMIT

Executive Summary

Policymakers since 2012 have stated that data protection, the processing of data pertaining to people, should be "risk-based." There is no consensus on what the term "risk-based" means. The lack of consensus is a problem since risk prevention and mitigation require a definition of negative outcomes to be avoided. Does the term "negative outcomes to be avoided" mean absence of individual control? Does it mean harm to people linked to the processing of data? Does it mean the human and financial costs associated with not processing data? The lack of consensus leads to uncertainty on the part of people, organizations, regulators, and policymakers and fails to recognize that mitigating risk means appropriate mitigations not elimination of risk.

On September 17, 2021, the IAF held a workshop to help address the question "risk of what?" The dynamic nature of "risk of what" has only accelerated since the Workshop. There have been enforcement actions, new laws and guidance covering topics such as artificial intelligence (AI) and global data movements, and a war in Europe. So, the context in which the question was asked continues to evolve. In the end, the IAF policy staff concluded the best indicator of "risk of what" is the concept of adverse processing impacts captured in the IAF model legislation the FAIR and OPEN USE ACT.

Preamble

The statement "data protection should be risk-based" seems like such a simple one. Yet, ten years after there was great enthusiasm for European policymakers' 2012 announcement of a risk-based data protection regulation that would be less focused on procedural requirements, such as database registrations, there is deep confusion about what risk-based actually means. To some, it means the risk of tangible, measurable harm to specific identified persons. To others, it means the risk that people will not be able to control "their data" in a world of online tracking and linking. To others, it means specific types of processing. For example, under the Colorado Privacy Act, profiling, if it presents a risk of substantial injury to consumers, and targeted advertising are automatically subject to risk assessments. To some regulators, it means risks that people will not be able to exercise their rights to know how data is processed and to exercise rights of control. To other regulators, the concerns are about organizations not having the proper amount of governance in place to protect data from misuse or cyber intrusions. And to still others, it means the risk of benefits to people lost because data are not processed for new insights. And lastly, 2022 has brought the real fear that signals of cyber intrusion will not be discovered because data are not shared. All of these meanings are risks in a data rich observational world. However, risks need to be prioritized if damage to people is to be avoided. The question is how is a consensus achieved on risk prioritization when context matters? With these questions in mind, the IAF held a workshop September 17, 2021, to seek answers to the question "Risk of What?"

Stakeholder Perspectives are key to Understanding the Question "Risk of What?"

There are at least four groups of stakeholders who must be appreciated in order to consider the question "Risk of What?"

The first group of stakeholders are the policymakers that enact laws. They typically understand that an information age creates tensions that translate into privacy problems. Often the default simple answer is that people should have greater control over their data. From that point on, it is a matter of rules to give people control - data subject rights, obligations for data users to put into place mechanisms so people might exercise their rights, regulatory powers so regulators can ascertain whether controls are in place, and authority to judges to make sure the rules are interpreted and enforced in an appropriate manner. However, policymakers' interests do not stop there. They also have an interest in encouraging digital economies that are pro-growth and enhance international competition. These interests lead to conflicting policies. The most tangible example is the UK Department for Digital, Culture, Media and Sport (DCMS) data protection consultation document that suggests the UK Information Commissioners Officer (ICO) has a co-equal objective to encourage innovation.

Another group of stakeholders are privacy and data protection authorities and agencies (DPAs) (including consumer protection agencies such as the U.S. Federal Trade Commission (FTC)), who begin with the obligation to protect data subject rights, even where processing is very complex, and who also must ascertain whether data are used to achieve fair outcomes when data are processed, even when the mechanisms to achieve both objectives work in distinctively different ways. DPAs also are under pressure to not inhibit a robust digital economy through complex processes and disproportionate enforcement. They often find that enforcing data subject rights or data security fundamentals is more straight forward than other objectives. An example is the FTCs settlement with CafePress in March 2022. So, even where they believe data driven outcomes are unfair, DPAs fall back on rights such as transparency, breach prevention, and the ability to object to processing as the basis for enforcement. Regulators also are bound by the courts and constitutional interpretations. Judges interpret the law based on their reading of laws, regulations, and constitutional mandates. These interpretations often limit how regulators prioritize risks. For example:

