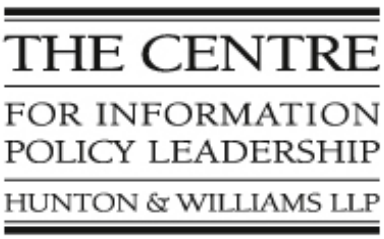
Accountability:

Data Governance for the Evolving Digital Marketplace[1]



[1] For the past three years, the Centre for Information Policy Leadership at Hunton & Williams LLP has served as secretariat for the Accountability Project. The Accountability Project is the work of an international group of experts that includes representatives of privacy enforcement agencies from Europe, North America, and the Asia-Pacific region; civil society; academia and business. Its mission is to consider how an accountability-based system of data protection might be designed. The inquiry originally focused on cross-border data transfers, but expanded to address how to apply accountability to improve compliance with privacy requirements and to enable more flexible information management. This paper reflects the discussions and findings of the Accountability Project, and is intended solely to serve as a report of the work of that initiative.

Introduction

Innovations in technology; more ubiquitous data collection, analysis and processing; the global flow and processing of data; and powerful analytics all have made an unprecedented array of beneficial products, resources and services available to individuals. In this data environment, organisations must employ effective and explicit data governance programs to protect individuals against the risks that these uses of information may raise. While individuals must continue to play an appropriate role in making choices about sharing their data, they cannot be held responsible for detailed decisions about vastly complex technologies and data uses. Thus, new models for data governance shift more responsibility for appropriate data controls to the organisations that derive and create value from data, and require those organisations to protect information in a manner more transparent to individuals and regulators. At the same time, organisations need to be able to process and analyze data in creative, innovative ways that enable them to respond quickly to the requirements of their customers and the marketplace. In exchange for increased corporate responsibility, accountability allows for more flexible use of data.

Over the last 18 months, policymakers around the globe have begun efforts to review and, where needed, update privacy protections to meet the demands of this new data environment. The accountability principle has been proposed as a means to more appropriately re-allocate the primary burden and responsibility for dealing with this enhanced complexity from individuals to organisations, requiring them to implement programs that put into effect the full complement of data protection principles, and to stand ready to demonstrate the effectiveness of those programs to data protection authorities. During this same period, policymakers have initiated reviews of a number of the foundational documents of data protection, paying particular attention to the role of accountability and to developing more effective regulatory outcomes.

The accountability principle is not new. It has been a feature of both the earliest of the major international instruments on privacy, the Organisation for Economic Cooperation and Development's Privacy Guidelines,[2] published in 1980, and the most recent, the Asia Pacific Economic Cooperation's Privacy Framework,[3] endorsed in 2005. Both require that organisations "should be accountable for complying with measures that give effect" to the fair information practices articulated in the respective guidelines.

New approaches to privacy protection currently under consideration rely significantly on accountability as a means to ensure protection of data. "The Future of Privacy," the joint paper of the European Union Article 29 Data Protection Working Party (Article 29 WP) and the Working Party on Police and Justice (WPPJ), notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalization and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability." In a later Opinion on accountability[4] submitted to advise the European Commission on how to amend the Data

---

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited 15 March 2011).

[3] APEC Privacy Framework, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf (last visited 29 July 2010).

[4] Article 29 WP "Opinion 3/2010 on the principle of accountability" (adopted 13 July 2010, 00062/10/EN, WP173), http://ec.europe.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, (last visited 7 April 2011).

Protection Directive, the Article 29 WP defined a statutory accountability principle to "explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request."

Accountability has traditionally formed the basis of privacy processes in the European Union (EU).[5] However, these processes can also impose significant bureaucratic burdens that do not further privacy protections. The current reconsideration of core data protection documents provides a critical opportunity to implement accountability in a way that minimizes bureaucratic obligations, enhances protections, and allows organisations flexibility in data use and protection.

Accountability requires that companies implement programs that foster compliance with data protection principles, and be able to describe how those programs provide the required protections for individuals. Requiring companies to implement such programs fosters an organized, coherent approach to compliance with data protection requirements. Accountability does not take rights away from consumers, but rests firmly on a foundation of principles of fair information practices. Moreover, it suggests a model where consumers and organisations share responsibility for protecting information by implementing transparent data protection programs and processes.

Faced with rapid advances in data analytics and increasingly complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions, even when they access privacy policies. In an accountability model, when the consumer can provide meaningful consent, the organisation is required to act based on that consent. But even when choice is not available or appropriate, accountability demands responsible, disciplined data storage, use and protection. Thus, an effective accountability framework relieves the individual of much of the burden of policing the marketplace against bad actors and places greater responsibility to safeguard data on organisations that collect and use data. Accountability encompasses a global dimension as well – it requires that organisations remain responsible and answerable for the protection and management of data, no matter where or by whom it is processed.

