International Chamber of Commerce
The world business organization

Discussion Paper

Prepared by the ICC Commission on
the Digital Economy

ICC Data Protection Principle of Accountability Discussion Paper

Highlights

- Background
- Global discussions of the data protection principle of accountability
  - OECD guidelines
  - Canada - Personal Information Protection and Electronic Documents Act
  - APEC Privacy Framework
  - CIPL Accountability Project
- Work moving forward

Document No. 373/508 – (23 January 2012)

Introduction

This document is intended to provide an overview of current global discussions of the data protection principle of accountability. Many groups and governments are examining the concept of accountability to understand whether it can provide assistance in promoting the free flow of information while protecting the privacy of individuals. This paper does not express any opinion on that point, but is intended only to summarize current discussions and developments.

Organizations are increasingly looking for opportunities to communicate that they manage personal data in a responsible manner. There is substantial guidance from regulators on specific obligations for processing data. However, this guidance is often focused on individual data uses and is not harmonized across country specific legal systems. There is surprisingly little guidance on what processes and structures an organization should adopt to show they are committed to make real the obligations they have under law, or that they take on voluntarily, for the collection, storage, processing and use of personal data.

In the past couple of years, work has begun to help define the program elements of a responsible organization. This project has been led by the Center for Information Policy Leadership (CIPL) and has focused on providing detail to help understand the Fair Information Policy Principle of "Accountability."[1] Much of the content in this discussion paper is drawn from the CIPL work.

Background of Accountability

Global discussions of the data protection principle of accountability

I. OECD Guidelines

One of the early references to the principle of accountability was in the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines).[2] The OECD Guidelines have been one of the largest pieces of the foundation of data privacy law of the last 30 years. The document calls out specific principles for the handling of data with the idea of both protecting individuals and providing for the free flow of information.

The OECD principles are:

- Collection limitation

[1] *http://www.informationpolicycentre.com/*
[2] *http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html*

- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

The OECD Accountability principle states:

> *A data controller should be accountable for complying with measures which give effect to the principles stated above.*

Further guidance on Accountability is provided in the OECD Guidelines commentary:

> *The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. Accountability under paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.*

This OECD approach to Accountability makes clear it can be an approach that cuts across geographic boundaries to ensure that commitments made for the processing of the data, continue to flow with the data. Unfortunately though, the OECD Guidelines do not describe what an organization must do to satisfy the Accountability principle.

II. Canada - The Personal Information Protection and Electronic Documents Act

In 2000, Canada adopted the Personal Information Protection and Electronic Documents Act (PIPEDA).[3] PIPEDA includes principles drawn from the OECD Privacy Guidelines. The Canadian Accountability Principle states in part:

[3] http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

> *An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*

This definition of Accountability is important as it emphasizes that the principle is focused on how an organization must behave to show it is "responsible". It also makes clear that the obligation continues to exist after the data has been transferred to a third party. However, The Office of the Privacy Commissioner of Canada has not provided any additional guidance to further define what an organization must deploy to demonstrate it is accountable.

III. Asia Pacific Economic Cooperation Privacy Framework (APEC Privacy Framework)

The Asia-Pacific Economic Cooperation forum is comprised of the 21 countries that surround the Pacific Rim.[4] Some of these countries have decades of work creating privacy laws (e.g. Australia, New Zealand, US and Canada), while others are addressing many of the commercial data privacy issues for the first time (e.g. Viet Nam and China). In 2004, APEC adopted the Privacy Framework based on principles similar, but not identical, to those in the OECD Guidelines.

APEC Privacy Principles[5] :

- Collection limitations
- Uses of personal information
- Preventing harm
- Notice
- Choice
- Integrity of personal information
- Security safeguards

[4] *APEC member economies include Canada, the United States, Mexico, Peru, Chile, South Korea, Japan, People's Republic of China, Chinese Taipei, Hong Kong China, the Philippines, Vietnam, Thailand, Singapore, Indonesia, Brunei, Australia and New Zealand.*

[5] *http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx*

- Access and correction

- Accountability

APEC also provided explanatory text for the Accountability principle:

> *A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.*

This guidance helps make clear that accountability is the measures put in place to "give effect" to the organization's obligations. Further, the APEC text echoes the OECD and Canadian concepts that the accountability measures must ensure the obligations continue to flow with the data when transferred to third parties and to other countries. The facing-page commentary uses the word "accountable" to further make this point.

