QUESTIONNAIRE FOR REVIEWING THE OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

DIRECTORATE OF SCIENCE, TECHNOLOGY AND INDUSTRY

COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

WORKING PARTY ON INFORMATION SEUCRITY AND PRIVACY (WPISP)

DOCUMENT Reference DSTI/ICCP/REG(2011)2

RESPONSE FROM THE CIVIL SOCIETY INFORMATION SOCIETY ADVISORY COUNCIL (CSISAC), 4 APRIL 2011

This response embeds the CSISAC response (in bold text) within the sections of the Questionnaire summarising the relevant provisions of the 1980 Guidelines and posing specific questions.

Section 1: The Objectives (the Vision)

Relevant Provisions of the Privacy Guidelines

RECOGNISING that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

RECOGNISING that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

RECOGNISING that transborder flows of personal data contribute to economic and social development;

RECOGNISING that domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such transborder flows;

DETERMINED to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

Questions

1. Do the objectives of the Privacy Guidelines, as reflected in the provisions in the box above, continue to reflect your government's[1] views and priorities today?

2. If not, which of these provisions should be reformulated to better reflect your government's objectives, in light of the mission of the OECD?

CSISAC Response

Civil Society believes that these objectives remain valid. From the perspective of citizens and consumers, the primary interest is the protection of privacy and individual liberties, rather than

[1] OECD footnote: For replies from non-governmental organisations "government" should be understood to refer to the organisation submitting the reply.

the promotion of the free flow of information. While the latter can bring benefits to individuals, it can also have adverse consequences, and should be seen as a qualified secondary objective.

Free flow of information is particularly problematic where it impacts on privacy and is for primarily commercial purposes that are unnecessary for a customer-initiated transaction.

In the context of the OECD's overall mission, Civil Society understands why the two interests appear to be given equal weight. It would however be valuable in these Privacy Guidelines to include some express reference to free flow of information not necessarily being desirable in all circumstances, for example in circumstances where protections in one member country may be considerably weaker than in another.

The reference to 'unjustified' obstacles already implies that domestic privacy legislation may impose some justified constraints, but it would be useful to more clearly explain this. Civil Society notes that where there are comparable and analogous levels of protection for privacy, the barriers to trans-border information flows become negligible.

Civil Society would prefer to see an alternative formulation of this objective, such as:

> **"DETERMINED to advance the free flow of information between Member countries to aid further development of economic and social relations, providing it does not compromise the protection of individuals' privacy and liberties."**

Civil Society would also be very concerned if justified restrictions on the free flow of information by commercial entities and governments in the name of privacy were directly applied to the activities of individuals – such restrictions could easily become an unwarranted and dangerous constraint on individuals' freedom of thought, expression and association.

The Principles in the Guidelines are admirably short and concise. However, this has allowed for significant variations in interpretation. Domestic laws claiming to implement the OECD Principles vary markedly in their detail. While the concept of general principles allowing for flexible application to meet local circumstances is theoretically attractive, it has in practice been abused, with some domestic law versions of the principles being at best significantly weaker and in at worst, completely ineffective. This experience suggests that it is necessary to include some further detail in the Principles, limiting the scope for weak interpretations. We include in this response some proposals for strengthening the Principles.

Section 2: The Strategy

Relevant Provisions of the Privacy Guidelines

RECOMMENDS:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;

b) encourage and support self regulation, whether in the form of codes of conduct or otherwise;

c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:
i) information exchange related to these Guidelines, and
ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Questions:

3. Is the strategy of the Guidelines, as reflected in the provisions in the box above, well adapted to implementing your government's objectives for the Guidelines, given the current context for privacy?

4. If not, what objectives are not well addressed by these provisions?

5. Are there other strategic approaches that might better address these objectives?

CSISAC Response

Civil Society broadly agrees with the 'strategies' promoted by the Guidelines but has some concerns.

Firstly, Civil Society repeats the observations about 'unjustified' obstacles to transborder data flows (Recommendation 2), and about the experience of weak interpretation (Recommendation 1), as already indicated in Section 1 above.

Secondly, Civil Society believes it is time to move away from the endorsement of self-regulation (19b), which has patently failed to deliver adequate privacy protection in those jurisdictions where it has been relied on, and is inherently incompatible with the objective of '... adequate sanctions and remedies ...' (19d). There can be a role for industry initiatives, such as codes of practice and privacy trustmarks or seals, but only as part of a 'co-regulatory' scheme where standards, and effective enforcement, are guaranteed by both legislation and regulators with adequate powers and resources.