Accountability and the robust data governance practices upon which such an approach relies also benefit companies by allowing them greater flexibility to adapt their data practices to serve emerging business models and technologies and to meet consumer demand. An accountability-based approach focuses on setting privacy-protection goals for organisations based on criteria established in current public policy, and allowing organisations discretion to determine how those goals are met. Accountable organisations must be able to adopt methods and practices to reach those goals in a manner that best serves their business models and structures, technologies, and the demands of their customers. In exchange, it requires that the organisation commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure that those policies are carried out in a way that protects information and the individuals to which it pertains.

Drawing on materials developed by the Accountability Project, as well as discussions held this year in Madrid,[6] this paper provides an overview of accountability as an approach to data governance. It

[5] Paragraph 19 of the Article 29 WP "Opinion 3/2010 on the principle of accountability " (adopted on 13 July 2010, 00062/10/EN, WP 173) cites Binding Corporate Rules used in the context of international data transfers as reflecting the accountability principle.

[6] "Data Protection Accountability: The Essential Elements - A Document for Discussion," October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountaiblity_Paper.pdf (last visited 15 March 2011); "Demonstrating and Measuring Accountability: A Discussion Document," October 2010, http://www.huntonfiles.com/files/webupload/CIPL_Paris_Accountability_Paper.pdf (last visited 15 March 2011). The Accountability Project continues this year at meetings convening in Madrid.

describes a model that requires organisations to adopt internal information policies based on recognized external criteria, and implement programs and procedures that ensure those policies are adhered to. The approach further calls upon organisations to assess and mitigate the risks to individuals raised by data use, and engage in review to determine whether their internal practices result in sound decisions about data. Finally, accountability necessitates that organisations remain answerable for the decisions they make about data, and stand ready to demonstrate their accountability to the appropriate third party.

Essential Elements of Accountability

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognized outside criteria, and puts in place performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist for an organisation to establish, demonstrate and test its accountability. An organisation's accountability is measured against these essential elements:

1. *Organisation commitment to accountability and adoption of internal policies consistent with external criteria*

The accountable organisation demonstrates its willingness and ability to be responsible and answerable for its data practices. Its practices are based on policies consistent with appropriate external criteria – applicable law, generally accepted principles, and/or industry best practices. Practices are designed to provide the individual with effective privacy protections.

2. *Mechanisms to put privacy policies into effect, including tools, training and education*

The accountable organisation deploys and monitors mechanisms and internal programs that ensure its privacy policies are carried out. Mechanisms may include tools to facilitate decision-making about data use and protection, training about how to use those tools and processes to ensure employee compliance.

3. *Systems for internal, ongoing oversight and assurance reviews and external verification*

The accountable organisation monitors and assesses whether its internal policies manage, protect and secure data effectively. Risk analysis appropriate to the organisation and the industry in which it functions is crucial to successful monitoring and risk management. The accountable organisation engages, as appropriate, an independent entity to verify and demonstrate that it meets the requirements of accountability.

4. *Transparency and mechanisms for individual participation*

Accountability requires transparency. The accountable organisation effectively communicates to individuals critical information about its data procedures and protections in a posted privacy notice. When appropriate, the information in the privacy notice can provide the basis for the consumer's consent or choice. Individuals should be able to see the data or a description of the types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. In some cases, however, public policy will limit that disclosure.

5. *Means of remediation and external enforcement*

The accountable organisation establishes a means to address harm to individuals caused by the failure of internal practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. The organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process to review and address complaints.

Programs and processes implementing the essential elements should be designed to be proportional to the size of the organisation and the extent and nature of the organisation's collection and use of information. Very small organisations that collect and use limited amounts of non-sensitive information could implement very simple data protection programs and in most cases should not be the focus of data protection authorities. Small, innovative organisations that heavily depend on personal data should have data protection programs that correspond to the data-rich nature of their enterprise and evolve as the organisation and its information holdings grow.

Demonstrating Accountability

Accountability requires that an organisation stand ready to demonstrate its program if asked to do so by a data protection agency. The Accountability Project identified nine common fundamentals that an accountable organisation should be prepared to implement and demonstrate to a regulator. While these nine fundamentals are designed to provide guidance, accountability is not a "one-size-fits-all" approach. Organisations will need to determine, consistent with recognized external criteria, which of these nine they will implement, or whether it may be necessary to apply others.[7] The fundamentals should be applied flexibly and in a way that is appropriate to the organisation's business model, data holdings, technologies and applications, and the risks to privacy they raise for individuals. The design of such programs should reflect and be proportional to the size and complexity of the organisation's data holding and business models**.**

1. Policies. *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards*

An organisation should develop, implement and communicate to individuals data privacy policies that are informed by appropriate external criteria found in law, regulation or industry best practices, and are designed to provide the individual with effective privacy protections. The organisation should also design and deploy procedures to put those policies into effect in light of the specific circumstances of its own organisations (e.g., what is collected; how it is used; and how systems and organisations are connected).

