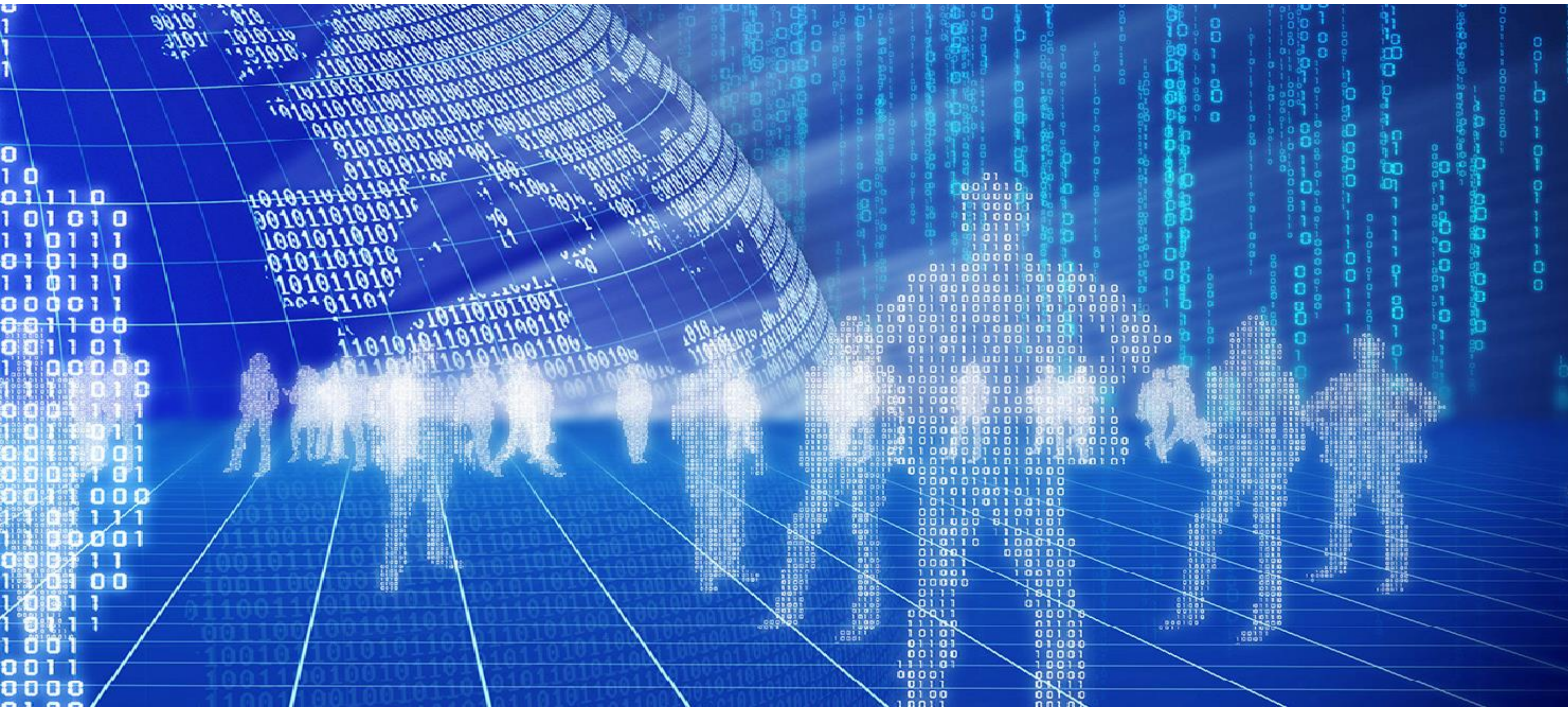
THE Information Accountability Foundation
COLLABORATIVE POLICY INNOVATION

The Movement Towards Demonstrable Accountability – Why It Matters

December 2020



Executive Summary

With Artificial Intelligence (AI), including advanced analytics and big data, beginning to affect almost every aspect of society, harnessing its potential for good while addressing its risks will require an end-to-end comprehensive, programmatic, repeatable demonstratable governance system[1] for adoption by all organizations seeking to use complex data analytical processing such as AI as part of their strategy and objectives. This system will be a step up beyond the accountability required for less complex data processing and will require a "trust" driven approach rather than just a "legal" compliance approach to accountability. This approach moves accountability based on legal privacy and data protection requirements to accountability based on "fair processing" of data.

At the same time, there is an accelerating trust gap between some regulators and general business practices. Regulators have expressed surprise at how unprepared organizations are to meet even legal compliance driven requirements. This revelation appears to be driving more prescriptive guidance on accountability which, while stating that "Accountability is not about ticking boxes," does seem to encourage check-the-box compliance. In addition, this trust gap has resulted in calls for more "demonstrable accountability."

In contrast to this trend, there are leadership companies that are going beyond compliance and adopting "trust" driven governance approaches because they view trust as a business-critical goal. Their goals are to make sure their technology, processes and people are working in concert to maintain the high levels of trust expected by their many stakeholders. In short, they are implementing trust driven, beyond legal compliance, demonstrable accountability processes.

This report will:

- Profile what these companies are doing to build trust in data innovations through enhanced accountability;
- Suggest some considerations for other organizations and for regulatory guidance and future public policy; and
- Lay out new Fair Processing Demonstrable Accountability Elements.