> *Efficient and cost effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred.*

Cross-border privacy rules (CBPR) were adopted by APEC as a mechanism that helps demonstrate an organization's accountability. Through CBPRs, a company self-certifies that it will be accountable for the transfer of data. An "accountability agent"[6] recognized by an APEC economy validates the self-certification. The method by which CBPRs are implemented is being developed through the work of nine APEC pathfinder projects.[7]

---

[6] *An "accountability agent" is often thought of as a third party organization that can operate to evaluate whether an organization is meeting its commitments to act responsibly.*

[7] *These pathfinder projects are staffed by representatives of government, privacy protection agencies, civil society and the private sector. The projects will develop practical tools for implementation, ranging from development of procedures and documents to qualify companies to be certified as having cross-border privacy rules that meet agreed-upon criteria, to the procedures that would guide privacy enforcement agencies assisting in investigations.*

IV. CIPL Accountability Project (Project)

As noted above, the CIPL has undertaken an effort to further define what an organization must do to show that they are accountable. In 2009, Phase I of the Project articulated the following set of essential elements of accountability:

(1) Organization 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 2010's Phase II of the project articulate the following nine fundamental components of accountability that were derived from the essential elements listed above:[9]

1. Policies: *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.*
An organization 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 organization should also design and deploy procedures to put those policies into effect in light of the specific circumstances of its own organizations (e.g., what is collected, how it is used, and how systems and organizations 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 organization leadership. Commitment by top management should include appropriate reporting and oversight of the organization's privacy program. Top management should empower and require senior-level executives to develop and implement the organization's programs, policies and practices. Small and medium-sized organizations 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 organization's privacy program is appropriately staffed by adequately trained personnel.*
While recognizing the need to work within economic and resource constraints, accountable organizations 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

[8] *Center for Information Policy Leadership, Demonstrating and Measuring Accountability: a Discussion Draft, http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF*
[9] *Id.*

privacy program and as that program evolves to address new developments in the organization'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 organization has been found to be effective in many accountable organizations. Many accountable organizations have found that situating the responsibility for privacy locally and throughout the organization has resulted in optimal resource placement and awareness. As in the case of oversight, staffing and delegation decisions in small and medium-sized organizations should reflect the particular circumstances of the organization 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.*

Organizations 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 organization.

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

To be accountable, organizations 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, organizations 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 an 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 organization's privacy promises. To be accountable for its risk assessment and mitigation practices, organizations also should be able to demonstrate the nature of their risk analysis. The organization 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 organization should be able to demonstrate how decisions are made and steps are taken to mitigate risk. The organization 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 organization should periodically review its privacy and data protection accountability program to ensure that it continues to meet the needs of the organization 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 organizations 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 organizations and regulators. The results of these assessment measures and/or audits should be reported to the appropriate personnel within the organization, 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 organization 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 organization's policies and discipline for non-compliance.*

Accountable organizations 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 organization provides remedies for those whose privacy has been put at risk.*

Accountable organizations should establish redress mechanisms whereby individuals may have their complaints heard and resolved. The redress mechanisms should be appropriate to the character of the organization, 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 organizations 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 organizations.

In 2011, the third phase of the Project has focused on the differences between accountability structures that most organizations should implement and more specific requirements that would be "recognized" by supervisor agencies and would likely provide benefits to the organization. This work has explored concepts around when regulators should ask for internal or external validation of an organization's accountability efforts, and what incentives regulators should provide to encourage organizations to adopt practices above the minimum

required by law. In 2012 the Project intends to focus on how to implement an accountability program with specific focus on validation and the role of accountability agents.

There has been considerable discussion of how organizations should implement the accountability principle. Of specific importance to how organizations are expected to implement and validate accountability will be an understanding of how potential requirements apply to small and medium enterprises (SMEs). One size clearly will not fit all. Any obligations need to be flexible enough so as to allow large organizations to establish their trustworthiness, but also so unreasonable obligations are not placed on SMEs. For example, it may make sense that an SME should have someone who is the contact person for privacy and data protection issues, but it would be unreasonable to require SMEs to retain a dedicated full time employee as a Data Protection Officer.

In addition, it is not only the size of an organization that differentiates what accountability measures may be introduced but also the type of operations, the organizational structure, types of data processed and the potential risk. Further, within the same organization, different measures may be needed in different departments, for different services or applications.

The degree to which accountability validation requirements are voluntary or obligatory will be an important point of emphasis moving forward, and on this point there may be substantially different implementations in the various jurisdictions globally that are considering accountability. It is essential any obligations for validation be narrowly scoped to only the most necessary (e.g., as a result of an enforcement action where the organization is found in violation of the existing law). The use of incentives to promote voluntary validation (e.g., a safe harbour from enforcement, a reduction in fines, or an exemption from notification/registration) should be the primary method for advancing accountability. There are a variety of different validation mechanisms that can be scaled up or down to be appropriate to the size and type of organization.