- The European Court of Justice has interpreted the term "adequacy" in the EU General Data Protection Regulation (GDPR) to mean equivalency. This interpretation has caused regulators to determine that the standard to be used is the "possibility" of bulk collection of data by security agencies outside the EU rather than the "probability" that such bulk collection will occur.
- The United States Supreme Court has limited standing to sue to where there has been demonstrable harm. This holding has had a practical impact on how the FTC enforces laws such as the Fair Credit Reporting Act.

A third group of stakeholders are organizations, with a priority on what is clear and enforceable. Since data subject rights are what are most enforceable, organizations design and execute on processes to protect growing data subject rights that are slightly different from jurisdiction to jurisdiction. There also is a growing demand that organizations operate in a "fair fashion" while processing data, but the requirements to do so are less explicit. Shareholders and employees of organizations are impacted by the profitability of those organizations. So, there is a demand on organizations to use data forward processes to deliver a fair return on investment. One byproduct of this tension is organizations are often investing in different processes that are to meet procedural data subject rights and forgoing investments that would enable fair processing.

Lastly, and just as important, people as consumers and citizens are stakeholders. While there have been collective actions in numerous jurisdictions, the rights to collective actions have been explicitly enhanced by the GDPR. For example, the EU non-profit NOYB has filed over five hundred lawsuits in Europe, and decisions in those lawsuits have disrupted data flows. This result has been impactful, particularly on the actions organizations must take when transferring data and using cloud providers.

Intermingled between the different stakeholders are frameworks, principles and standards academics and organizations develop and propose that are intended to guide risk evaluations. Those groups and their materials range from the NIST Draft AI Risk Framework, the COSO Guidance on Enterprise Risk Management for Cloud Computing, or the Markkula Center for Applied Ethics at Santa Clara University Best Ethical Practices in Technology.

The lessons that come from these various stakeholder interests have muddled the prioritization required to have a risk-based system. Risk requires prioritization and then appropriate mitigation; that is exactly what is missing. Defining "risk of what?" was not supposed to be so difficult.

It is not just an absence of policymaker prioritization. "Risk of what?" has become more difficult, in part, because of an acceleration in technology and observation. There are sensors in everything, and modern computing and communications technology make the collection and use of that observed data both possible, attractive in some cases, and necessary in other cases so smart devices are smart. Predictive data sciences have become easy, compelling, and scary all at the same time. The policy approach, in some cases, is to create a layer of regulation apart from data protection. The proposed AI regulation in Europe and the newly passed AI regulation in China are examples.

Context for the IAF "Risk of What?" Workshop

Risk-based Laws and Regulations

2022 marks the 10th anniversary of the introduction of the GDPR. EU Commissioner Vivien Redding, with responsibility for data protection in 2012, said the new GDPR would be risk-

based, making it easier for consumers to understand and for organizations to implement. That theme, risk-based, continued throughout the four years it took the EU regulatory process to enact the GDPR and the subsequent two-years it took for the GDPR to go into effect. Risk-based was the key phrase, but the debate did not parse exactly what that phrase meant. The debate also did not anticipate the pace in which AI, and other data forward strategies, would become a major business imperative and a driver of international competitiveness.

The degree of difficulty is not just a European problem. Since the GDPR was enacted, new laws have been passed in numerous jurisdictions, including four states in the U.S.: California, Virginia, Colorado, and Utah, with six more expected in 2022. And the push for conflicting risk objectives continues. In December 2021, the new Canadian Minister for Innovation, Science and Economic Development was directed by the Prime Minister to both encourage digital growth and update privacy protection, and the UK ICO published a Consultation on risk management in enforcement.