These new Fair Processing Demonstrable Accountability Elements enable many of the economic benefits the use of advanced analytics that drive technologies like AI can bring to individuals, groups of individuals, society and organizations while meeting the broader needs of individuals, groups of individuals and society for ethical and fair data processing. The Information Accountability Foundation (IAF) believes these new Fair Processing Demonstrable Accountability Elements advance what the original Essential Elements of Accountability[2] are capable of doing in two key ways:
First, when implemented, they facilitate the trust necessary to enable the adoption of data driven

[1] Michael Hanford, IBM, Defining program governance & structure, 4/15/05, https://www.ibm.com/developerworks/rational/library/apr05/hanford/index.html (Governance typically refers to the collective set of policies, procedures and oversight internally & externally that manage the risk of systems and meets required obligations).

[2] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Data-Stewardship-Elements-002-1.pdf

technologies like AI and its associated data use. Second, they demonstrate accountability that goes beyond compliance. The original Essential Elements of Accountability, while key, simply meet compliance objectives regarding existing law.

The companies profiled in this study are continually improving on their processes. By contrast, many other organizations, seemingly encouraged by regulators, are focused on procedural risk elements associated with legal compliance accountability. This approach will not drive the trust required to enable the full potential of a digital driven strategy. While meeting compliance-based requirements, these leadership companies have shifted the focus to fair processing. They are concentrating on trust-based accountability built around ethical approaches. Regulators could look more to these leadership companies as examples of demonstrable accountability.

Introduction

On October 8, 2020, The Economist Intelligence Unit (EIU) made the bold statement "The AI Revolution is Now." 75% of the respondents to an EIU survey said they are experimenting with AI.[3] With AI, including advanced analytics and big data, beginning to affect almost every aspect of society, organizations should harness AI's unparalleled potential for the 'common good' and mitigate its potential for harm. This effort will include an end-to-end comprehensive, programmatic, repeatable demonstratable governance system[4] for adoption by all organizations seeking to use complex data analytical processing such as AI as part of their strategy and objectives. Governance and by extension accountability become increasingly challenging given the probabilistic nature of AI systems and the opacity associated with them. Organizations who want to use complex data analytical processing such as AI have to step up beyond the accountability required for less complex data processing.

Accountability is a basic tenet of 21st century data protection law and governance. It is referenced explicitly in the European Union General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the APEC Privacy Framework. It was touted as a major change from the EU Data Protection Directive to the GDPR. The IAF, as its name suggests, has been a major advocate for building out measures so organizations manage and use data in a responsible and answerable manner. To be trusted, accountability always has needed to be demonstrable. The IAF, which studies policies and practices necessary to use data wisely in a manner that serves people, is finding that organizations need to be explicitly accountable in a more formal manner. Why? More complex data analytical processing requires more accountability, and there is increasing evidence that regulators do not trust the current state of accountability. Regulators report they do not find accountability measurable and adequately implemented. For example, in its 2018-2019 Report to the Parliament of Canada, the Office of the Privacy Commissioner (OPC) criticized the governance component of accountability when it stated:

[3] "Staying ahead of the curve – The business case for responsible AI," 08/10/20, https://www.eiu.com/n/staying-ahead-of-the-curve-the-business-case-for-responsible-ai/

[4] Michael Hanford, IBM, Defining program governance and structure, 4/15/05, https://www.ibm.com/developerworks/rational/library/apr05/hanford/index.html (Governance typically refers to the collective set of policies, procedures and oversight internally & externally that manage the risk of systems and meets required obligations).

> We are increasingly noticing the ways in which it [accountability] has become deficient in today's world of complex data flows and less than transparent business models. Our recent investigations into Facebook and Equifax, for example, revealed that accountability as traditionally framed in the law is not strong enough to protect Canadians from the intrusive practices of companies who say they are accountable, but are in fact found not to be.[5]

The OPC is not the only regulator who has this view. In conversations with other regulators, the IAF has heard similar comments. For example, data protection and privacy regulators have expressed surprise at how unprepared organizations are to conduct even basic privacy impact assessments (PIAs) let alone Data Protection Impact Assessments (DPIAs)[6] required when data processing is considered risky.

The Irish Data Protection Commission conducted a cookie audit of 38 companies between August and December 2019 and found the cookie compliance of 35 of the 38 companies to be significantly lacking. According to the Commissioner, the audit is indicative of systematic non-compliance with the cookie rules.[7] Organizations that are not in compliance with laws and regulations have not met the first element of accountability – adoption of internal policies consistent with external criteria.

Moreover, the UK Information Commissioner's Office published an Accountability Framework[8] that tells organizations how to demonstrate their data protection compliance. The ICO Framework is divided into ten sections: Leadership and Oversight, Policies and Procedures, Training and Awareness, Individuals' Rights, Transparency, Records of Processing and Lawful Basis, Contracts and Data Sharing, Risks and DPIAs, Records Management and Security, and Breach Response and Monitoring. Each of those ten sections contains the same two subsections: "Ways to meet our expectations" and "Can you answer yes to the following questions?". Despite saying that "Accountability is **not about ticking boxes,"** the ICO approach does seem to encourage check-the-box compliance. Demonstrable accountability goes beyond these ten sections and the topics covered and the questions asked in the two subsections.

Complex data analytical processing like AI requires an investment in groundbreaking data governance and accountability standards. Recital 4 of the GDPR sets the tone for transitioning from a compliance environment which has a focus on procedural risk to a risk management environment based on impacts. It identifies the impacts and rights as follows:

> *The processing of personal data should be designed to serve mankind. The right to protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This regulation respects all fundamental rights and observes freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for*

[5] Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy, 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/

[6] GDPR Article 35

[7] Report by the DPC on the use of cookies and other tracking technologies, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf

[8] https://ico.org.uk/for-organisations/accountability-framework/

> *private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.*

Check-the-box compliance without explicit and formal demonstrable accountability has the potential to impact the next generation of organizational data protection programs and the future privacy and data protection law inspired by the GDPR.