Thirdly, the need for effective cooperation and consultation (Recommendations 3 &4), and mutual assistance (21) between supervisory authorities should be emphasised, as the track record for most of the last 30 years has not been good. Developments such as the OECD Global Privacy Enforcement Network (GPEN) and APEC Cross Border Privacy Enforcement Cooperation Arrangement (CPEA) have laid important foundations but have yet to demonstrate their effectiveness in practice.

Fourthly, the objective of ensuring that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries (20), whilst desirable, should not be pursued at the expenses of international best practice and effective enforcement. Some current initiatives, including those focussing primarily on the concept of accountability (see below), could result in a weakening or levelling down of standards. In the three decades since the Guidelines were first drafted there has been a vibrant global discourse around privacy protection and trans-border information flows along broader and more sophisticated grounds than the pursuit of simplicity and compatibility through lowest common standards.

Section 3: The Policy – Definitions and Scope

Relevant Provisions of the Privacy Guidelines

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   a) as few as possible, and

   b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Questions:

6. Are the definitions and scope of the Guidelines, as reflected in the provisions in the box above, well-adapted to the current context for privacy?

7. If not, what issues are not well addressed by these provisions?

8. Are there other policy approaches that might better address these issues or is there a need for additional definitions?

CSISAC Response

The definition of 'personal data' needs to be sufficiently broad to cover all information which has the potential to be used in ways which can impact adversely on the data subject. Unfortunately, while the current OECD definition (1(b)) is very broad on paper, its transposition into many domestic laws has resulted in narrower definitions which require the identification of the data subject to be possible from the data or information itself. The OECD

definition also arguably excludes indirect identification where the actual identity (i.e. name) of a data subject is not known to the data controller, who nevertheless holds a unique identifier (including a communications address such as IP address, email address, telephone number) which allows individually targeted actions based on information about the (unknown) individual known or assumed to be associated with an identifier. Whether this is a limitation of the current definition or not, it is desirable to clarify that indirect identification is covered, to avoid the potential for inconsistencies across different member countries.

There is currently an active worldwide debate as to whether there is a need for separate privacy principles or rules for traffic or location data, or for a separate 'right not to be tracked'. However, there would be no need for this additional complexity if personal data is defined as expressly including any information which enables or facilitates communication or other interaction with a person on an individualised basis, whether or not it meets the current definition of personal data. This would include information about an individual's communications or location, such as the 'communications addresses' mentioned above, and geolocation data.

Any suggestion that the need for privacy compliance can be obviated by 'de-identification' should be treated with scepticism. The de-identification paradigm has been seriously challenged by recent research[2]. The proliferation of personal information in many different locations relatively easily accessed via the Internet has significantly increased the possibility of 're-identification' of purportedly anonymised data.

The scope limitation in (2) is undesirable. Any personal data has the potential to '...pose a danger to privacy or individual liberties.' The issue of whether any particular processing, in any particular context, causes harm to an individual is one that should be addressed at the point of considering complaints, or determining appropriate penalties[3]. It should not be used as a filter for deciding whether the Guidelines apply at all. If it is, it opens the door to self serving decisions by data controllers that some data sets pose so low a risk that the basic obligations for notice, quality, security etc do not apply. The Guideline principles should apply by default to all personal data, however that is defined (see above). However, as already mentioned, we believe that regulators must seriously consider individual rights of self-expression in applying the principles.

It may be desirable to include a definition of 'data processor' and distinguish obligations of processors as distinct from those of controllers, as is done in some other international instruments and in some domestic laws. Transborder flows of personal information increasingly involve one or more processors located in different jurisdictions from one or more related controllers with an interest in the same data.

The right of individual countries to impose higher standards in their domestic law (6) must be maintained, including where those standards relate to Transborder transfers. Similarly, the right of countries to apply different protective measures to different categories of data (3(a)) must be preserved. While international standardisation and consistency are desirable, this

---

[2] E.g. Arvind Narayanan & Vitaly Shmatikov, Myths and Fallacies of "Personally Identifiable Information," 53 Comms. of the ACM 24, 26 (2010); Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets. 29 Procs. of the 2008 IEEE Symp. on Security & Privacy 111 (2008); see also Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev 1701, 1704 (2010); and K. El Emam, "De-Identification: Reduce Privacy Risks When Sharing Personally Identifiable Information", (Ottawa: Privacy Analytics Inc., 2009).

