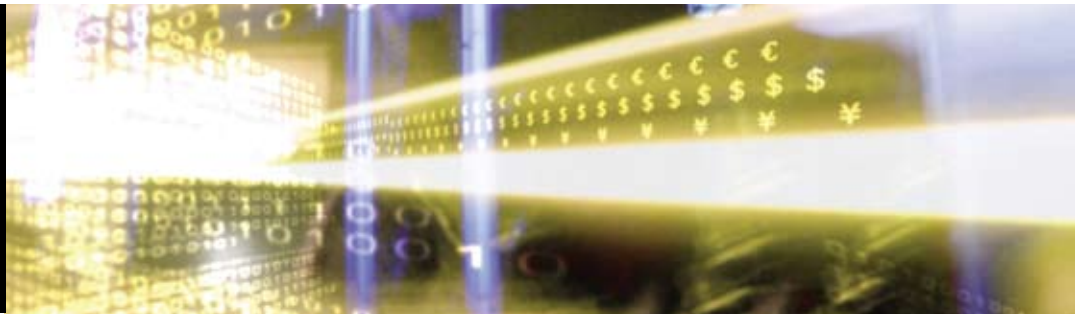
THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



Demonstrating and Measuring Accountability
A Discussion Document

Accountability Phase II – The Paris Project

October 2010

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Paris Project

Preface

Martin E. Abrams
Centre for Information Policy Leadership

When the participants in the Accountability Project released its discussion paper on accountability's essential elements in October 2009, they did so recognizing that within the framework described in that document, it would be necessary to address questions about the its real-world implementation The Centre for Information Policy Leadership at Hunton & Williams LLP was pleased to facilitate further work on accountability, assembling experts to consider practical questions: How do organisations demonstrate their accountability? How do regulators measure it?

This document proposes fundamental conditions that accountable organizations should be prepared to implement and demonstrate to regulators. It further considers how and under what circumstances organisations would measure accountability. Participants recognized that accountability could not be a one-size-fits-all approach. For accountability to work, both organisations and regulators must be able to implement and measure fundamentals in a way that is appropriate for the organization, its business model, and the way that it collects, uses and stores data. When accountability is demonstrated and measured may depend in some cases upon the risks to individuals an organisation's activities raise.

In discussions and in the writing of this paper, participants recognized an increased focus on accountability in national and international discussions about improved data governance. Since October 2009, the principle of accountability has featured prominently in the "The Future of Privacy," released by the Article 29 Working Party in December 2009, The Opinion of the Article 29 Working Party released in July 2010, and the global data protection standards of the Madrid Resolution. It is hoped that this paper reflects the participants' awareness of this growing body of work.

An accountability approach requires organizations to establish policies consistent with recognized external criteria. One universally accepted set of guidance would enhance accountability's potential to bridge various national and regional legal regimes. The Madrid Resolution, adopted by the International Conference of Data Protection and Privacy Commissioners in October 2009, is an important first step toward realizing that vision and deserves close consideration.

Looking ahead, we are pleased that the Spanish Data Protection Authority has agreed to facilitate next year's meetings. That phase of the work will likely consider what will be required of accountability agents, how and when organisations will validate their accountability, and incentives for organisations to attain different degrees of accountability.

This paper has benefited from the insights and perspectives of all sectors – industry, civil society, academia, and government.[1] The Centre is particularly encouraged by the participation of data protection commissioners and privacy regulators from Canada, France, Germany, Hungary, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, the United Kingdom and the United States, as well as the European Data Protection Supervisor. Their active involvement highlights the significance and timeliness of this effort.

The Centre would like to thank the CNIL for graciously facilitating the March and June meetings and for providing us with critique and counsel, and all of the experts who thoughtfully and generously contributed to the discussions in Paris and to the drafting of this paper. While their participation has been critical to the success of the work, the Centre alone is responsible for any errors.

[1] The members of the group of experts are listed in the Appendix.

Demonstrating and Measuring Accountability
The Accountability Project – Phase II
Paris, France

Introduction

Over the past 18 months, policymakers around the world have undertaken efforts to examine and update privacy protections in a way that better serves the needs of individuals and organisations[1] and takes into account the realities of technologies and data flows of the 21st century. The concept of accountability has figured prominently in many of these discussions.