The IAF is a global non-profit organization that conducts research and education on data protection and privacy from an accountability perspective. It long has advocated for accountability based on the impacts data use has on individuals. This approach requires taking accountability to a higher level so that the decisions made by organizations on complex processing of data, such as AI represents, are responsible and answerable. In order to explore its thesis that organizations need to be explicitly accountable in a more formal manner, the IAF studied leadership companies with a wide variety of data business practices. By leadership, the IAF means those companies with goals that go beyond basic compliance with data protection requirements to higher objectives such as those reflected in Recitals 1-6 of the GDPR. The results were encouraging. These leadership companies have basic accountability mechanisms that are easily demonstrable and adequately implemented. However, these leadership companies have gone well beyond the basics of accountability. The IAF learned that these companies are implementing demonstrable accountability against a broader objective of trust. These findings match the research in The Ohio State University report, Business Data Ethics: Emerging Trends in the Governance of Advanced Analytics and AI,[9] that a group of organizations implement ethical approaches that go beyond legal compliance objectives in order to build trust in complex data analytical processing. As these companies see it, ”the law lags the rapid emergence of advanced analytics and AI and so, to address the risks that their use of these technologies poses, companies need to go beyond legal requirements and into the realm of "ethics."

The Data Environment in Which These Companies Operate

In order to understand the approaches these companies are taking and why they are taking them, it is important to understand the environment in which data organizations are operating today and in which they anticipate operating in the future. There are related trends that explain this environment and contribute to the added complexity and governance accountability required.

First of all, in general, the amount of generated data is expected to grow exponentially due to: (1) the increasing number of internet users doing everything online from business communications to shopping and social networking, and (2) the billions of connected devices and embedded systems that create and share a wealth of Internet of Things data analytics every day all over the world.[10] Specifically, these two factors have been impacted by the current COVID-19 pandemic which has accelerated internet and device use.

[9] https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/3/96132/files/2020/10/Final-Report-1.pdf [hereinafter OSU Report]

[10] Sandra Khvoynitskaya, The future of big data: 5 predictions from experts for 2020-2025, 30/01/2020 [hereinafter Predictions] https://www.itransition.com/blog/the-future-of-big-data

Second, this data, coupled with technologies enabling advanced analytics such as AI use is expanding rapidly within organizations, in both commercial and public sectors. It is used to automate existing processes, augment decision making, and to enhance customer experience with new products and services. PwC's analysis of the AI market has shown just how big a game changer AI is likely to be, potentially contributing $15.7 trillion to the global economy by 2030.[11]

Third, machine learning (ML), a subset of AI, is becoming more sophisticated and has yet to see its full potential – beyond self-driving cars, fraud detection devices or retail trend analyses. Until recently, ML and AI applications have been unavailable to most organizations due to the organizations' lack of skills to configure required open-source platform solutions on their own. Once commercial AI vendors started building affordable connectors to open-source AI and ML platforms and to offer features which open-source platforms lacked, such as ML model management and reuse, ML and to a certain extent AI became even more available. The combination of big data with ML, e.g., natural language processing (NLP) where computers do the analysis by themselves, makes machines more intelligent and capable of reading emotions, driving cars, exploring space and treating patients.[12]

By the end of 2024, 75% of enterprises will shift from piloting to operationalizing AI, driving a 5X increase in streaming data and analytics infrastructure. Within the current pandemic context, AI techniques such as ML, optimization and NLP are providing vital insights and predictions about the spread of the virus and the effectiveness and impact of countermeasures. Other smarter AI techniques such as reinforcement learning and distributed learning are creating more adaptable and flexible systems to handle complex business situations.[13]

Finally, fast data – where data is processed in real-time streams – allows data to be analyzed promptly, e.g., within as little as one millisecond. This capability brings more value to organizations that can make business decisions and take actions immediately when data arrive. As businesses are getting more digitized, which drives better customer experience, individuals expect to access data on the go and expect it to be personalized. Actionable data is the missing link between big data and business value. Big data in itself is worthless without analysis. By processing data with the help of analytical platforms, organizations can make information accurate, standardized, and actionable.[14]

"To innovate their way beyond the post-COVID-19 world, data and analytics leaders require an ever-increasing velocity and scale of analysis in terms of processing and access to succeed in the face of unprecedented market shifts."[15] These systems are complex; from opaque to unpredictable decision making, this complexity carries over into the requirements for organizational governance. It makes it harder for organizations to understand the impact, both expected and unintended, of a given AI application. Unintended consequences can yield risks and potentially harms for both individuals and the organizations using and deploying AI and algorithmic decisions. Some of these unintended

[11] Sizing the Prize: What's the real value of AI for your business and how can you capitalize?, PwC 2017, (accessed 2 Dec 2019) https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

[12] Predictions

[13] Laurence Goasduff, Gartner Top 10 Trends in Data and Analytics for 2020, June 9, 2020 [hereinafter Gartner] https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-in-data-and-analytics-for-2020/

[14] Predictions

[15] Gartner

consequences have been manifested as bias in disparate medical device efficacy for darker skin,[16] in how students are assigned grades on university entrance exams,[17] and in predictive policing.[18]

In this environment, there are two emerging trends favoring increased accountability:

1. A dramatic shift to more complex and complicated technology and data use that holds the promise of significant benefits but is dependent on enhanced accountability and how well stakeholders trust the development and application of these technologies.
2. A growing lack of trust between some regulators and businesses which is driving calls for more demonstrable accountability.