What is meant by privacy?

As the terms "data protection" and "privacy" often are used interchangeably, the term "privacy" is important. There literally are thousands of definitions for the term "privacy." When definitions in foreign languages are translated, the diversity of definitions increase. For example, a literal translation of a Chinese definition is "the ability to hide shameful secrets."

Neil Richards' book, "Why Privacy Matters," begins chapter one with **Privacy's Definitional Problems.** He offers a working definition: "Privacy is the degree to which human information is neither known nor used." He immediately flips that definition to state, "privacy is: (1) information about (2) humans that is (3) used as well as known and is (4) a matter of degree."

The most important elements of Richards' definition are that they are not limited to personal information (instead, it is "information about humans"), and he adds the concept of context when saying "a matter of degree."

European fundamental rights law contains separate rights to privacy and to data protection. In this Report on the Workshop, the term "privacy" means the individual's interest in data pertaining to people to be governed in a fair fashion, and the term "data protection" means the rules and processes used to achieve that objective.

Risk Management Definitions and "Risk of What?"

"Enterprise risk management (ERM) is a methodology that looks at risk management strategically from the perspective of the entire firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may interfere with an organization's operations and objectives and/or lead to losses." – Definition by Adam Hayes at "Investopidea."

Many organizations have very well-established "ERM" programs. If that is the case, then the answer to "risk of what" should be found easily within those traditional programs. However, the ERM definition is limited to the "potential for harms that may interfere with an organization's operations and objectives." Privacy law is not about risk to the organization's operations but rather addresses the individuals to whom data pertain and those impacted by the processing.

The Merriam-Webster dictionary defines the verb risk as ***"to expose to hazard or danger"*** while the noun risk is defined as "*the possibility of loss or injury*."

A legal dictionary defines risk as *"the potential danger that threatens to harm or destroy an object, event, or person."*

The Oxford Languages dictionary defines a risk assessment as "*a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking*."

Wikipedia has a useful definition for risk management: "*Risk management is the identification, evaluation, and prioritization of risks followed by coordinated risk and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.***"**

The common element in all these definitions is a negative impact that should be avoided or mitigated that impacts a subject. That subject can be an object, a person, a group of persons, or some greater grouping such as an organization or nation state. For the purpose of this Report, the subject is a person or collective of persons. The risk management definitions add the component of lost opportunities, which require balancing the negative outcome of forgoing an opportunity because the potential negative outcome from engaging in an activity is substantial. In other words, a risk to those subjects needs to be balanced against a benefit to those same subjects. If the party that bears the risk is different from the party that receives benefits, the disconnect must be understood.

Neil Richards talks about privacy as power that comes from knowing human information. Therefore, risk analysis requires an evaluation of who is impacted by the gathering and application of data pertaining to people, where those impacts may be either positive or negative. Richards is defining a situation where the negative impacts and the positive impacts are different parties, with the party with the power receiving the benefits.

Corporate risk management programs are typically focused on the risk of negative outcomes to the organization, and that attention means the party to be protected is the party with power over others. Data protection law is focused on the risk not to the organization, but rather the individual to whom the data pertains. A "risk of what?" analysis needs to bridge between the typical subject to be protected and the subjects that are protected by data protection law and enforcement agencies.

The parties to be protected from adverse outcomes

Privacy as a fundamental human right is the legal foundation for data protection in most of the western world.[1] This right is actuated through the individual's right to know how and for what purposes data about him or her will be processed and the individual's ability to either allow or disallow that processing. The individual's inability to control the data that pertains to him or her, is, from a legacy fundamental rights perspective, the foremost negative impact to be avoided. This perspective places the individual to whom the data pertains front and center as the subject to be protected.

However, the law also is concerned with other negative outcomes to individuals' "rights and freedoms," and the interests of others impacted by a processing also are relevant. Furthermore, privacy and data protection are not absolute rights. So, from a risk management perspective, negative outcomes beyond control and negative outcomes to others should come into consideration.