An accountability principle 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, published in 1980,[2] and the most recent, the Asia Pacific Economic Cooperation's APEC Privacy Framework, endorsed in 2005.[3] 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 joint paper of the European Union Article 29 Data Protection Working Party (Article 29 WP) and the Working Party on Police and Justice (WPPJ), "The Future of Privacy,"[4] notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalisation and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability."[5] In a later Opinion on accountability submitted to advise the European Commission on how to amend the Data 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."[6]

The APEC Privacy Framework depends upon an organisation's implementation of fair information practices, particularly accountability, to facilitate protected cross-border data flows. Discussions held during the recent series of Federal Trade Commission Roundtables entitled "Exploring Privacy" repeatedly identified accountability as an approach to data governance in a world of increasingly complex data uses and flows. And the proposed international data protection standards of the Madrid Resolution include accountability, stating that responsible persons should take all necessary measures to observe the obligations set forth in the resolution and put in place the mechanisms necessary to demonstrate such observance to individuals and supervisory authorities.[7]

For purposes of this project, accountability can be described as a *demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data.*

---

[1] This document uses the term organisation generally. An accountability approach may apply to public and private sector bodies including – but not limited to – for-profit organisations, non-governmental organisations, educational and cultural institutions, and government and law enforcement agencies.

[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 10 May 2010).

[3] 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] "The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," 02356/09/EN WP 168, December 1, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

[5] Commissioner Peter Hustinx, speaking at the European Data Protection Conference on 29 April 2010, said, "the principle of accountability in our contribution was. . . intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice."

[6] Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN - WP 173, para. 5. http://www.cbpweb.nl/downloads_int/wp173_en.pdf.

[7] "Internacional Standards on the Protection of Personal Data and Privacy: The Madrid Resolution," released October 2009, http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf (last visited 30 July 2010).

In 2009, Phase I of the Accountability Project (Galway) articulated a set of essential elements of accountability. It is against these elements that an organisation's accountability would be established. They are as follows:

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

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

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

(4) Transparency and mechanisms for individual participation.

(5) Means for remediation and external enforcement.[8]

In Phase I,[9] participants recognized that for the approach to work in practice, it would be necessary to resolve practical, implementation-oriented questions, such as how organisations demonstrate accountability, and how regulators measure it. These questions were the subject of Phase II of the Accountability Project which convened in Paris in March and June 2010. At those meetings, experts considered the objectives of accountability, and began to formulate a set of common fundamentals to be demonstrated and measured.

This paper is the result of the discussions at the Paris meetings and of extensive comment and review by participants. While this document does not answer all outstanding questions, it does consider in practical terms how accountability may be measured and demonstrated. Participants in Phase II – international experts from government, industry, academia, and civil society – recognized the importance of framing the practices related to demonstrating and measuring accountability as accurately as possible to avoid unnecessary burdens or unintended consequences that could inadvertently stifle innovation or adoption of new, beneficial technologies.[10]

Approaches to accountability include both regulatory and voluntary components. This paper addresses concepts, principles, methodologies and techniques that could apply across legal frameworks and cultural orientations. Discussions related to accountability have reflected consensus about the need to allow organisations, the flexibility to develop, consistent with recognized external criteria, appropriate practices, and regulatory authorities similar flexibility to adapt compliance reviews and methods to the organisation under review. Thus, even in regulated environments, accountability schemes may first emerge as voluntary mechanisms that enable a "race to the top." Early adopters would demonstrate the hallmarks of accountability in measureable ways. As the confidence of regulators and others in the concept of accountability increases, especially if early adopters take a responsible and constructive approach, it can be widely expected that others will follow. In due course, accountability could become a major and widely-used means of achieving practical effectiveness without imposing unnecessary burdens.

The Scope of Accountability and Benefits to Organisations

A General Requirement of Accountability

When its work began in early 2009, an important goal of the Accountability Project was to develop an approach to privacy and data governance that would facilitate cross-border transfers of data. The project sought to establish the conditions necessary to certify organisations as accountable for the exchange of data with entities outside of their jurisdiction. Such an approach would create a trusted environment in which regulators would have high confidence that organisations would continue to comply with data protection requirements when processing outside their jurisdictions, and would address problems once identified.