How Companies are Responding to This Environment

The 12 companies who participated in this study have or are evolving their governance approaches based on a "trust" driven business strategy. While they each are doing so in their own way and consistent with their own cultures and strategies, they also are continually investing and changing. They are going beyond legal compliance and instead are implementing practices and processes that are based on a digital trust-based objective. The companies recognize that to be successful in their business strategy in a digital environment, trust will be key, in addition to meeting legal compliance objectives. As a result, they are implementing demonstrable accountability against a broader objective of trust in an arena made more complex with the advent of advanced technology and data use.

As with the companies researched as part of the OSU Report, there are several drivers contributing to the beyond compliance objective that include protecting their reputation, preparing for anticipated law changes (as the law catches up), making better decisions and fulfilling values. In particular, the practices of these leadership companies, coupled with what will be required to enable the advance of trusted technology and trusted data, identify a need to refine the IAF's proposal in 2019 relating to Data Stewardship Accountability Elements in its work, Ethical Accountability Framework for Hong Kong, China.[19][20] Those elements should evolve into the Fair Processing Demonstrable Accountability Elements (discussed below).

In the IAF's view, these new Fair Processing Demonstrable Accountability Elements provide many of the economic benefits the use of advanced analytics that drive technologies like AI can bring to individuals, groups of individuals, society and organizations while meeting the broader needs of individuals, groups of individuals and society for ethical and fair data processing. IAF believes these new Fair Processing

[16] Moran-Thomas, A. 2020. How a Popular Medical Device Encodes Racial Bias. Boston Review

[17] Osborne, C. 2020. When algorithms define kids by postcode: UK exam results chaos reveal too much reliance on data analytics. ZDNet

[18] Ensign, D. et al. 2017. Runaway Feedback Loops in Predictive Policing. Proceedings of Machine Learning Research (FAT*) (2017), 1–12.

[19] https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf

[20] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Hong-Kong-Report-FINAL-for-electronic-distribution-10.22.18.pdf

Demonstrable Accountability Elements advance what the original Essential Elements of Accountability[21] are capable of doing in two key ways:

- First, when implemented, they facilitate the trust necessary to enable the adoption of data driven technologies like AI and its associated data use.
- Second, they demonstrate accountability that goes beyond legal compliance.

The original Essential Elements of Accountability, while key, simply meet compliance objectives regarding existing law. A review of the practices of the leadership companies shows why the IAF's thinking in 2019 has evolved into the Fair Processing Demonstrable Accountability Elements.

Summary and Profile of Study Participants

Key Findings

As noted, these business leaders are going beyond compliance to drive for a broader business objective in numerous ways.

- **Digital trust (not regulatory compliance) is the strategic driver**, and this development is being driven by tone at the top. This approach is driving investments well beyond legal compliance and aligning overall business strategy and (privacy) structures and programs in new ways.
- **Broadening the areas of focus of the Privacy Group** – To drive a business objective that requires trusted technology and trusted data, functions such as data ethics, end to end data governance and, most significantly, AI governance are being added to the group privacy office remit. Collaboration is increased significantly with other key functions such as advanced analytics teams, data governance teams, and operational risk functions, and they also are becoming more intertwined.
- **Review processes (PIA/DPIA/Ethical Data Impact Assessment (EDIA)) are significantly broadening** and are focused now on customer and user impact and trust and organizational reputation. In some organizations, a standard PIA is no longer used. A much broader "impact" assessment has taken its place.
- **Risk based, formalized escalation processes are being established** - Different levels of formalized senior leadership involvement is becoming the norm for the impact reviews of new/revised products and services.
- **Instrumentation and formalization of digital organization wide accountability** - Even in heavily culturally driven organizations, there is a shift to "organizing the culture."

These leadership companies are creating a growing gap between a strategy of digital trust that also achieves compliance than a more purely compliance focused approach by other organizations. **This distinction has the potential to drive competitive differentiation as trust becomes more of a consumer driver in an increasingly digital world**.

[21] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Data-Stewardship-Elements-002-1.pdf

Profile of Companies Studied[22]

Twelve companies were studied; six are in a highly regulated environment, and five operate in a B-to-B market or have limited to no direct contact with individuals. They include a broad sectoral coverage that encompasses Pharma, Technology, Telco and Communications, Advertising, Financial Services/Insurance, and Health Care/Insurance. Most have or are making the pivot to the importance of data to their business strategy.

For all of the leadership companies, the results suggest the strategic shift to trust and going beyond bare legal compliance is not market segment driven. This lack of market specific approach is consistent with the OSU Report findings.

All have a "federated" governance model. In other words, to a lesser or greater extent, a central group drives or creates requirements, and Lines of Business (LOBs) are accountable for meeting the requirements. Some companies have a hybrid operating model in which operational aspects are more centrally run.

Strategy and Structure

The "Strategy" is very clear in these companies. "**Trust" is tied to or is the strategic driver of the company.** Digital responsibility is the primary driver with compliance as the byproduct, albeit a necessary one. By extension, trust (not regulatory compliance) is driving investment. **Ethics or an ethical approach** is embedded or implicit. In one company, it is an explicit business driver. This result is consistent with previous work on ethics which suggests trust is tough to codify and requires translation into/alignment with a business strategy. **An outcome of investment in this area is a programmatic approach to "fairness."** Because strategy is clear, there is no need to modify structure. For example, it remains fitting that the Chief Privacy Officer (CPO) reports to the General Counsel as he/she subsumes the organizational strategy of trust even if it is broader than legal services. Some companies have evolved to have governance operational units report outside of a legal/compliance function, e.g., to the head of Engineering or to the Chief Trust Officer. The net is that the structure revolves around strategy. As part of this trend to trust, some CPOs now have titles that include digital/responsibility/trust/ethics.