[3] For example, the New Zealand Privacy Act 1993 provides that an action is only an 'interference with privacy' giving rise, potentially, to penalties and sanctions, if it is *both* a breach of one of the Information Privacy Principles *and* causes harm etc (section 66(1)). But the obligations in the Principles apply to all personal information held by (public and private sector) agencies.

should not come at the expense of standards or of rigorous enforcement. Convergence should be through levelling up to the highest common standards, not levelling down.

Section 4: The Policy – Basic Principles of National Application

Relevant Provisions of the Privacy Guidelines

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

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

Questions:

9. Are the basic policy principles, as reflected in the provisions in the box above, appropriate to the current context for privacy?

10. If not, what issues are not well addressed by these provisions?

11. Are there other approaches or new or revised principles that might better address these issues?

CSISAC Response

Introduction

The basic principles remain valid, and have stood the test of time well, being essentially similar to those in other international privacy instruments such as the Council of Europe's Convention 108 (also 1980) the EU Data Protection Directive (1995) and the APEC Privacy Framework (2004). However, the experience of implementing these principles in domestic laws has exposed some limitations, weaknesses and gaps that need to be addressed. It is also the case that other instruments, and domestic laws, have typically found alternative ways of structuring the principles that are more practical and easily implemented. The comments which follow suggest both detailed enhancements and some structural adjustment.

Some of the comments below relate to the fact that in translating the OECD principles into operational laws and regulations it has proved necessary to re-structure them – for example, specific requirements or rules contribute to more than one of the *Purpose Specification*, *Use Limitation* and *Individual Participation* principles. The need to 'map' provisions in domestic laws back to different principles in international instruments creates opportunities for self-serving interpretation and weakens the authority and influence of instruments such as the OECD Guidelines. We submit that it is desirable to re-structure the principles so that they more closely match the common distinction in domestic laws between rules for collection and conditions for subsequent use and disclosure, including cross-border transfers.

Collection limitation

Reasonableness

An overall 'reasonableness' limitation should be included to remedy limitations inherent in consent-based data collection models such as informational imbalances. The following is an example from the Canadian law - PIPEDA[4]:

> **"An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."**

Data minimisation and proportionality

The OECD *Collection limitation* principle (7) does not currently expressly include the concepts of data minimisation and proportionality; i.e. that the least amount of personal information necessary for the intended purpose should be collected in the first place and that collection should not be excessive. These could usefully be added, as could a requirement that collection should be by the least intrusive practicable means (complementing the existing fairness requirement).

Where knowledge/consent are used as justification to define the purposes by which limitation and proportionality are defined, the discussion of the limitations and mitigation of consent-based harms (below) needs to be considered.

Anonymity

While an absolute right to anonymity is unreasonable and impracticable in many circumstances, there is no reason why data controllers should not be required to justify any requirement for identification, and to offer options such as the use of pseudonyms, often

[4] The *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, section 5(3), currently applying to commercial activity of private sector organizations

employed in privacy-enhancing technologies (PETs). This is particularly important in the online environment. Civil Society calls for the inclusion of a principle similar to that already included in Australian privacy law as the 'anonymity principle'[5], with the following suggested generic wording:

> **"Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is either a legal requirement for identification or where it is impracticable for the entity to deal with individuals who have not identified themselves or who use a pseudonym."**

The exceptions in this principle for legal requirement and 'impracticability' could easily be abused, and there should be no suggestion that governments should not have to separately justify any legislated requirement for identification under the other principles.

Data Quality

The Data Quality Principle (8) remains valid and is appropriately worded.

Purpose Specification and Use Limitation

In practice, these OECD principles (9 & 10) have generally been implemented via two separate requirements – firstly to notify individuals of the intended purposes and disclosures; and secondly to limit uses and disclosures to those necessary for the purpose of collection, subject to a limited set of exceptions.

Notice

A requirement to give appropriate notice to data subjects is necessary to give effect to the Purpose Specification and Use Limitation Principles and also contributes to the Openness principle (12)

Use and Disclosure

In practice, implementations of these elements of the OECD principles also address the individual participation principle in relation to consent and choice. They interact closely with collection principles.