As the Accountability Project's work progressed, the principle of accountability became the subject of discussions in other forums considering improvements to existing data protection regimes. In particular, accountability figures prominently in the European Commission's consultation on the legal framework for data protection. The Article 29 WP and the WPPJ in December 2009 issued a joint contribution to the consultation that identified challenges to the current EU legal framework for data protection and the Commission's opportunity to introduce accountability as an innovative response. In July 2010,

[8] "Data Protection Accountability: The Essential Elements - A Document for Discussion," October 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last visited, 30 July 2010).

[9] In Phase I, the Accountability Project began a series of discussions about accountability, particularly as an improved approach to governing trans-border data flows. The Project assembled a group of international experts from government, industry and academia to consider how an accountability-based system might be designed. The experts defined the essential elements of accountability, examined issues raised by the adoption of the approach, and proposed additional work required to facilitate establishment of accountability as a practical and credible mechanism for information governance.

[10] Participants in Phase II of the Accountability Project are listed in the Appendix.

the Article 29 WP issued Opinion 3/2010 on the principle of accountability, proposing that accountability "would 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." The opinion considered accountability in light of both global movement of data and EU framework as a "way of encouraging data controllers to implement practical tools for effective data protection."[11]

This proposed application of accountability to all aspects of data governance prompted the Accountability Project to consider how accountability might serve the full range of data protection functions within organisations, of which the transfer of data across borders represents only one.

Such broad implementation suggests that, as a starting point, all data controllers should be required to meet a level of accountability that provides fundamental assurances. Some controllers, however, may be motivated by stated incentives, and may choose to demonstrate various degrees or kinds of accountability. It may be that certain kinds of accountability, with specific or more rigorous standards, will facilitate proof of the organisation's readiness to engage in certain activities (such as international data transfers) or to be relieved of certain administrative burdens that may be established in regulation (such as notification or registration requirements).

The Accountability Project anticipates several benefits for multiple stakeholders that could result when organisations fulfill a general requirement of accountability. Organisations that can demonstrate adherence to and implementation of accountable practices encourage a data environment where the confidence and trust of individuals is enhanced. Organisations would be better positioned to re-allocate scarce resources to activities that encourage optimal privacy protection for individuals and away from fulfilling requirements (such as re-notification of minor changes in processing) that are costly but that may provide little added protection for data in practice. Were organisations as a general rule to meet the requirements of accountability, data protection authorities' resources could be redirected away from more *pro forma* administrative activities and toward addressing irresponsible actors in the marketplace.

A Customized Approach

This paper proposes a set of common fundamentals that an organisation will need to demonstrate to establish their accountability. These nine fundamentals are designed to provide guidance. Accountability is not a "one-size-fits-all" approach, however, and all organisations will need to determine, consistent with recognized external criteria, which of these nine and/or others they will implement. The fundamentals should be applied 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. For example, an organisation with highly sensitive data that regularly employs the services of third party processors may need to fulfill a set of fundamentals different from those adopted by an organisation holding less sensitive data. Each organisation would be required to make thoughtful decisions about the fundamentals it needs to implement to demonstrate its accountability.

Paragraph 41 of the Article 29 WP Opinion proposes its own set of common accountability measures.[12] The measures set forth are not intended to represent a comprehensive list. But perhaps more importantly, it is welcome that the document does not anticipate that all measures will necessarily apply to all organisations in every circumstance. It also envisions that the general legal obligation to adopt accountability measures is supported by a proposed "toolbox" of measures for data controllers that would provide guidance about what could constitute, depending on the circumstances, the appropriate measures to be adopted by the data controller. What measures are appropriate would be decided on a case-by-case basis by the organisation, resulting in custom-built solutions, whereby controllers tailor measures to the specifics of their data holdings and their systems.

[11] Legislation introduced before the United States Congress also includes provisions requiring corporate accountability for privacy protections.

[12] The Article 29 Working Party proposed a set of "common accountability measures" that might include: 1. Establishment of internal procedures prior to the creation of new data processing operations (internal review, assessment, etc.); 2. Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc.), which should be available to data subjects; 3. Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations; 4. Appointment of a data protection officer and other individuals with responsibility for data protection; 5. Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.; 6. Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects; 7. Establishment of an internal complaint handling mechanism; 8. Setting up internal procedures for the effective management and reporting of security breaches; 9. Performance of privacy impact assessments in specific circumstances; 10. Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc.). Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN - WP 173, Paragraph 41.