Program Direction

The companies all:

1. Have (or are building) a part of their program that goes beyond basic (even mature) GDPR compliance – the path is clearly programmatic compliance or
2. Have evolved (or are evolving) their program and approaches to drive reputation and trust as the principal driver or
3. **Both (more common) – Have trust as the driver, and compliance is a by-product**

Positioning

Tone from the top plays a key role where the senior executives tie a trust objective to digital responsibility and to data and technology and to a strategic purpose. In some cases, trust drives overall organizational culture which is more key than more programmatic approaches.

[22] See Appendix 1

Trust drives Public Positioning

Roughly 40% have some version of public principles on data responsibility that are often Board socialized or approved. This vertical strategic alignment drives internal positioning. These companies enjoy a very close partnership between the Group Privacy Office and the Lines of Business (LOBs); the Group Privacy Office is seen as an enabler of the business strategy with clear senior executive support. One interesting observation was that companies with a strong culture of privacy and trust plus customer first "can" or can be seen to require fewer distinct programmatic elements**.** However, organizing culture becomes more key as complexity of technology and data use increases.

Essential Elements of Accountability Need Updating

The advancements that these companies have made and are in the process of making have confirmed that the Essential Elements of Accountability are key still for organizations in establishing their basic governance programs, but organizations that engage in complex data analytical processing have found it necessary to evolve their accountability programs. This evolution includes making accountability more explicitly and formally demonstrable, i.e., more transparent – through policies, processes and assessments – to stakeholders such as customers, the public, auditors, investors, and regulators.

In January 2019, the IAF recognized that the adoption of the GDPR had elevated accountability from check-box compliance to a risk-based approach but that the GDPR had not kept up with advanced data-processing activities, such as AI and ML, that may impact individuals in a significant manner. In order to be able to transform data into information and information into knowledge and insight and knowledge into competitive advantage, and in order for individuals to be able to trust data processing activities that might not be within their expectations, the IAF concluded enhanced data stewardship accountability elements (Data Stewardship Accountability Elements) were needed.[23] Based upon work done for the Hong Kong Privacy Commissioner for Personal Data, the Data Stewardship Accountability Elements were revised and published as the Enhanced Data Stewardship Accountability Elements for Data Processing Activities such as AI and ML that Directly Impacts People (Enhanced Data Stewardship Accountability Elements).[24] This work was formally submitted to the 2018 International Conference of Data Protection and Privacy Commissioner whose focus was on Digital Ethics.[25] Based upon the learnings from the study of these 12 leadership companies, IAF has modified further the Enhanced Data Stewardship Elements as the Fair Processing Demonstrable Accountability Elements.

Introduction of Fair Processing Demonstrable Accountability Elements

In parallel to this study of demonstrable accountability, the IAF examined the Enhanced Data Stewardship Accountability Elements developed as part of the work done for the Hong Kong Privacy

[23] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Data-Stewardship-Elements-002-1.pdf

[24] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Hong-Kong-Report-FINAL-for-electronic-distribution-10.22.18.pdf

[25] See https://edps.europa.eu/press-publications/press-news/press-releases/2017/2018-international-conference-data-protection-0_en

Commissioner for Personal Data.[26] The examination suggested some modifications were required, including a change in the name to “Fair Processing Demonstrable Accountability Elements.” Key modifications include the change from a single focus on oversight to the addition of the use of escalation paths for decision making. The companies studied have or are on a path to implementing many aspects of the Fair Processing Demonstrable Accountability Elements and by extension are achieving a higher level of demonstrability. In summary, this new version better aligns with the studied organizational practices, creates a better umbrella or foundation (Fair Processing), aligns with the IAF’s Fair Processing Act draft legislation,[27] and is consistent with the Global Privacy Assembly’s Resolution on Accountability in the Development and Use of Artificial Intelligence adopted October 2020.[28]

Fair Processing Demonstrable Accountability Elements
Organisational commitment to fair processing demonstrable accountability and the adoption of internal policies consistent with external criteria and established fair processing principles. As a matter of commitment, organisations should define fair processing values and/or principles which then are translated into organisational policies and processes for fair data processing. a. These principles should be organizationally derived and are in addition to laws or regulations. They may go beyond what the law requires but should be aligned, and not be inconsistent, with existing laws, regulations, or formal codes of conduct[29]. b. Organisational policies and processes derived from these principles should be anchored to clearly defined, accountable individuals within the organisation and should be overseen by designated senior executives. c. The organisation’s fair processing guiding[30] principles should be easily understood by all staff, and in particular by technical staff, and should be capable of being programmed into activity objectives.
Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education. Organisations should use a risk based “ fair processing by design” process to translate their fair processing principles and other policy requirements into their data-analytics and data-use system design [31] processes so that society, groups of individuals, or individuals themselves, and not just the organisations, gain value from the data processing activities, such as AI or ML.

[26] Original Data Stewardship Elements can be found here

[27] https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/FairOpenUseAct.9.23.19.FINAL-V2-1.pdf

[28] https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN-1.pdf

[29] Examples of existing professional or industry codes of conduct are those that relate to AI or ML. These Elements should work with those codes and not replace them.