Outcome risks increasingly are coming into focus in the literature and regulatory and public policy rhetoric. For example, the new Chinese AI regulation seems to be outcomes based. It targets adverse processing outcomes that come from the use of AI, a form of processing. It is not targeted to a fundamental right to privacy, a right that does not exist in Chinese law. The Chinese AI regulation also is not structured to provide the government with control over knowledge about people, as the Chinese privacy law does. Rather, its purpose seems to be to encourage social harmony by outlawing discrimination in pricing and other factors very visible to people. Negative outcomes, that would not take place but for advanced analytics driven by observed data, increasingly, are listed as a risk to be avoided. In the case of China, it is price and recommendations that have the effect of being discriminatory. In the United States, this focus particularly occurs when the potential enhanced discrimination of protected classes of people is considered.

So, from a risk based on negative outcomes to the subject at issue, from a public policy perspective, one risk to be managed is the inability to exercise rights, and negative social and economic outcomes are other risks to be managed. Those risks are to the data subject or other individuals impacted by the processing. Neither subject of the risk is the business, the entity to be protected in legacy ERM programs.

As mentioned above, much of the literature suggests privacy risk management should be part of an organization's overall ERM process. However, legacy risk management is typically focused

[1] Privacy and data protection law in the non-western world may or may not be based on fundamental human rights. For example, privacy law in China is more concerned with social harmony, and how consumer harm might impact that social harmony.

on risks to the organization. Those risks are not the risks that data protection law typically cares about, and not the ones identified in legislation such as the Chinese AI regulation. So, there is a conflict between the typical focus of corporate risk management, and the risks targeted by data protection.

There is a growing understanding that when organizations do not manage the adverse consequences they create for individuals, reputation, regulatory, and business continuity risks for the organization are created. In other words, third party risk becomes first party risk for the organization, and that is the bridge necessary between the differences in how business organization and regulators see risk. That bridge accommodates integration into organizational risk management activities.

IAF "Risk of What" Workshop

It is in this complex policy environment that the IAF held the "Risk of What?" Workshop. The IAF approaches data protection issues from an accountability perspective: Organizations should process data in a responsible manner as defined by law and norms and be answerable in a proactive manner for being responsible. Taking a risk-based approach is consistent with and helps organizations implement accountability. To be responsible, an organization must know the risks they create for others as well as themselves and manage those risks in a manner that serves the needs of the full range of stakeholders. That responsible behavior should be consistent in creating new insights and acting on those insights in a responsible manner. Therefore:

- New insights should drive innovation in a people-beneficial fashion;
- People should be protected from the dark side of data and insights' misuse;
- A risk-based governance system should further these goals;
- Such a governance system is dependent on an agreement on the negative outcomes that should be risk-based;
- There should be a means to contextually prioritize risks when making choices to process or not process; and
- There should be methods for oversight by an enforcement agency.

There is no shortage of definers of risk or risks that have been defined. Risks are being defined by lawmakers; privacy, consumer, telecommunications, healthcare, and competition regulators; national security experts; professional associations; academics; advocates; and even think tanks. What seems to be lacking is the means to prioritize the risks in a contextual manner. If every risk is a priority, then no risks are prioritized. Prioritization of risk is consistent with accountability strategies and frameworks.

Not every risk of an adverse outcome can be paramount; there needs to be a methodology for rank ordering. Not every regulator can be an expert on every human situation. So, authority must be distributed to the regulators with the most appropriate authorities and skill sets to

prevent unlawful outcomes, such as discriminatory lending. Solutions to this morass require well defined problem statements. A problem statement requires an understanding of the stakeholder interests involved.

Exploring Risk Ordering at the Workshop

The IAF laid out four potential negative consequences related to the processing of data pertaining to people:

1. People cannot exercise their rights to know and control because of procedural or transparency shortcomings.
2. People restrain their behavior or thoughts because of excessive observation.
3. People are harmed by inaccurate, biased, or inappropriate decisions related to civil, consumer or patient rights or societal norms.
4. The rights of stakeholders to jointly benefit from appropriate innovative uses do not take place.