Compatibility (as used in Principle 9 – 'not incompatible) is a subjective concept, and would be better expressed as 'uses or disclosures which are within the reasonable expectations of the data subject (to which a 'reasonable person' test would be applied). However, it should be made explicit that 'reasonable expectations' can only encompass uses or disclosures which a reasonable person would consider to be both fair and compatible with the original purpose of collection. This qualification is necessary to avoid data controllers simply creating expectations which data subjects may nonetheless find unfair or unreasonable.

Uses and disclosures outside 'reasonable expectations' should only be permitted with (genuine) consent or under a prescribed exception.

[5] Currently National Privacy Principle (NPP)1 in Schedule 3 of the Privacy Act 1988, applying to private sector organisations only, but proposed in draft amendments before the Parliament to be applied to public sector agencies as well (Australian Privacy Principle (APP1)).

Consent

The concept of consent is fraught with difficulty in a data protection context. If it is used as an exception – as it is in Principle 10(a) – then it needs to be expressly defined as meaning free, informed and revocable, and not bundled with other consents. There are many current transactions which misleadingly use 'consent' when they in reality amount only to 'notice, and acknowledgement that nominated uses/disclosures are a condition of the transaction'. There should be a general principle that genuine consent (i.e. informed, unambiguous, unequivocal, revocable etc) should be the basis of fair processing (subject to other public interest exceptions). This would be consistent with the overall aim of transparency in transactions involving personal data. It would also be consistent with the introduction of a 'right of opposition' (see below) – a right to refuse secondary uses is necessary to avoid data controllers making them a condition of service.

A distinction also needs to be made between overall consent for a relationship or transaction and consent for the specific terms and conditions – individuals may typically be willing to give the former but not be happy with the latter, but are rarely in a position to negotiate.

It is important that any consent or opposition/refusal provisions also expressly address the form in which consent is sought and recorded. Interface design and choice defaults have a dramatic effect on user choices. 'Privacy by default' should be expressly indicated as the preferable form of consent, with individuals having to make a conscious choice to permit any secondary uses.

The relevant provisions of the Canadian private sector privacy law (PIPEDA[6]) are relevant, as is the following currently proposed amendment to PIPEDA:

> ***"the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting."***[7]

Right of opposition

A right of opposition in the sense used in the EU Directive (Article 14); i.e. a right to reject processing, should be included, even when consent was originally granted, if it is reasonable for consent to be revocable in the circumstances.

Right to be forgotten?

A right to oblivion (to be forgotten) has been raised in recent debates. This is superficially attractive and may be particularly relevant in the commercial private sector context. However, it needs further consideration, as there may be many circumstances in which it would be unreasonable or impractical, and would even conflict with other principles such as security or data integrity, or interfere with the audit trail needed for accountability. If applied to individual non-commercial action, it should be carefully balanced against other important values such as free expression. Whilst it may be possible to apply such a right to the records of data controllers it would be intolerably oppressive to try to apply it to the memories of individuals.

A right to be forgotten is closely related to the concept of retention limitation (which in some laws appears under the security principle). Retention limitation is unarguably desirable, being consistent with data minimisation and proportionality principles, and should be expressly

---

[6] Personal Information Protection and Electronic Documents Act (PIPEDA), see Schedule 1, Principles 4.3.4, 4.3.5, and 4.3.6

[7] Bill C-29, the *Safeguarding Canadians' Personal Information Act*, 3rd Session, 40th Parliament, 59 Elizabeth II, 2010

recognised. Any wider 'right to be forgotten' should at the very least encompass a requirement that personal data should be deleted or made inaccessible once the purpose for its collection is complete, though this does not meet all situations where such a right is needed and may be justifiable. In relation to 'making inaccessible' we refer to concerns about the effectiveness of de-identification already mentioned above (see footnote 2)

Legal authority

The exception for 'by the authority of law' (10(b)) needs to be qualified as 'required or expressly authorised by or under law'. 'Authority of law' on its own is too ambiguous and has been interpreted in some jurisdictions as in effect allowing any use or disclosure that is not expressly prohibited, which seriously undermines the effectiveness of the Use Limitation Principle.

Security

The OECD Security principle (11) appropriately refers to 'reasonable ... safeguards' as security precautions should be proportionate to the risk involved, which can be influenced by the nature of the personal information and the likely consequences for data subjects of any security breach.