The Role of Certification - Review and Acceptance of Practices

For purposes of accountability, certification of an organisation's practices involves review and acceptance by the appropriate supervisory authority or accountability agent. The general requirement to be accountable does not carry with it an obligation to be certified by a third party. However, organisations that wish to engage in certain activities or accrue certain benefits may be required to obtain certification. For example, an organisation may wish to engage in transfer of data outside of its home jurisdiction, or be relieved of certain administrative burdens imposed by regulation. To attain such benefits, organisations may be required to obtain some level of certification. Doing so may involve submitting to a consultation with the certifying authority, which could specify certain fundamentals that the organisation must demonstrate.

It is anticipated that evaluation of organisations by a certifying authority would also be conducted on a case-by-case basis. As stated earlier, one size does not fit all, and certifying authorities will need to determine which of the common fundamentals of accountability an organisation will need to demonstrate.

Binding Corporate Rules (BCRs) provide a good example in principle, though not yet in practice, of how certification of accountability can provide benefits to individuals. BCRs require that organisations demonstrate that they are compliant and will remain compliant with requirements defined by EU data protection authorities for transferring data outside of the EU. When organisations enter into BCRs they are relieved of the pre-approval requirement for specified cross-border data transfer, giving them greater flexibility.

When certification would be required, what a certification process might entail, what benefits to organisations might flow from certification, and how to design a certification process that is cost effective and efficient for both regulators and organisations are all issues that remain to be considered.

Demonstrating Accountability

For What Are Organisations Accountable?

Any discussion about what organisations should demonstrate to establish their accountability raises the question: for what are organisations accountable?

- *Existing law and regulation* - Organisations are accountable for complying with applicable law and regulations.
- *Private sector oversight programs* - Organisations that sign on to a self-regulatory program meet the requirements of that program and submit to its oversight and enforcement in order to be deemed accountable.
- *Privacy promises* - Accountable organisations fufill the promises stated in their privacy policies.
- *Ongoing risk assessment and mitigation* - Accountable organisations assess and understand the risks that collection, use, processing and retention of data pose to individuals, and take steps to address those risks.[13] In an environment in which the nature of data collection, analysis, and use changes rapidly, law, regulation and guidance often lag behind new developments. Within accountable organisations, risk assessment and mitigation keeps pace with changes in technology, applications, business models, personnel, and the commercial and political climate in a way that more traditional means of protection often may not. It also aligns with evolving societal or cultural norms.

To Whom Are Organisations Accountable?

Organisations may be accountable to three entities: data subjects/individuals, regulators, and business partners.

- *Individuals* - Individuals expect their data to be secured, and to be used and managed responsibly. They require that organisations handle their data in a manner consistent with the requirements of law, regulation, and the organisation's posted privacy policy.
- *Regulators* - Privacy and data protection regulators require that organisations comply with applicable law and regulation, and that they honor the commitments they make to individuals regarding the collection, use, and management of their information.

[13] "Data Protection Accountability: A Document for Discussion," October 2009, http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (last visited 10 May 2010).

→ *Business Partners* - Accountable organisations also answer to business partners. While contracts and legal obligations apply, vendors need adequate information about the nature of the data and the obligations attendant to it, and assurances that the accountable data owner has complied with any requirements with respect to that data and its sharing with the vendor. Accountable users of outside vendors need assurances that these obligations can be met by their business partners no matter where the vendor may process the data.

Common Fundamentals of an Accountability Implementation Program

Participants in the Accountability Project identified nine common fundamentals that an accountable organisation should implement. Organisations that wish to be deemed accountable should be cognizant of the fundamentals, and prepared to demonstrate their fulfillment of these conditions as appropriate to the nature of the data they collect, their busniess model, and the risks their use of data raises for individuals.

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 informed by appropriate external criteria found in law, regulation, or industry best practices, and 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 will require the creation of a data privacy leader supported by appropriate resources and personnel, and responsible for reporting to organisation leadership. Commitment by top management should include appropriate 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 its 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 ensure 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 and technologies, and offerings to consumers. Delegation of authority and responsibility for data protection to appropriate units or parts of the organisation has been found to be effective in many accountable organisations. Many accountable organisations have found that situating the responsibility for privacy locally and throughout the organisation has resulted in optimal resource placement and awareness. 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 involve keeping employees aware of new data protection issues that may affect the performance of their job, and 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, implemented and evolve, and as their data requirements change. In response to the findings of those assessments, organisations must take measures to mitigate those risks. Risk assessment is not static, but an ongoing function that responds to the dynamic, evolving nature of data collection, use and processing.