To these consequences, the IAF added possibility that organizations do not have the program capabilities to manage the four mentioned possible negative outcomes. In other words, organizations do not have the comprehensive programs to be fully accountable.

Five breakout groups discussed risk ordering from five different perspectives:

1. Privacy Interests and Risk Ranking
    - Can one rank order privacy interests of seclusion, control, and fair processing?
    - Does the risk from reticence to impacting other fundamental rights rise to the same level as privacy risk?
2. Focus for Governance – Data Origination or Use
    - Does one apply privacy risk management based on data origin, or does one place greater emphasis on intended and actual outcomes?
    - Does organizational intent (knowingly creating a risk to people) modify the risk equation related to likelihood and level of consequences?
3. The Compatibility of Privacy and Innovation Risk management (Privacy Risk by Design)
    - Discussion paper by the UK Department for Digital, Culture, Media & Sport suggests that data innovation by design as a co-objective with data protection by design when designing risk mitigation. How does that get translated into corporate policy?
4. Observation and Risk to Secluded Space
    - What is out-of-bounds observation, and does it merit its own legal guidance?
    - How does one factor in applications such as mobile phones, smart medical devices, smart water meters where observation is necessary for the technology to work?
5. Fair Processing Risk and Prescriptive Law

- Can the law prescribe the process for assessing risks or just the purpose for such risk management?
- Does this include accountability for how other parties use predictive tools developed by an organization when that use impacts fundamental rights?

For the" Risk of What?" Workshop, the IAF postulated: Privacy has so many different meanings to different people it is more useful to define the interests that encompass privacy:

- A secluded space free from observation and intrusion
- Control over data that might define my nature and person
- The fair application over the processing of data that pertains to me – including an interest in data creating value that serves my needs or the needs of my community

Throughout the Workshop, the elements of those definable interests were reviewed iteratively by the participants, including a classification of risks to be managed in data protection.

<u>Key Findings from the Workshop Breakout Groups</u>

Discussion groups looked at risk ordering from these five different perspectives. There was no clear consensus on rank ordering risks. Instead, some of the following comments were heard:

- Most organizations are stressing data subject rights processes since regulatory requirements are specific and there is a clear sense that a failure to implement data subject rights could lead easily to an enforcement action.
- Passive data collection (not easily addressed by data subject rights, particularly transparency rights) increasingly has become important during the pandemic, in part because more activities have been virtual. How should that be addressed?
- Do current mechanisms for transparency inform anyone other than experts? What does that result mean for individual control?
- Risks are contextually based. So, the emphasis should be on the manner in which data are used and not how they are collected. However, laws and regulations typically require that purpose be described at collection and future use be in context (compatible with) the initial collection. This requirement is closer to the risk of loss of individual control and not about ultimate outcomes.
- For the most part, algorithms and AI are inconsistent with privacy regulations because they meet the various definitions for profiling. So, the risk is that the regulatory structure is inconsistent with the economic, competitive, and societal interests that need to be considered in outcomes-based risk assessments.
- Different types of regulations, or maybe even types of oversight agents, are needed to balance the targetable risks described.

- Organizations would prefer regulators describe what risks should be targeted but feel they increasingly are seeing very prescriptive descriptions of how the regulators would like to see risks managed and mitigated.
- Many organizations are not ready to demonstrate a comprehensive privacy management program.
- There is an attractiveness to standards-based certifications such as NIST and ISO even though they are viewed by some as overly prescriptive.
- There is frustration that there is no clear path for reusing data for beneficial purposes, even for scientific research and knowledge creation. "… in its simplest form, yes, limitations of data reuse can negatively impact both individuals and competitiveness."
- There is an increasing desire for ethics-based analysis. There have been efforts to formalize ethical analysis, such as corporate Environmental and Social Good programs and the ethics section added to the NIST Privacy Framework, but ethics is not law and is very situational. There is, of yet, no clear pathway to get there.
- Risk to "intrusion on secluded spaces" was downplayed because of a sense that those places are disappearing. This result is despite the growing rhetoric on surveillance capitalism and concerns about observational technologies.
- Organizations increasingly are focused on compliance strategies to permit data transfers from Europe regardless of whether there is even the remotest possibility the data might be subject to bulk collection by national security authorities.

