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

MODERNIZATION OF CONVENTION 108: NEW PROPOSALS

T-PD-BUR(2012)01REV

MARCH 30, 2012

Tamir Israel, Staff Lawyer

Council of Europe
Modernization of Convention 108: New Proposals

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. Pursuit of its public interest mandate includes expert testimony before parliamentary committees, interventions in Canada's judicial system, appearances and submissions to various tribunals such as the Office of the Privacy Commissioner of Canada, and participation in international Internet governance bodies. In addition, CIPPIC advises clients (organizational and otherwise) on matters with a public interest dimension and provides public education resources on various legal issues.

Privacy and data protection have been central to CIPPIC's mandate since its inception. CIPPIC's organizational experience includes active participation in the development and ongoing modification of Canada's federal data protection statute, the Personal Information Protection and Electronic Documents Act (PIPEDA). 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 Internet Service Provider customer's data for the purpose of traffic management using Deep Packet Inspection network equipment, the implications 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.

While Canada is not a member of the Council of Europe, nor is it a signatory of Convention 108, the Canadian government participates in CoE activities by virtue of its status as an Observer State. More importantly, as in most areas of Internet governance, we cannot live in splendid isolation and the policies of one governance body will often impact on others with like-minded ideas and values. With this in mind, CIPPIC offers the following comments based on its domestic experience with Canada's data protection regime as well as on relevant experiences in international policy-making venues.

Generally, CIPPIC commends the Council of Europe on adopting a balanced set of proposals for the modernization of its privacy protective framework. Our selective comments here supplement our initial comments of March 10, 2011,[1] and are restricted to those areas where our institutional experience is deemed to be of greatest potential benefits. Lack of comment on a specific provision should not be taken as endorsement thereof. It is our hope that our comments below are helpful.

Article 2 – Definitions

The document intends to narrow the definition of 'personal information' in order to provide guidance on the limits of data protection principles in an age where de-anonymization is almost always a real and tangible risk. This should only be done with great caution, as too great a limitation may well exclude many privacy harms that should rightfully remain subject to data protection principles.

The proposal intends to clarify, in the explanatory report, that 'personal information' excludes anonymized data that cannot be linked to an individual without 'unreasonable time or effort'. This raises

[1] CIPPIC, "Comments on the Modernization of Convention 108", Submission to Consultation on the Council of Europe's Discussion Paper, March 10, 2011, <http://www.cippic.ca/sites/default/files/20110310-CIPPIC-Comments-Conv108.pdf>.

concerns, as it may not provide adequate protection for personal information. For example, it may fail to account for scenarios where specific interest in a specific individual might justify an 'unreasonable' amount of time and effort, such as in the case of a nosy neighbour attack, or if there is organizational interest in identifying a specific sub-category of individuals. As 'personal information' is the gatekeeper of data protection regimes, it is important to adopt a broad and expansive definition so as not to exclude categories of information best left within the scope of the statutes.

The express inclusion of data capable of facilitating 'individualisation' is a welcome clarification, and adequately addresses online scenarios where tracking is largely traceable back to an anonymous identifier. However, the inclusion of this qualifier does not in and of itself alleviate all concerns raised by the 'unreasonable time or effort' standard.

Consideration should be given to adopting a higher standard. Canadian jurisprudence, for example, has converged on a definition of personal information that applies wherever "there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information."[2]

Article 3 - Scope

The document proposes to exempt private conduct from the Convention's scope. Specifically, 'purely personal or household activities' are to be exempted unless the data is "made accessible to persons outside the personal or household sphere."

CIPPIC agrees that limiting the scope of data protection regimes to exclude purely private activities may be justified. While the capacity of individuals to injure each other's privacy has grown significantly in a web 2.0 environment, data protection regimes are far better designed and suited to ensuring accountability in organizations than in inter-personal interactions. PIPEDA, Canada's data protection regime, is limited in application to an transaction or course of conduct that is of a commercial character.[3] With respect to the particular line drawn in proposed changes to Article 3, including information 'made accessible to persons outside the personal or household sphere' appears intended to ensure that while private user interactions (social network interactions) are excluded, commercial activities of those entities that facilitate these interactions (the social network itself) remain subject to the regime.

This should remain the guiding principle for any demarcation aimed at excluding private conduct. Proposed Article 3 suggests the possibility that this 'private conduct' exception be extended to all 'legal persons'. This appears to imply the inclusion of corporations which, if it is the case appears at first glance to have great potential for undermining the careful demarcation indicated in proposed 1bis of Article 3.