[30] See IAF Blog: The Need for an Ethical Framework https://informationaccountability.org/2017/01/iag-blog-ethical-principles-and-framework/

[31] Big data analytics, advanced analytics, ML and AI all refer to analytic operations that take advantage of the massive data sets and processing capabilities that have become available in the past decade or so and that use them to find correlations and make and use predictions

a. Organisations should establish a programmatic risk management approach to identify, assess, mitigate and monitor processing benefits and detriments on an ongoing basis.
b. At a minimum, "processing risk" should assess the level of "adverse processing impact" potentially created by processing that includes 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.
c. Processing risk should assess the benefits and/or missed outcomes that may or may not occur.[32]
d. All staff involved in data impacting processing should receive training so that they may competently participate in a "fair processing by design" process.
e. Where appropriate, organisations should follow codes of conduct that standardize processes to industry norms.
f. Fair Processing Impact Assessments (FPIAs)[33] should be required when advanced-data analytics may impact people in a significant manner and/or when data-enabled decisions are being made without the intervention of people. FPIAs should include a risk-based approach to assess the likelihood and significance of benefits and adverse impacts
    1. Where an analytical data driven use has potential impact at the individual level, or at a higher level, such as groups of individuals and society, the benefits and adverse impacts should be explicitly defined and balanced. The adverse impacts should be necessary and proportional to the benefits and should be mitigated to the extent possible.
    2. Adverse impacts and benefits should be assessed using the established programmatic risk management approach.
    3. Where data processes begin with analytic insights, those insights (and the underlying data) should be tested for accuracy, predictability, bias and fairness and consistency with organisational values.
    4. The systems, technology and the data that feed those systems should be assessed for appropriateness based on the decision the data are being used for and should be protected proportional to the risks. This assessment should be ongoing.
    5. Instrumentation and/or tooling should be developed and implemented to help enable the outcomes of a FPIA and to support the development of products and services that meet the organisation's Fair Processing principles and other policy requirements.

Internal review processes that assess higher risk FPIAs[34] and the overall fair processing program.

a. Higher risk or higher impacting data initiatives, or where the adverse impacts have not been sufficiently addressed, should be referred to more senior organisational decision-making group(s) for their review and approval.
b. The escalation process should be based on and be part of the programmatic risk management approach and should address that issues raised as part of the FPIA have been resolved and that the advanced data processing activities have been conducted as planned.

[32] The IAF believes that a risk assessment should include both benefits and adverse impacts.

[33] See here for A Model EDIA. (FPIA). This assessment can be added to or incorporated into an organization's existing assessment process.

[34] What is "higher risk" is scenario and impact driven. See Assessment Choice for Ethical Data Stewardship as one example of determining risk levels

c. Where internal reviewers need external expertise, that expertise should be sought.
d. The full organisational fair processing system should be assessed for its effectiveness and whether the controls are effectively established and are meeting the organisation's risk objectives.
e. The review of the fair processing process should be separate and independent from the parts of the organisation implementing and governing the fair processing process.

Individual and organisational demonstrability and mechanisms for individual participation.

The fair processing principles that govern the advanced data-processing activities, and that underpin decisions, should be communicated widely; processes should be proactively transparent and explainable wherever possible. Furthermore, societal and individual concerns should be addressed and documented as part of the FPIA process, and accountability feedback mechanisms should be established.

a. Organisations should be open about their fair processing principles, making them publicly accessible.
b. Organisations should be able to explain how data are used, how the use may benefit and potentially pose detrimental impact to society, groups of individuals, or individuals themselves whose data are associated with the processing, and how society, groups of individuals and individuals themselves may participate and object. This explanation should allow individuals to understand the nature and elements of the decision to which they are being subject or the rules that define the processing and the decision's principal characteristics.
c. Some form of meaningful explanation always should be possible without compromising intellectual property
d. Organisations should make public on at least an annual basis the types of advanced analytics activities the organisation engages in, how data are used to achieve each beneficial purpose and a summary of the decision process relative to these data activities. This disclosure should include the types of third parties to which personal data may be transferred as part of these data activities.
e. Organisations should document and disclose descriptions of the fair processing governance processes they employ (e.g., policies and procedures) and make public program elements
f. Organisations should be open and provide a clear explanation about how analytical data use and advanced data processing activities, such as AI or ML systems, have been developed. Individual and societal concerns should be part of the data system evaluation.
g. Individual accountability systems that provide appropriate opportunities for feedback, relevant explanations, and appeal options for impacted individuals should be designed and be effective, and effectiveness should be tested.
h. Specific mechanisms should provide individuals with the ability to challenge the outcome of automated processing.

Means for remediation and external enforcement.

Organisations should stand ready to demonstrate the soundness of internal processes to the regulatory agencies that have authority over them, including certifying bodies to which they are subject, advanced data-processing activities, such as AI or ML processes, as well as when data processing does or may impact people in a significant manner.

a. Organisations should stand ready to demonstrate the soundness of the policies and processes they use and how data and data-use systems are consistent with their fair processing principles. Organisations must maintain and document an accountable processing management program, taking into account the entity's size and complexity, activities, and legal requirements. The program should be designed to:
    1. Achieve compliance with the applicable legal or regulatory requirements, industry best practices, and organisational policies;
    2. Promote effective management and oversight of processing;
    3. Manage risk, including processing risk, on an ongoing basis;
    4. Evaluate both adverse and beneficial impacts of processing; and
    5. Demonstrate the entity's ongoing commitment to fair processing.