Privacy Impact Assessments are one important risk assessment and mitigation tool. A Privacy Impact Assessment is carried out as part of the process for determining whether to collect data, deploy a new technology or data-driven business model, or use or manage data in a particular way. It is also important when making decisions about how best to secure data. It involves close examination of each new application or process, an evaluation of its attendant risks, and a determination of the steps that must be taken to ensure that the manner in which data is used meets the requirements of applicable law, regulation and the organisation's privacy promises.

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 steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective.

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.

To encourage transparency, the results of that program review should be available to those persons or organisations external to the reviewing group tasked with program oversight. The method by which this information is derived and reviewed must be both appropriately rigorous and cost effective for both organisations and regulators. The results of these assessment measures and/or audits should be reported to the appropriate personnel within the organisation, and when necessary, corrective action should be taken.

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 will need to effectively address data protection problems, such as data misuse, misappropriation or breach. They also must include a formal complaint procedure to address concerns of individuals regarding data protection practices, and potential or actual failures, and to ensure that the rights of individuals related to their data are respected.

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

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

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 redress mechanisms should be appropriate to the character of the organisation, the nature of its data holdings, and the way the data is used and appropriate for the specific issue. The redress mechanism should be readily and easily accessible by individual, and address complaints efficiently and effectively. Industry groups may offer options for individual organisations seeking to implement a redress mechanism. As the specific attributes of an appropriate redress 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.

Measuring Accountability

Although measurement may not always be required, accountable organisations should be prepared to demonstrate their programs when asked. For example, under Canadian law,[14] while every organisation is required to be accountable, not every organisation will undergo accountability review. However, even when measurement is not required, accountable organisations should be prepared to demonstrate on an ad hoc basis how they safeguard personal data.

[14] Canada's Personal Information Protection and Electronic Documents Act provides that every organisation must be accountable for its compliance with the requirements of the Act. It does not as a matter of course, however, require review of an organisation's compliance.

When an organisation wishes to demonstrate its accountability to enable 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 an organisation's compliance with applicable regulations and in some cases its privacy promises. They will also measure accountability based on the organisation's demonstration of policies, privacy programs, and assurance processes.

Such organisations must thus be able to provide evidence of the programs they have 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 third-party recognized 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. Again, consistent with applicable legal frameworks, supervisory authorities may recognize third-party accountability to undertake this role.

Finally, resolution of complaints, spot checks and enforcement will be important to the credibility of an accountability approach. When recognized by supervisory authorities, third-party accountability agents can assume an important role in carrying out these functions, alleviating the burden on authorities with scarce resources.

The Accountability Project identified the following stages in the measurement of an organisation's accountability program. These may or may not occur sequentially, but represent an ongoing process of education, risk assessment, self-certification, review and enforcement.

1. The organisation takes appropriate measures to establish processes and procedures that implement its privacy policies. It carries out risk analysis and mitigation based on their understanding of its obligations under an accountability approach. The organisation may enlist the consultation of the supervisory authority or recognized accountability agent in this process and complete the appropriate documentation.

2. The organisation self-certifies that it meets the requirements of accountability.

3. The supervisory authority or recognized accountability agent reviews such filings and provides some form of acceptance of the certification.

4. The organisation submits to enforcement by the supervisory authority or recognized accountability agent. The supervisory authority or accountability agent will hear and resolve complaints from individuals. It will also conduct appropriate organisation spot checks to ensure that they continue to meet the criteria to which they have self-certified.[15]

5. Supervisory authorities, recognized accountability agents, trade associations, and government agencies engage in raising the awareness of organisations about the obligations that an accountable organisation must meet, and the benefits that flow from being accountable.