Developments Since the Workshop

The FTC has announced a rulemaking related to unfairness and observational technologies. The European Union is moving forward with digital legislation to complete during the mandate of the European Commission Strategy on Data and AI that expires in 2024. Privacy scholars increasingly are focused on outcomes and placing less emphasis on individual control. Yet consent and consent-like requirements for informed objection are focused more on procedural rights related to individual control. Lastly, Russia's invasion of Ukraine has created additional geopolitical issues that still need to be identified.

Making Sense of it All

The IAF team believes "risk of what?" is the right question. Yet the question's answer is dependent on where a specific stakeholder sits in the data ecosystem. An individual's place in the ecosystem may be different based on the context of the information processing. At one moment, an individual may be the person generating behavioral information and, at another time, the person might be the beneficiary of research conducted with observed data.

Therefore, the IAF team went back to the desired objective for legislation. The IAF's model legislation, the FAIR and OPEN USE Act, set a key objective to be the governance of "adverse processing impacts." To determine the "adverse processing impacts," risks must be identified. There are four risk elements that organizations must identify and manage and that regulators

may evaluate. The corresponding "adverse processing impacts" that could result, as determined by assessing the four risk elements, are set forth in the "Fair Processing and Risk of What" Guide set forth below.

"FAIR PROCESSING AND RISK OF WHAT" GUIDE

The IAF developed four overarching risk elements to be managed through a risk-based approach to privacy. The four elements link to the three privacy interests the IAF postulated for the "Risk of What" Workshop. Privacy is difficult to define; however, the interests that encompass privacy can be defined:

- A secluded space free from observation and intrusion (Neil Richard's neither known)
- Control over data that might define my nature and person
- The fair application over the processing of data that pertains to me – including an interest in data creating value that serves my needs or the needs of my community

Four Risk Elements that Organizations Must Manage and Regulators May Evaluate

Risk Element 1: Inability to Exercise Rights

This element links to the concept that data protection begins with the individual's ability to control the data that pertains to him or her. For individuals to exert control, data protection and privacy law has created sets of data subject rights. These rights include: the right to know in great detail how data will be used and, in many cases, the right to consent to those uses, correct data, exclude or erase data and insights pertaining to the individual. In Europe, those data subject rights also include the right to object to some processing permissioned by a means other than consent. In California, those rights include the right to request that date not be sold or shared. There is a growing consensus that even though consent as a means of control is not practical, policymakers still are enthusiastic about data subject rights. Furthermore, where outcomes from the processing of data are seen as not being fair, regulators can look for flaws in data subject rights' implementation for an enforcement nexus.

Negative Impact to be Avoided

People cannot exercise their rights because of procedural or transparency shortcomings. Those shortcomings may range from websites that are not use friendly to data use descriptions that are either too dense, too incomplete or both.

Public Policy Objectives as Expressed by Laws

The laws or regulations will require organizations to have sound processes to make sure data subject rights are actionable by the person to whom

the data pertains. From an organizational risk management perspective, every law must be parsed for the manner in which the data subject right is to be exercised, and those means must be put in place so these rights can be exercised within the geographies covered by the laws.

Examples:

- Right to know
- Right to see data that pertains to them
- Right to a record of processing
- Right to object to some processing
- Right to approve some processing
- Right to prevent the sale or sharing of some data
- Right to have data be secured in an adequate manner

Measurables and Metrics

Individual complaints, assurance reviews and audits that indicate:

- Rights are not easily exercisable
- Rights are not transparent
- Rights are not properly implemented
- Processing is not explained completely
- Demonstrable privacy program is not apparent

Regulatory Oversight

Data protection and privacy authorities, consumer protections agencies with privacy authority, and sub national authorities with data protection jurisdiction (like state attorneys general).

Indicators of Fairness

- Individuals can easily exercise their rights
- Transparency is effective in informing individuals

Risk Element 2: Intrusion into Secluded Spaces

The respect for private and family life is set forth in Article 7 of the EU Charter of Fundamental Rights. It provides: "Everyone has the right to respect for his or her private and family life, home and communications." The Fourth Amendment to the U.S. Constitution establishes a similar protection from government intrusion, and there is a tradition against intrusion into individual physical private spaces. In California's State Constitution, Article 1, Section 1, privacy is an inalienable right that is protected, not only from the government intrusions, but also from violations by other individuals and private companies. In the physical world, there is a delineation between private spaces free from observation and public spaces in which there is no "privacy" expectation.

The virtual world has less clarity. Concepts such as "surveillance capitalism" concern themselves with this loss of clarity. As limited as it might be, there is some sense there is some space in the virtual world where seclusion will be respected.

Negative Impact to be Avoided

People stifle their behaviors or thoughts because of excessive observation. The watchful eye stifling behavior dates back to Alan Westin's "Privacy and Freedom, was developed more fully in Oscar Gandy's "Panoptic Sort" and was advanced most currently in Neil Richards' "Why Privacy Matters."

Public Policy Objective as Expressed by Laws

Organizations should not observe where there is an expectation of being in a private space. Where observation is necessary, the observed data that are created must be used only for purposes that a reasonable person would see as being in context. There should be no secret observation.

Examples:

- Inappropriate intrusion into secluded (private) space
- Disruption and intrusion from unwanted commercial communications or contacts
- Loss of control over private spaces

Measurables and Metrics

Reports, assurance review and audits that indicate:

- Assessments are conducted on whether observation was necessary and conducted with proper controls
- Assessments are conducted on whether use of observed data was appropriate in context

Regulatory Oversight

- Data protection and privacy authorities and other agencies
- Telecommunications regulators
- Medical device regulators
- Department of Transportation

Indicators of Fairness

- Secret observation does not take place
- Data are used in context

Risk Element 3: Inappropriate Outcomes to People

Former EU EDPS Giovanni Buttarelli famously said in 2018: "Data should serve people." The GDPR requires fairness, which includes fair outcomes, and the FTC Act prohibits unfairness. There are laws, draft laws and regulations that prohibit inappropriate discrimination caused by flawed analytic systems. China's new AI regulation prohibits discrimination in price and products made available. These rules are not new. U.S. regulatory guidance required that credit scores must be in compliance with the Equal Credit Opportunity Act. The California Consumer Privacy Act (CCPA) provides consumers with a right to non-discrimination when they exercise any of the rights provided by the CCPA. Therefore, the third risk element is outcomes-based.

Negative Impacts to be Avoided

- People are harmed by biased or inappropriate decisions related to civil, consumer or patient rights.
- People do not receive the tangible benefits of data driven insights because of data use reticence.

Public Policy Objectives as Expressed by Laws

Organizations are expected to recognize, mitigate, and /or minimize inappropriate outcomes to people and demonstrably contribute to trusted digital innovation. This expectation includes opportunity costs to people for not processing data where the outcomes would be people beneficial.