Article 5 – Legitimacy of data processing

The document envisions the adoption of a consent regime. This should be undertaken with great caution. The proposal does well to limit data processing to scenarios that are proportionate and

[2] Office of the Privacy Commissioner of Canada, "Interpretations: Personal Information", Last updated October 2011, <http://www.priv.gc.ca/leg_c/interpretations_02_e.cfm >.

[3] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, paragraph 4(1)(a).

necessary to legitimate objectives. It should be made clear, at the outset, that consent does not override a data controller's obligation to ensure data processing is proportionate and necessary to achieve a legitimate objective.

The definition of consent could benefit from added clarification on what constitutes 'freely given, specific and informed'. It should be manifestly clear that 'informed' consent entails more than mere 'notice' and does not import concepts developed in the context of contract law. Consideration should be given to 'meaningful consent' as a better defined standard. Further, 'time' of consent is important in this context and merits specification in either the Article or its accompanying explanatory note. Consent should be premised on information provided prior to the initiation of any data processing (or as soon as is practically possible thereafter).[4]

Further, in an online environment, the viscosity or 'effort' associated with achieving a privacy-friendly service configuration is critical.[5] In this context, subtle changes in privacy settings or in the mechanisms by which consent is sought can have dramatic impact on citizens' privacy choices.[6] It leads to privacy practices conducted under the superficial appearance of 'consent' but which depart dramatically from user expectations of how their data is actually being processed.[7] It then becomes critical to ensure that 'quality of consent' obligations recognize impact. Recognizing the principle of 'privacy by default' will help achieve this objective.[8] Privacy by default is a concept that obligates data controllers to assume

[4] For examples of 'time of consent' provisions, see the *Personal Information Protection and Electronic Documents Act*, , S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principle 4.2.3: "*The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.*"

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Council Recommendation, September 23, 1980, <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>, Part Two, paragrpah 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.*"

[5] See Office of the Privacy Commissioner of Canada, "Report on Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", May 2011, <http://www.priv.gc.ca/resource/consultations/report_201105_e.pdf>.

[6] See R.H. Thaler & C.R. Sunstein, "Nudge: Improving Decisions About Health, Wealth, and Happiness" (Michigan: Caravan Books, 2008), for a description of the impact of 'effort' on economic efficiency and customer choice, generally. See L. Church & A. Whitten, "Generative Usability: Security and User Centered Design beyond the Appliance", *NSPW 2009*, <http://www.nspw.org/papers/2009/nspw2009-church.pdf> for a description of the impact of interface design and viscosity on user choices (albeit in the context of security, not privacy. For more privacy-specific examples see I. Kerr, J. Barrigar, J. Burkell, & K. Black, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent", in I. Kerr, V. Steeves, & C. Lucock, *Eds*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799> and A. Acquisti & J. Grossklags, "Privacy and Rationality in Individual Decision Making", (2005) January/February *IEEE Security & Privacy* 26, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1392696&userType=&tag=1>.

[7] As a recent example, see: P.G. Leon, J. Cranshaw, L.F. Cranor, J. Graves, M. Hastak, B. Ur & G. Xu, "What Do Online Behavioural Advertising Disclosures Communicate to Users?", Carnegie Melon CyLab, CMU-CyLab-12-008, April 2, 2012, <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf>, the results of this wide-ranging user expectation survey revealed that only a fraction of users were able to identify an industry standard opt-out mechanism was, in fact, an opt out mechanism (many believed it as actually a mechanism for purchasing ads!). This demonstrates the importance of providing clear guidance on the need for privacy defaults or clear obligations on the mechanism of consent.

[8] CIPPIC notes that while it views 'privacy by default' as an element of consent, under the proposed scheme for Convention 108 modernization it may be best positioned as a 'Right of the Data Subject' under Article 8 (not, it should be noted, as an 'additional measure for the controller').

that users *prefer* privacy, as opposed to 'sharing', in contexts where there is a user choice to be made. Another manner in which the 'privacy by effort' problem may be addressed is by providing direct guidance (in the Article itself or in the explanatory note) on the *form* of consent. PIPEDA, for example, expressly ties the form of consent to reasonable user expectations as well as to the sensitivity of the data being processed, given the context in question.[9] This permits for more nuanced and contextual protection for sensitive user data (conversations with friends, movie preferences, reading lists) that respects the contextual integrity of user expectations even in scenarios that fall short of the imperative found in proposed Article 6.