Questions about when measurement should take place are yet to be resolved. When should organisations submit to evaluation? When review is necessary, should it occur at the time an accountability program is implemented? Or is it effective and efficient to allow organisations to self-certify their accountability and open themselves to spot checks and review when a significant data protection problem arises or breach occurs?[16] These questions also arise depending upon the scope of an organisation's accountability. Should the timing and requirements of measurement differ if an organisation seeks accountability certification for cross-border data sharing, or for accountable data practices generally?[17]

Issues for Resolution

1. How will remediation work in an accountability approach?

For an accountability approach to have credibility, it must include a mechanism by which complaints are heard and addressed. Policymakers will need to explore and establish effective remediation mechanisms that will reflect and serve the

[15] The manner in which spot-checks might be conducted, and the criteria by which the decision whether to carry out such a review might be determined, requires further consideration. When developing a policy related to such reviews, it will be important to consider the burdens to organisations, the need for defined processes and regulator expectations, and strategic approaches that direct oversight toward where the risks are greatest.

[16] The question of whether ex-ante or ex-post review is appropriate to measure accountability has been the subject of significant discussion. It may be that review prior to or after implementation of an accountability program will depend upon the degree or level of accountability an organisation wishes to achieve. For example, an organisation wishing to attain certification for the highest level of accountability may submit to review before their program is operational. Some data protection authorities (i.e., Canadian), however, rely primarily on ex-post assessment by means of a complaint process.

[17] In many ways, these questions relate to the issue of validation, which this paper identifies as a question for consideration in future work.

requirements of national culture, regulation, self-regulation and law. In cases where industry sectors, regulatory authorities or non-governmental organisations have already established complaint and investigation redress processes, organisations and policymakers may wish to use them as a foundation for the development of remediation mechanisms that specifically serve an accountability approach. Such efforts are already underway as part of the re-examination of the EU data protection directive,[18] the review of the Australian privacy law,[19] and the notice of inquiry issued by the Department of Commerce in early 2010, "Information Privacy and Innovation in the Internet Economy."[20] Organisations will also need to correct or improve processes or procedures that have been shown to be inadequate as a result of a complaint investigation, findings of a validation procedure or data breach.

2. How do organisations determine the appropriate validation mechanism?

Validation by appropriate parties that organisations are in fact implementing the necessary processes and procedures will be important to the effectiveness and credibility of an accountability approach. Validation is distinct from certification; validation rather is a step in the certification process that establishes confidence that policies, implementation mechanisms, and assurance processes are in place and working. The objectives of validation include testing the existence of program elements, assessing the appropriateness of the accountability program's coverage throughout the organisation, and ensuring that the policies and processes are effective. Costs of validation vary based on what is being tested.

Validation takes many forms and carries different meaning in different countries and within different industries. Terms such as audit, internal audit, specialized negative audits and assurance reviews – all of which refer to forms of validation – have different meanings in different industries and locations. Extensive discussions will be required to fully understand the various validation options, the applicability of those options in an accountability program, and the kind of validation necessary to establish confidence in an organisation's accountability program.

Participants in the accountability meetings in Paris reviewed validation mechanisms and requirements that ranged from the most procedurally demanding (e.g., binding corporate rules) to approaches like that taken in Canadian law which require accountability but make no provision for validation.

In Paris participants did not, however, decide what level of validation is appropriate. Making this determination will require evaluating costs, the nature of the data in question, the manner in which the data is to be used and possible legal requirements. Additional exploration is needed to better understand the factors involved in identifying the right validation method, and policymakers will need to make that determination.

3. On what basis are third-party accountability agents recognized?

Third-party accountability agents may play a role in measuring accountability. Accountability agents can be recognized and charged with certifying that the organisation's risk analysis is sound and its program is capable of maintaining effective accountability processes. They may also be accredited to evaluate and approve organisations' applications to be certified as accountable. Accountability agents may play a role in resolution of complaints, spot checks and enforcement.

Third-party review of an organisation's practices against appropriate criteria will greatly facilitate the success of an accountability approach. Qualified, recognized accountability agents will be an important to addressing resource constraints.

Policymakers will need to establish criteria for organisations that wish to serve as accountability agents, and to articulate their role and the extent of their authority. Policymakers will also need to develop criteria by which the credibility and trustworthiness of third party accountability agents can be judged. In establishing this guidance, it will be important that policymakers are mindful that the services of accountability agents must be priced to allow them to develop and sustain a viable business, but still ensure that services are affordable to organizations with less funding as well as those with deeper resources.