2. Executive oversight. *Internal executive oversight and responsibility for data privacy and protection*

Executive oversight should require the creation of a data privacy leader (or leadership team) who is supported by appropriate resources and personnel, and is responsible for reporting to organisation leadership. Commitment by senior management should include appropriate

[7] The Article 29 Data Protection Working Party's "Opinion on the principle of accountability" (Adopted on 13 July 2010, 00062/10/EN, WP 173) takes a similar approach, stating "[T]here is no option but 'custom built' solutions. Indeed, the specific measures to be applied must be determined depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and types of data. A 'one-size-fits-all' approach would only force data controllers in to structures that are unfitting and ultimately fail."

reporting and oversight of the organisation's privacy program. Top management should empower and require senior-level executives to develop and implement the organisation's programs, policies and practices. Small and medium-sized organisations will need to allocate oversight resources appropriately, keeping in mind the extent and sensitivity of their data holdings and the nature of the use of the data.

3. Staffing and delegation. *Allocation of resources to ensure that the organisation's privacy program is appropriately staffed by adequately trained personnel*

While recognizing the need to work within economic and resource constraints, accountable organisations should have in place sufficient staff to promote the success of their privacy program. Such staff should receive adequate training both as they assume their role in the privacy program and as that program evolves to address new developments in the organisation's business model, data collection practices, technologies, and offerings to consumers. Delegation of authority and responsibility for data protection to appropriate units or parts of the organisation have been found to be effective in many accountable organisations. As in the case of oversight, staffing and delegation decisions in small and medium-sized organisations should reflect the particular circumstances of the organisation and its activities, and the nature, size and sensitivity of its data holdings.

4. Education and awareness. *Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations*

Organisations should provide the necessary briefings, information and education for their personnel to keep them apprised of current and emerging requirements. Such education should raise employees' awareness of new data protection issues that may affect the performance of their job, and make them sensitive to the importance of data privacy to individuals and to the success and reputation of the organisation.

5. Ongoing risk assessment and mitigation. *Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks*

To be accountable, organisations must assess the risks to privacy raised by their products and practices as they are developed and implemented, as they evolve, and as their data requirements change. In response to the findings of those assessments, organisations must take measures to mitigate risk. Risk assessment is not static, but an ongoing function that responds to the dynamic, evolving nature of data collection, use and processing.

To be accountable for its risk assessment and mitigation practices, organisations also should be able to demonstrate the nature of their risk analysis. The organisation must show the rigor of the criteria against which analyses are carried out, and the suitability of those criteria to the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are made and the steps taken to mitigate risk. The organisation also must demonstrate that the decisions it takes to respond to identified risks are appropriate and effective. Privacy impact assessments are one important risk assessment and mitigation tool.

6. Program risk assessment oversight and validation. *Periodic review of the totality of the accountability program to determine whether modification is necessary*

An accountable organisation should periodically review its privacy and data protection accountability program to ensure that it continues to meet the needs of the organisation by supporting sound decisions about data management and protection that promote successful privacy outcomes.

7. Event management and complaint handling. *Procedures for responding to inquiries, complaints and data protection breaches*

An accountable organisation should implement a well-designed, reliable procedure for addressing data protection problems when they arise. Such procedures would need to effectively address data protection problems, such as data misuse, misappropriation or breach. They would also need to include procedures that ensure that the rights of individuals related to their data are respected, and that address their complaints and concerns regarding data protection practices, and potential or actual failures.

8. Internal enforcement. *Internal enforcement of the organisation's policies and discipline for non-compliance*

Accountable organisations should have policies and procedures in place for enforcement of internal data protection rules. Personnel who disregard those rules or misappropriate or misuse data would be subject to sanctions.

9. Redress. *The method by which an organisation provides remedies for those whose privacy has been put at risk*

Accountable organisations should establish redress mechanisms whereby individuals may have their complaints heard and resolved. The mechanism should be appropriate to the character of the organisation, the nature of the data holdings, the way the data is used, and the specific issue raised. It should be readily and easily accessible by the individual, and address complaints efficiently and effectively. Industry groups may offer options for individual organisations seeking to implement a redress mechanism. Because the specific attributes of an appropriate redress tool may vary from culture to culture and from industry to industry, decisions about redress will likely be local. Guidance about redress would optimally be developed in consultation with experts, regulators, civil society, and representatives of public- and private-sector organisations.

General and Validated Accountability

Accountability was articulated as a principle of fair information practices in the OECD Guidelines in 1980 and is implicit in the EU Data Protection Directive.[8] For an accountability approach to data governance to be effective, a general requirement of accountability would be explicitly applied across the marketplace. General accountability would mean that all organisations would implement privacy programs proportional to the size and complexity of their data holdings and business models.