Work Moving Forward

In jurisdictions where accountability is being considered or has already been introduced as a requirement, further definition of how organizations can measure and demonstrate their efforts to responsibly process personal data is needed. This demonstration of accountability will help individuals determine which organizations are deserving of trust in the provision of services and processing of data. There are currently five main areas where this further definition is happening:

1. **CIPL Project**
   As mentioned above, there are plans to continue this project in 2012, with a focus on how organizations can implement the fundamental components.

2. **APEC Data Privacy Subgroup**

   The APEC E-Commerce Steering Group's Data Privacy Subgroup launched in 2011 two workgroups. The first effort will compare their existing country private sector intake and assessment processes ("trustmark") to the current APEC Privacy Framework intake documents for organizations and accountability agents. The group will identify any gaps that exist between them, and suggest the additional steps that companies who have trustmarks need to take to fill any such gaps. The second working group will look at the broader issue of interoperability of privacy systems. This group will develop a governance model for determining whether other companies' privacy policies meet the APEC Privacy Principles.

3. **EU Data Protection Directive**

   The European Data Protection Supervisor[10] and the Article 29 Working Party[11] have commented that accountability should be considered during the examination of the European Commission's 95/46 Directive consultation. Any additional accountability provisions in the new framework would need to focus on removing bureaucratic requirements and accomplishing the objective of aiding the free flow of information. The Working Party document specifically calls out that any new principle should not impose "cumbersome new legal requirements upon data controllers."[12] Accountability provides an opportunity to move away from the ex-ante approvals of specific data processing operations, by instead allowing organizations to demonstrate their overall responsibility in an ex-post structure.

4. **US FTC White Paper**

   During 2010, the FTC hosted a series of roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices. As a result of these roundtables, the Commission published in December of 2010 a document titled "Protecting Consumer Privacy in an Era of Rapid Change". The report asked a series of questions, solicited input, and the Commission has stated they will be issuing a white paper in response to those comments soon. The December 2010 paper mentions the concept of accountability several times as an important goal of the procedures companies need to put into place to implement their policies and commitments. It will be important to analyze how the upcoming white paper integrates accountability into the Commission's proposals.

5. **US Department of Commerce White Paper**

   On December 16, 2010, the Internet Policy Task Force of the US Department of Commerce issued a green paper titled, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework". Many parties have submitted comments to the questions asked in the document. A white paper based on those

---

[10] *http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf , paragraphs 101-107.*

[11] *http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm WP 173 Opinion 3/2010 on the principle of accountability*

[12] *Id., see paragraph 35.*

comments is due from the Department shortly. The green paper mentions accountability many times, and includes the concept explicitly in its second recommendation:

> "To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority."

The paper asked a number of questions on how to implement this recommendation, including what incentives are necessary to encourage accountability, and what technical tools are available to help organizations integrate the concept into their procedures and processes. It will be important to analyze how the forthcoming Commerce white paper addresses these questions.

6. Council of Europe

In the scope of its current work on modernization of its Convention 108, the Council of Europe[13] is considering whether the principle of accountability could be incorporated. The ICC has provided input to the Council of Europe on how accountability should be taken into account, particularly in the area of transborder data flows. The Council will hold a series of discussion meetings, with a goal of finalizing a new Convention by the end of 2012.

[13] http://www.coe.int/lportal/web/coe-portal

The International Chamber of Commerce (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the last century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rules-setting, dispute resolution and policy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law and intellectual property, among others.

ICC enjoys a close working relationship with the United Nations and other intergovernmental organizations, including the World Trade Organization, the G20 and the G8.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC (http://www.iccwbo.org/)

ICC Commission on the Digital Economy

Business leaders and experts develop and promote the continued and stable growth of the Digital Economy, and further adoption of its underlying ICT foundation, through regulatory advocacy of key business positions and best practices through ICC's Commission on the Digital Economy.

Through its members who are ICT users and providers from both developed and developing countries, ICC is recognized in expert circles as the global consensus voice for private sector expertise on policy matters that drive the Digital Economy. It also provides the ideal platform for developing global voluntary rules and best practices for this area of interest to companies worldwide. Dedicated to the expansion of secure ICT-facilitated trade, ICC champions the liberalization and regulatory harmonization that are required to achieve a free flow of information across all borders.

ICC led and coordinated the input of business around the world to the United Nations World Summit on the Information Society (WSIS), Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis).

International Chamber of Commerce
The world business organization
Policy and Business Practices
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org