We submit that the wording of the security principle could usefully be broadened to cover the risk of *authorised but inappropriate* use, disclosure etc. For example, use or disclosure of personal data in contravention of a Use and Disclosure Principle, even by someone authorised to use/disclose in other circumstances, should be also a breach of the Security principle. Reasonable security safeguards should include measures such as access control tools to limit the risk of authorised but inappropriate uses, and audit tools to detect such uses. The addition of a 'catch-all' term such as '..other misuse' to the security Principle (already found in some domestic laws) would also be useful to cover a range of events which while difficult to define in advance, will manifestly be inappropriate when detected.

The principle should also expressly refer to security safeguards/measures as encompassing both technological and other means. While it may not be appropriate to mention specific technologies in general principles, it needs to be clear that technologies such as encryption can make a significant contribution to privacy protection.

Consideration should be given to adding a data breach notification requirement. This has already been implemented in some jurisdictions as a separate law (e.g. many US States) or guideline (e.g Australia, UK) but can also logically be associated with a security principle as it is an obligation that flows directly from a breach of security. Any data breach notification requirement needs to be proportionate to the severity and implications of a breach; i.e. there need to be appropriate criteria for triggering the requirement. It should also involve notification of affected individuals in appropriate cases meeting the threshold criteria, as well as of relevant regulators in all cases.

Openness

The OECD Openness principle (12) remains valid, and an essential element of the Guidelines. In the new technology environment, 'usual residence' of a data controller is of limited value – what should be required in addition to identity is a functional means of contacting the controller (e.g. an email address or phone number that is answered within a reasonable time).

Individual Participation

The OECD Individual Participation principle (13) only deals with two specific aspects of participation – access and correction/deletion, which are the words used in many domestic laws.

Another important aspect of participation is the role of consent and choice, which we have addressed under the Use Limitation principle above.

The existing principle provides appropriate criteria for access and correction. In addition, the right of access should include a right to be informed, on request, of the source of the data, also all recipients of the data (more specific than the general description given in collection notices), and also, where practicable, an explanation of the logic of the processing, e.g. credit scores (this latter would arguably already be required under 13(b)(iv) '... readily intelligible').

The inclusion in the existing individual participation principle of a right to have data erased is valuable, although it has in practice been implemented in most domestic laws as only a limited right of erasure of inaccurate data. A right to erasure has a particular resonance in relation to social networks and 'cloud computing' and could usefully be extended with an express 'right to be forgotten' – erasure of factual information – where practicable and lawful.

Accountability

Accountability is an important Principle, but only effective if it means more than just responsibility. And mere assertions by data controllers that they are accountable are not sufficient. There should be an obligation to *demonstrate* that measures have been taken to ensure full respect for data protection rules. Such demonstration should include some combination of monitoring/auditing; internal privacy oversight at various stages of any new product development process; reporting, and an obligation to cooperate with monitoring and inspection by supervisory authorities.

Caution should be taken in the use of 'accountability' which has been suggested in recent data protection debates as alternative to specific requirements for compliance with rules. In particular, 'Accountability' cannot be and must not become an alternative to data export restrictions.

Section 5: The Policy – Basic Principles of International Application

Relevant Provisions of the Privacy Guidelines

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Questions:

12. Are the policy principles reflected in the provisions in the box above well-adapted to the current international context for privacy?

13. If not, what issues are not being well addressed by these provisions?

14. Are there other approaches or new or revised principles that might better address these issues?

CSISAC Response

The basic Principles of International Application remain valid – in particular the acknowledgement in 17 that restrictions on cross border transfers are legitimate and justifiable where they are designed to ensure no loss of privacy protection. While the principles do not address the situation of transfers to non-OECD member countries, it is implicit that restrictions and controls are equally acceptable where the destination non-member country does not 'substantially observe' the Guidelines. 'Substantially observe' should mean not only that there are similar rules but that there is adequate monitoring and enforcement – and this could be made more explicit.

These Principles provide a sound foundation for cross border controls in domestic legislation, and for defending such controls from pressures to allow exceptions which would weaken them. Commercial data controllers in particular are constantly lobbying for exceptions that would allow them to process personal data in low-cost locations with dubious privacy and data protection standards. They argue that their acceptance of responsibility for the data wherever it is held or processed should be a sufficient basis for transfer. But the reality is that data subjects cannot be guaranteed the same level of privacy protection, including access to remedies for breaches of the Principles, without enforceable privacy laws in the countries where processing takes place. Contracts and agreements between 'exporting' data controllers and 'importing' data processors or controllers cannot replace a proper legal framework with accessible complaint mechanisms and an effective supervisory authority.

CSISAC can be contacted via liaison@csisac.org Website: http://csisac.org