Examples:

- Inappropriate bias
- Inappropriate discrimination
- Preventable bad outcomes
    - Credit or employment denial caused by bias
    - Less than optimal health outcomes from insights not pursued
- Lost opportunities
- Diminished access to key services
- Loss of liberty

Measurables and Metrics

Reports, assurance reviews and audits that make visible:

- Demonstrable data stewardship program details
- Data use scenarios and decision-making processes
- Data use and escalation path to executives

Regulatory Oversight

- Scenario/Sector specific regulators
- Certification organizations
- Courts

Indicators of Fairness

- Data used appropriately to create value for stakeholders
- People are not harmed by the inappropriate use of data

Risk Element 4: Insufficient Programs to Mitigate Adverse Impacts

2012 Canadian regulatory guidance informed private sector companies that privacy accountability required organizations have comprehensive privacy programs. While ten-years old, Canada's accountability guidance is still the most referenced. The U.S. Federal Trade Commission required a similar program as part of an enforcement action against Google, Facebook and others. Hong Kong and Colombia adopted guidance similar to Canada. Singapore's privacy maturity model requires comprehensive programs, and such programs are part of the plans for an updated UK data protection law. The GDPR does not explicitly require a comprehensive program but instead requires most of the components

of such programs. There are many different types of assessments, including privacy, data protection, ethical, fairness and balancing assessments, and they increasingly are required by law and guidance.

Negative Impact to be avoided

Program capacity and capabilities are insufficient to mitigate the risks of procedural outcomes or shortcomings or adverse impacts to people.

Public Policy Objectives as Expressed by Laws

Organizations must have a comprehensive program, and where necessary, that program must include assessments. Laws tend to list the elements that must be included in the program and the situations that would require assessments. Program independence is sometimes discussed.

Examples:

- Requirements to have a comprehensive program
- Requirements that the program have executive sponsorship
- Requirements that the program be staffed and resourced at a level commensurate with the risks

Measurables and Metrics

Reports, assurance reviews and audits that show:

- Presence of a comprehensive program
- Evidence of the program functions
- Internal policy requirements that standards are implemented and that impacts from processing are assessed
- Assessments take into account data-related incidents and responses
- Program aligns with relevant standards, laws, and regulations
- There are assessment logs and reports

Regulatory Oversight

- Data protection and privacy authorities and other agencies (e.g., financial services regulators)
- Certification organizations

Indicators of Fairness

- Assessments are conducted with competence and integrity
- Programs are demonstrable to an oversight agency
- Outside experts' opinions sought where appropriate

Conclusions and Settling on Adverse Processing Impacts

Ultimately, "risk of what?" is filtered by context and how stakeholders are impacted by the context. A secluded space free from intrusion, individual control, fairness, and impact on other rights and interests, such as positive and negative innovations, are the priorities based on the context. Therefore, the IAF team believes that "adverse processing impacts" best captures the

concept that risks should be based on negative outcomes to be avoided, which means risk management should be part of a comprehensive, accountable privacy program.

The IAF model legislation, FAIR and OPEN USE ACT, is risk-based with a broad requirement that covered entities conduct risk assessments to identify, avoid, manage, and mitigate adverse processing impacts. The model legislation does not use the terms "harm" or "injury." Instead, the model legislation defines a broad concept of "Adverse Processing Impact." The definition of Adverse Processing Impact aligns with the approach to privacy risk and "privacy problems" codified in the National Institute of Standards and Technology's publication, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 2020. NIST defines privacy events as "potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal."[2] NIST identifies the range of problems an individual can experience as a result of processing as ranging from dignity-type effects, such as embarrassment or stigmas, to more tangible harms, such as discrimination, economic loss, or physical harm.[3] The definition of Adverse Processing Impact is also generally consistent with NIST's Catalog of Problematic Data Actions and Problems, which is a non-exhaustive, illustrative set of problematic data actions and problems that individuals could experience as the result of data processing. The IAF's model legislation defines the term "adverse processing impact" as follows:

> ADVERSE PROCESSING IMPACT.— 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;

[2] NIST Privacy Framework at p, 3.
[3] Id.

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
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 [4]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[5]
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.

[4] 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.

[5] 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".

In the final analysis, the answer to the question of “risk of what?” is best understood to be the overarching risk which must be managed by organizations and that is “adverse processing impacts”.