Detailed Key Findings

Trust is driving a range of demonstrable accountability type investments. The drivers are a digital strategy and a recognition that regulatory compliance is simply one objective; other drivers are more tied to the business strategy and to reputation. Ethics or ethical approaches are an implicit driver/goal. Trust based goals and principles are incorporated into company policy and procedural requirements resulting in alignment with ethics-based codes of conduct and a compliance program aligned with evolved corporate policy not just legal requirements. While "trust" is the business objective, an outcome of these leading organizational practices is a demonstrable programmatic approach to "fairness."

One way to examine in detail the practices of the companies studied is to organize the key findings around the Fair Processing Demonstrable Accountability Elements. For emphasis, this report covers representative "key findings" and is not intended to be a reflection of what each company is doing in each section of the principles nor to infer every aspect of these elements as drafted has been adopted by each company. Further, as the focus of this report is on demonstrable accountability, the methods these companies have developed with respect to individual participation were not captured or highlighted.

1. **Organisational commitment to fair processing data stewardship accountability and the adoption of internal policies consistent with external criteria and established fair processing principles.**

    Trust drivers/positioning are being translated into corporate policy and operating procedures and therefore fit with "compliance." However, in these companies, compliance is to broader company policy not just legal requirements. These trust-related requirements frequently accompany a public positioning (e.g. TELUS, Mastercard, Facebook and Apple.) Like Apple, Cisco posits privacy as core to human rights. These principles are often built around Data for Good, digital responsibility, etc. Positioning trust this way means business drivers other than compliance exist, resulting in **less friction to implement** and a demand from business units who want centrally driven solutions. These trust drivers also are being incorporated into "ethical codes of conduct" resulting in a "this is the way we function" mindset. For example, at Sun Life, this approach creates alignment with their Code of Conduct, further reinforced by operationalization of new client data principles.

2. **Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education.**

   There is a trend for some aspects of privacy operations to be centrally run. This centrality can be specific functions (e.g., access and breach management) to PIA facilitation and decision making to building expanded second line of defense compliance functions to a full set of privacy operations run centrally. **AI governance** is the next wave of elements to be incorporated into group privacy functions. This centrality will involve incorporating separate algorithmic assessment processes and model evaluation and testing criteria programs.

   Review processes such as PIAs or DPIAs are being expanded to include a broader set of elements. AI, ethics, algorithmic model evaluation, end-to-end data analysis, all types of data, fairness, proportionality are an outcome. The evaluations are aligned with the company's strategy and digital trust objectives and are becoming more like an Ethical Data Impact Assessment (EDIA) first introduced as part of the Hong Kong project.[35] For example, assessments are pivoting to explicitly involve impact to the customer from a trust perspective and impact to the company's reputation and trust drivers. Sun Life is including considerations for unintended bias, unjustified discrimination and fair treatment of clients in their evolving PIA process.

   Programmatic tooling is key. Many of the companies are significantly investing in and/or modifying technology enabled governance tools to help automate their goals. They are developing complimentary controls across different programs as support for this approach. For some, the combination of trust driven requirements and other elements like AI are resulting in "naming" tensions. For example, some companies no longer call a PIA a privacy impact assessment.

   Instrumenting of accountability - another area of development. Assessment tools and data tooling (e.g., extending decision outcomes in engineering how data is handled) are being substantially re-tooled. Assessment tools and privacy control frameworks are being instrumented to provide data driven decisions, compliance investment decisions and program enhancements (IPG, AT&T, Facebook, Google and Sun Life). Second lines of defense are being enhanced to measure compliance capacity and capabilities. **Formalization of risk** is being implemented into reviews from data elements to the degree of risk and who can review/approve.

   Core data management and governance is becoming part of assessments and structure. TELUS has formally aligned core data governance to the group privacy office. At Acxiom, a full understanding and assessment of the underlying data is a core part of their assessment process. Most companies are extending governance beyond just personal data.

[35] See https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf

3. **Internal review processes that assess higher risk use fair processing impact assessments (FPIAs) and the overall fair processing program.**

   Decision escalation processes are well defined and consist of multiple layers of senior review processes. At, for example, Acxiom, Facebook, Google, Mastercard, and Highmark, very centralized data use governance processes result in all data intensive initiatives being centrally reviewed and approved.

   More formalization of accountability. Some companies such as Merck and Sun Life have established formal accountability agreements with LOB leaders or data sharing arrangements that outline accountability requirements. Internal Audit (IA) is a more formal part of accountability validation. At Merck and TELUS, accountability is measured, and IA is supported through required surveys. Accountability is reported on, score carded and is part of the review by senior leadership. At Facebook, individual business units are required to certify business unit compliance with privacy program requirements.

4. **Individual and organizational transparency and mechanisms for individual participation.** As noted above, individual participation was not part of this project. However, as a translation of Data Transparency and Trust, Cisco has privacy data sheets and maps for its more personal information rich products that are publicly available.[36]

Implications to Demonstrable Accountability and Recommendations

An interesting finding from this study is that trust, rather than legal compliance, is driving a whole range of Demonstrable Accountability type investments. Ethics or ethical approaches are an implicit driver/goal. While “trust” is the business objective, an outcome of these leading organizational practices is a **demonstrable programmatic approach to “fairness.”** This result was one reason why the IAF concluded pivoting the revised accountability elements around “demonstrable fair processing” made sense.

In the IAF’s report prepared for Innovation, Science and Economic Development Canada, in addressing “A Path to Trustworthy People Beneficial Data Activities,”[37] it was suggested that organizations should: “Be Transparent: Demonstrate transparency to the public, to employees and to the government. There are different audiences, and organizations should make sure they are reaching the right audience with the right communication method. For example, on the organization’s websites, organizations may disclose:

- The types of People Beneficial Data Activities the organization engages in, how data are used to achieve each people beneficial purpose and the types of third parties to which personal data may be transferred in order to achieve each people beneficial purpose;
- Descriptions of the governance processes it employs (e.g., policies and procedures) regarding People Beneficial Data Activities;

[36] See Privacy Data Sheets: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet and Privacy Data Maps: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Map

[37] https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/A-Path-to-Trustworthy-People-Beneficial-Data-Activities.pdf

- A description of the PBIA [People Beneficial Impact Assessment] process, including identification of benefits to people, its conclusion why the organization's interests are people beneficial, identification of processing risks and appropriate ways to reduce risk, analysis of residual risks, identification of risks from forbearing activity, and explanation of why the factors that support processing are not outweighed or counterbalanced by residual risks (this is meant to be a summary of the PBIA process and is not meant to include a summary PBIA for each People Beneficial Activity) . . . ."

The companies studied each had demonstrably more investments (people, process and technology) in their privacy programs than organizations that are approaching their programs more from a legal compliance objective. They could extend these investments to, for example, provide more public transparency as to their overall governance processes, the decision-making process, types of data activities and even a summary of some of their decisions. What is clear from this study is that all of these companies are continuously investing and improving on their approaches, suggesting that demonstrable trust requires more fluidity and demonstrable compliance.

Verifiable Trust is an Extension of Demonstrable Accountability

Building programs that reflect compliance with data protection law is necessary but not sufficient for organizations to drive sustainable data driven competitive advantage and trust. In the lead up to the 2018 International Conference of Data Protection and Privacy Commissioner hosted by the European Data Protection Supervisor, Giovanni Buttarelli boldly asserted that compliance with the law was not sufficient to assure data serves people. The IAF's work on Artificial Intelligence, Ethics and Enhanced Data Stewardship in 2017 suggested "there is a growing sense that even the newest data protection laws, such as the GDPR, are lagging the fast evolving and compelling technologies and a sense that the ethics that go beyond the explicit words captured in law may guide data [and technology] governance in an actionable manner." Today, when technology and advanced analytics are resulting in data processing being both compelling and scary and laws that are increasingly complex and convoluted, organizations are unsure what "ethics that go beyond the law" even means.

There are literally hundreds of research papers written by academics, NGO's, professional associations and government created models pursuing this question of AI and data-centric ethics within several disciplines, such as engineering and computer science. It is now widely accepted that for the tremendous opportunities AI/ML advancements can offer, these benefits will not be fully realized absent trust - trust in the technology, trust in the data that drives the technology and trust in the impact of the technology and data use.

Yet, trust is a loaded word in data protection. In the early laissez-faire era that followed the development of the consumer Internet, "trust" was a word that meant "leave me alone because I have good intent." The perceived abuses of that era led to a general consensus that trust needs to be linked to something more substantial. This view led to the Global Accountability Dialog, Canadian and Hong Kong guidance on accountability, and accountability as a component of the GDPR. However, this need for verified trust thus far has not linked business strategy, processes, and data governance. Most important, why, from a business strategy perspective, would an organization want to implement more trust based ethical governance as well as the law, since ethics is not required by the law, has not been considered. These leadership companies have found and created this linkage.

Conclusion

The bottom-line is that an accelerating trust gap between some regulators and general business practices exists at a time where "trust" is key to enable the advances AI/ML technology and associated data use can bring both to individuals and society. Leadership companies are approaching trust as a business-critical goal. They want to make sure that their technology, processes and people are working in concert to maintain the high levels of trust expected by their many stakeholders.

In order to achieve this goal, these companies have several commonalities: there is organizational commitment, broad impact assessments are used, and there are risk-based formalized decision-making processes with escalation paths defined. In short, they are implementing trust driven, beyond legal compliance, demonstrable accountability processes. Many of these same commonalities are evidenced in the OSU Report.

These companies continually are improving on these processes and could take advantage of the recommendations that came out of the IAF's People Beneficial Data Activities work to increase transparency in a demonstrable manner. By contrast, many organizations, seemingly encouraged by regulators, are focused on procedural risk elements associated with legal compliance accountability. While meeting compliance-based requirements, these leadership companies have shifted the focus to fair processing. They are concentrating on trust-based accountability built around ethical approaches. While all the leadership companies have strategies that are driven from the top, are associated with more data driven corporate strategies, and target trust, their implementation processes are very different; perhaps these differences are a byproduct of continually improving on these processes. Regulators could look more to these leadership companies as examples of demonstrable accountability.

Recognizing the commonalities at these leadership companies, IAF realized it was necessary to modify its Enhanced Data Stewardship Accountability Elements into Fair Processing Demonstrable Accountability Elements. Implementation of the Fair Processing Demonstrable Accountability Elements can help organizations forge a trust relationship with their stakeholders. While the investments these leadership companies are making align with many aspects of the Fair Processing Demonstrable Accountability Elements, the trust gap could be further closed by more transparency as to the governance processes they employ, including types of data activities they are engaged in and the decision-making processes they use to achieve a level of fair processing.

Organizations who create products and services and make decisions based upon a demonstrable accountability foundation to build trust can earn the ability to use advanced analytical data processing and AI to their full potential. This is why demonstrable accountability matters.

Appendix 1

Contributing Participants - The following companies were among the participants in the IAF's project.

Merck
AT & T
Cisco
Apple
Facebook
Google
MasterCard
TELUS
Sun Life
Acxiom
IPG
Highmark
PwC