In certain cases, organisations may choose to be recognized and validated as accountable. Validation may be needed when organisations wish to engage in certain activities, or be relieved of certain administrative requirements. They may want, for example, to transfer data across borders for processing. They may need enhanced flexibility to explore new, innovative data uses that raise risks. In such instances, organisations would likely be required to seek *ex ante* recognition of its processes and demonstrate its accountability.[9] Future discussions will explore the appropriate nature of *ex-ante* review required, and how accountability might rely more on *ex-post* review.

[8] Paragraph 26 of the Article 29 WP "Opinion 3/2010 on the principle of accountability," (adopted on 13 July 2010, 00062/10/EN, WP 173) refers to accountability as being in accordance with provisions of the current legislative framework, specifically Articles 6 and 17.1 of the Directive.

[9] Binding Corporate Rules provide an example of *ex-ante* review.

Measuring Accountability

When an organisation wishes to proactively demonstrate its accountability to qualify it to engage in certain activities, make certain assertions, or be relieved of certain regulatory requirements, more formal review and measurement by a supervisory authority or a third-party accountability agent recognized by the supervisory authority may be required. In such cases, supervisory authorities or third-party accountability agents will be responsible for evaluating and measuring the capacity of an organisation's program to assure compliance with applicable regulations and its privacy promises. The regulator or third-party authority will review the organisation's policies, its means for putting those policies into effect, and its assurance processes.[10]

An accountable organisation is prepared to provide evidence of the programs it has implemented to ensure that privacy/data protection principles are put into effect. The evidence may be reviewed at the request of the supervisory authority or as part of a review by a recognized third-party accountability agent. Depending on legal requirements, supervisory authorities may be able to request such evidence proactively or in the course of an evaluation or investigation. Consistent with applicable legal frameworks, supervisory authorities may also recognize third-party accountability agent such as a seal program to undertake this role.

Benefits of Accountability

General Accountability

When organisations are held to a general requirement of accountability, various benefits are likely to accrue to individuals, the marketplace, and the organisations themselves.[11] General accountability is expected to:

- For organisations, reallocate privacy protection resources from compliance with *ex-ante* processes such as data registration and notification of minor changes in processing to risk analysis and mitigation;
- For data protection and privacy authorities, shift resources from administration of general bureaucratic requirements to oversight of those organisations that create the greatest privacy risks for individuals;
- Lead to higher levels of compliance by explicitly requiring organisations to have programs that put data protection principles into effect and to stand ready to demonstrate that compliance;
- Enhance data protection efficiency by giving regulators a more transparent view of companies that stand ready to demonstrate their accountability, allowing them to focus their oversight and enforcement on those activities that create the most risks for individuals;

[10] Self-certification may also serve as a mechanism for *ex-ante* review. Such an approach is currently under consideration in Accountability Project discussions in Madrid.

[11] The stated goal of the review of the Directive is to explore ways to streamline administrative procedures associated with compliance and to enhance the effectiveness of data governance. Accountability offers mechanisms that could further those goals.

- Help organisations improve the quality of data protection by allowing them to use tools that best respond to specific risks, and to rapidly update those tools to quickly meet the requirements of new business models and emerging technologies;
- Enable organisations to better deploy processes that strengthen privacy protection;
- Enable regulators to police marketplace participants whose activities fall outside the bounds of law, regulation and recognized guidance, by enabling them to invest limited resources toward organisations that have not established their accountability or that fail to comply;
- Heighten the confidence of individuals that their data will be protected wherever it is stored or processed; and
- Bridge data protection regimes across jurisdictions, but allow countries to pursue common data protection objectives through different but equally reliable means.

Validated Accountability

Organisations that seek accountability validation for their data protection programs may do so to attain specific benefits. The Accountability Project continues to explore when validated accountability might be required of companies to allow them greater latitude in their data activity. Among the possible benefits that could be made available to companies that validate their programs are:

- Enhanced flexibility to use data in innovative ways.
- Recognized qualification to engage in cross-border data transfer and data teaming.
- Relief from specified administrative requirements.
- Recognized Binding Corporate Rule status.
- Mitigation of enforcement sanctions when appropriate.

Conclusion

As policymakers update data protections to meet the challenges of the rapidly evolving digital marketplace, accountability offers important opportunities and benefits. Properly implemented, it can provide solutions to the issues raised by emerging technologies, analytics and business models. It shifts much of the burden of policing against bad actors and irresponsible data use from individuals to the organisations that derive value from data. It reallocates resources from burdensome administrative processes to activities that identify and mitigate risks to individuals that potentially are raised by 21st century data applications. In doing so, it holds the potential to improve data protection in the emerging data environment.