Ideally, policy related to the role and operation of third-party accountability agents will be developed in consultation with those organisations, business users, government representatives, experts and civil society.

[18] Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN, WP 173.

[19] "Australian Privacy Principles: Exposure Draft," http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/exposure_draft.pdf (last visited 30 July 2010). This review of privacy principles is one part of a broader inquiry into information privacy protection law in Australia.

[20] http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf (last visited 9 September 2010).

Conclusion

Accountability has assumed increased prominence in international and national discussions about data protection regimes. Phase II of the Accountability Project builds upon the essential elements to articulate practical guidance about how accountability may be demonstrated by organisations and measured by regulators. It envisions a general requirement of accountability that will be met by all organisations and that will benefit organisations, regulators and individuals. While organisations would not, as a general rule, be reviewed by regulators or their recognized accountability bodies, every organisation would be required to stand ready to demonstrate its accountability. For organisations that wish to engage in activities that may raise heightened risk to individuals, certification may be necessary.

To be deemed accountable, organisations will need to demonstrate and regulators will measure certain fundamentals. Accountability is a customized approach, so that what those fundamentals are will depend upon the nature of the organisation, its data holdings, and the risk its activities raise for individuals. The fundamentals include:

(1) Policies

(2) Executive oversight

(3) Staffing and delegation

(4) Education and awareness

(5) Ongoing risk assessment and mitigation

(6) Program risk assessment oversight and validation

(7) Event management and complaint handling

(8) Internal enforcement

(9) Redress

Exploration of how these fundamentals will be validated and certified, how third party accountability agents will be recognized is still necessary.

The need for an accountability-based approach to international privacy protection to ensure robust transfer and use of information in a manner that minimizes risks to individuals and ensures meaningful protection – continues to grow. Identifying and understanding the practical means necessary to implement accountability will be key to its successful adoption. While additional issues require resolution, understanding the way in which organisations demonstrate, and regulators measure accountability is an important step toward that goal.

Appendix

Accountability Project Phase II – The Paris Project Participants

The following lists the participants in the Accountability Phase II – The Paris Project. This list indicates participation in the Paris Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Amit Ashkenazi, Law Information and Technology Authority, Israel

Carman Baggaley, Office of the Privacy Commissioner, Canada

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Emmanuelle Bartoli, CNIL

Bojana Bellamy, Accenture

Emma Butler, Information Commissioner's Office, United Kingdom

Daniel Burton, Salesforce.com

Fred H. Cate, Indiana University, Maurer School of Law

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Leigh Feldman, Bank of America

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Peter Fleischer, Google

Anne-Marije Fontein-Bijnsdorp, Data Protection Authority, The Netherlands

Christine Frye, Bank of America

Jose Leandro Nunez Garcia, Data Protection Agency, Spain

Jose Manuel de Frutos Gomez, European Commisssion

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Yoram Hacohen, Head, Law Information and Technology Authority, Israel

Silke Harz, Office of the Federal Data Protection Commissioner, Germany

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Sandy Hughes, Procter & Gamble Company

Peter Hustinx, European Data Protection Supervisor

The Honorable Michael Kirby

Christopher Kuner, The Centre for Information Policy Leadership, Hunton & Williams

Laraine Laudati, European Commission

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Director, Data Protection Agency, Spain

Brendon Lynch, Microsoft Corporation

Fran Maier, TRUSTe

Olivier Matter, CNIL

Madeleine McLaggan, Commissioner, Data Protection Authority, The Netherlands

Daniel Pradelles, Hewlett-Packard Company

Olivier Proust, Hunton & Williams

Krisztina Rajos, Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary

Kathryn Ratte, United States Federal Trade Commission

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Sachiko Scheuing, Acxiom

Russell Schrader, Visa Inc.

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Blair Stewart, Office of the Privacy Commissioner, New Zealand

Jennifer Stoddart, Privacy Commissioner, Canada

Scott Taylor, Hewlett-Packard Company

Omer Tene, College of Management School of Law, Israel

K. Krasnow Waterman, Massachusetts Institute of Technology

Nigel Waters, Privacy International

Jonathan Weeks, Intel Corporation

Yael Weinman, United States Federal Trade Commission

Boris Wojtan, Accenture

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

Richard Thomas, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP