Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa|ON|K1N 6N5
cippic@uottawa.ca
www.cippic.ca

SUBMISSION TO THE COUNCIL OF EUROPE

CONSULTATION ON THE COUNCIL'S DISCUSSION PAPER

MODERNIZATION OF CONVENTION 108

MARCH 10, 2011

Tamir Israel, Staff Lawyer

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a law and technology clinic based at the University of Ottawa in Canada. CIPPIC's advocacy covers diverse technology-related issues, and has been advocating in the public interest on privacy issues since its inception. CIPPIC's experience in this area includes, but is not limited to, testimony before Canadian parliamentary committees on privacy-related legislation including active participation in a review of Canada's federal data protection statute, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), intervention before the Canadian judicial system on various privacy related issues, and provision of legal assistance for under-represented Canadians on privacy issues.

In addition, CIPPIC has filed over 20 privacy complaints under PIPEDA on data protection matters such as the privacy practices of social networking sites, the use of mid-network collection of data on customers by Internet Service Providers for the purpose of traffic management using Deep Packet Inspection tools, the implication of online data breaches of sensitive data, the cross-jurisdictional data collection practices of US-based websites and web-based services, and the potential privacy implications of the Google/Double-Click merger, to name a few.

CIPPIC is in receipt of comments submitted to the Council of Europe by Nigel Waters and Professor Graham Greenleaf on behalf of the Cyberspace Law and Policy Centre (CLPC) as part of this consultation. CIPPIC offers this submission in support of those comments and to offer our experience with Canada's data protection regime in aid of the Council's efforts at reviewing its Convention 108. Many of our comments are based heavily on those of the CLPC submission and where we fail to expressly comment on specific elements of that submission, we can be taken to be supportive of those elements. We structure our submission around the general questions in the Council of Europe "Modernisation of Convention 108: Give Us Your Opinion!" document.

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

A principled, technologically neutral approach is preferable. PIPEDA is drafted in a flexible manner that has allowed it to remain relevant in an era where the rate of technological change has been perhaps unprecedented and continues to increase. A flexible, principled approach is essential, but needs to be updated from time to time to address some shifts in practices and technologies.

2. Should Convention 108 give a definition of the right to data protection and privacy?

Many have struggled to define 'privacy' in different ways and in different contexts. Privacy is, in CIPPIC's view, a human right best defined within the context of human rights instruments and applied to the specific context and protections set out in the Convention.

In this respect, the CLPC recommendation to define privacy rights in broad strokes within the Convention itself should be followed.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes. While Canada has taken a bifurcated approach to privacy protection vis-à-vis the public and private sectors, this has been criticized. Particularly, Canada's Federal *Privacy Act*, which offers Canadians added privacy protection against the state, has been criticized by civil society and our Federal Privacy Commissioner for failing to remain relevant where it fails to follow the principled approach adopted in PIPEDA. Canada operates under a federal system and a number of Canadian provinces have adopted principled public-sector privacy statutes that have proven more flexible and capable of keeping up with the times.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0)?

CIPPIC shares concerns stated in the CLPC submission with respect to this question. PIPEDA is limited in its application to 'commercial activity', defined broadly. While it is able to capture Web 2.0 activity, this is only at the intermediary/organizational stage. This has been recognized as one of the coming challenges for PIPEDA's ability to protect privacy in an increasingly participative web. At the same time, it is recognized that data protection principles will be difficult for individuals acting in pursuit of private activity to meet and that, if applied to such activity, careful balancing against the free expression rights of individuals will be required. Courts may be best placed to apply evolving norms to this space, but, as noted in the CLPC submission, tribunals are of lower cost and may be able to contribute to this evolving field in a more flexible manner.

5. The definition of automated processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

   The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

CIPPIC is supportive of the CLPC submission on these points. Particularly, clarification that all collection processes should be minimized as much as possible to necessary purposes and should be conducted by non-intrusive means is integral.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

CIPPIC supports the CLPC's call for a flexible approach that emphasizes proportionality and reasonable expectations. Consent can play a role in this framework but should be adopted with caution. Consent-based protections should be coupled with specific requirements to detail intended collection, use and disclosure; to minimize such collection, use/disclosure to what is necessary for specified purposes/uses; to a right of opposition/opt-out/opt-in for secondary purposes to avoid tied-selling, and guidance on the form of consent to be utilized when acquiring consent to address consent viscosity in user interface or a strict notification-based regime where notice to unexpected or sensitive data practices is buried in long, rarely read policies.

The form and acceptability of consent should be informed by reasonable expectations and proportionality, as well as the sensitivity of the information in question, and it should be recognized that consent is not definitive in all circumstances. In addition, data controllers should not be permitted to rely on consent in circumstances where it is unreasonable to believe that individuals have provided it on an informed basis.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Data breach notification requirements are crucial for a number of reasons. First and foremost, it is important for individuals to be aware that a breach has occurred so that they are able to take steps to reduce potential harms, where necessary. Second, without such requirements, particularly backed with potential fines for non-compliance, incentive to disclose data breaches is minimal. Finally, breach notification requirements have the tertiary effect of providing strong incentives to strengthen security measures as well as an opportunity to study how and where breaches occur.

The CLPC submission properly stresses that notification requirements should be guided by specified threshold criteria. To balance the need to provide certainty in light of subjective criteria with the need to avoid notification fatigue, some have suggested a two-tiered reporting system, with a low threshold for reporting to a data protection authority and a higher threshold for reporting to affected individuals.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

The CLPC submission properly notes that a flexible regime should be able to account for the additional sensitivity and expectations raised by this type of data and to provide added protection in kind.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Accountability is an important element of any data protection regime but should not, as stated in the CLPC submission, be capable of overriding other requirements.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Specific requirements of proactivity in architectural and product design so as to account for privacy concerns is integral. More important is a commitment to 'privacy by default' as an overriding design principle. CIPPIC notes the CLPC's caution in ensuring that data protection authorities do not compromise their ability to provide *ex post* criticism by adopting an overly proactive prior approval process.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Yes. The right to access needs to be expanded in light of the increasing complexity of computational models on which criteria and assumptions are based.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

PIPEDA's reasonable retention requirements which require personal information be made inaccessible once the purpose for which it has been collected has expired are an important part of the overall principle of minimization, limitation, and proportionality. PIPEDA additionally includes a right to opt-out of unnecessary purposes for the collection, use and disclosure of personal information.

A right to be forgotten is becoming more important in many contexts and deserves further exploration in light of the potential practical obstacles attached to its realization.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

20. Should a right 'not to be tracked' (RFID tags) be introduced?

Both of these rights can be achieved through more general principles of confidentiality, privacy, and accuracy.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

Anonymity is a right that deserves distinct articulation and protection. The capacity to act anonymously is central to protection of privacy in inherently public/semi-public spaces such as those that are pervasive online. It is also integral to the minimization/limitation principle and at the core of proposed federated identity systems. Yet incentives are strongly aligned to require identification in situations where it is not necessary. The language proposed in the CLPC submission is instructive.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

As noted in the CLPC submission, additional balancing of free expression (beyond that already inherent in conceptions of reasonableness and proportionality) is more appropriate where individual activity such as citizen journalism is covered by the Convention. Even in such contexts, care must be taken as it will be difficult to capture the appropriate balance between expressive activities and privacy in a categorical manner. Even 'news reporting' may amount to an invasion of privacy where the public importance of the news is low and the level of invasiveness is extremely high.

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Expanding the scope of available remedies can only further the scope of protection offered. The CLPC paper notes that remedies are available only in contexts where requests for correction have been denied. It is appropriate, in CIPPIC's view, to add fines as well as civil and class action remedies for breaches of the principles in certain contexts. ADR mechanisms could be beneficial but should not operate to frustrate other available remedies.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

A choice of laws provision will provide certainty, but should not operate to frustrate locally offered consumer protections. A place of purchase or place of sale default jurisdictional rule should also be applied with caution, taking into account the limited means of individuals, as opposed to organizations, to bring complaints in distant jurisdictions.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

26. Should their role and tasks be specified?

The points made in the CLPC submission on the role of DPAs are directly on point and particularly the requirements for statistical reporting mechanisms and provision of objective reasoning for decisions. Thought might be given to making DPA decisions binding by common law concepts of *stare decisis*.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

CIPPIC mirrors concerns stated in the CLPC of a potential 'race to the bottom' that may result from any global effort to establish minimum rules. This applies to both private and public sectors.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

CIPPIC has no comment on this point.