Finally, the proposal in Article 5.2(b), which would exempt data controllers from seeking consent in certain contexts, should not permit data controllers to ignore user consent simply for the purpose of meeting binding contractual obligations. Such obligations are typically within the data controller's power to negotiate and define and, hence, entering into such obligations should not be used as an excuse to bypass what would otherwise be a mandatory consent requirement. Indeed, data controllers could easily enter into such obligations for the sole purpose of bypassing data protection consent requirements. CIPPIC notes that PIPEDA, which puts in place a primarily consent-based data protection regime, has no exception for binding contractual obligations, yet, to our knowledge, this has this has yet to emerge as an obstacle to legitimate business practices.

Article 7 – Data Security

The proposed addition of a data breach notification provision is a welcome addition to Article 7. With data breach notification obligations, care must be taken to strike a careful balance. On the one hand, user notification fatigue should be avoided, so user notification of any and all breaches is not a workable solution. On the other, setting too high and subjective a standard leaves the decision-making process largely in the hands of data controllers subject to strong countervailing incentives militating against disclosure (public embarrassment/loss of organizational reputation; the prospect of costly regulator-imposed security safeguards to remedy the cause of the problem; or even lawsuits resulting from the exposure of user data).[10]

Proposed changes to Article 7 aim to address this issue by adopting a two tier reporting system. A first tier obligates data controllers to report "any violation of data security which may seriously interfere with the right to the protection of personal data" to a competent authority. Tier two, expressed in the explanatory note, adds that where serious risks exist, the data controller should also notify potentially affected data subjects.

The two tier structure adopted by the proposed breach notification regime is effective, but the standards employed should be carefully assessed. Particularly, the first standard should be low enough to ensure that, at minimum, the majority of breaches are reported to a data protection authority. The benefits of an inclusive first tier reporting obligation are several, including: ensuring an objective assessment of whether the breach threatens user privacy, or whether user remedial measures will be necessary (and, hence, user notification should ensue); facilitating evidence-based policy-making with

[9] See *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principles 4.3.4 to 4.3.6.

[10] For a comprehensive overview, in the context of an assessment of flaws in a proposed Canadian data breach notification regime, see: J. Lawford & J. Lo, "Data Breaches: Worth Noticing?", December 2011, <http://www.piac.ca/privacy/change_data_breach_bill_to_notify_more_consumers_new_piac_report_1/>.

respect to cyber security by allowing DPAs to track the scope and breadth of the data breach issue; providing strong and necessary incentives for data controllers to adopt strong technical safeguards by assuring their accountability for breaches; ensuring that adequate steps are taken to remedy the underlying factors of a breach. As even low-risk breaches of safeguards can be indicative of more serious security flaws, it is important to ensure an inclusive reporting obligation at the first tier if these objectives are to be fully realized.

The standard employed by the proposed Article 7 amendments – 'may seriously interfere with the right to the protection of personal data' – may not be sufficiently rigorous. By contrast, proposed EU data breach provisions obligate data controllers to report *any* personal data breach (defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed").[11] The EU proposal similarly obligates data controllers to report on the cause of the breach and on steps taken to address it and prevent its recurrence. The Uniform Law Commission of Canada adopted a similar approach (broad 'report to a data protection authority' obligations coupled with the obligation to include details relating to the nature of the breach and steps taken to address it) in its draft data breach notification statute.[12] While U.S. federal data notification proposals do not opt for a two-tier approach, they do obligate data controllers to notify customers of a breach unless there is "no reasonable risk of harm or fraud".[13] The CoE should consider adopting a more rigorous reporting criterion – at least for the lower 'supervising authority' reporting tier.

Finally, it should be specified explicitly (whether in the Article or in the explanatory note) that supervising authorities be given the power to compel data controllers to notify affected customers whenever it is deemed that the second tier reporting standard is met. DPAs in this context serve a function that transcends mere 'reporting' and encompasses oversight. This is critical, as data regimes that leave this assessment in the hands of data controllers are open to subjective organizational decision-making that is likely to favour non-disclosure more often than not.

Article 8 – Rights of the data subject

The proposal adopts a number of new and important user rights that will help citizens protect their privacy in a world that increasingly challenges their capacity to do so. The addition of a user right to information relating to the logic involved in data processing of automated decision-making is especially critical, as is the right to avoid scenarios where automated decision-making can have significant legal implications or other impacts.

[11] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data", January 15, 2012, COM(2012) 10 final, 2012/0010(COD), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF>, 'personal data breach' is defined in Article 3, section (9). The obligation to inform a data protection authority is found in proposed Article 28.

[12] Uniform Law Conference of Canada – Civil Section, "Protection of Privacy Amendment Act (Data Breach Notification), Interim Report 2009, <http://www.ulcc.ca/en/poam2/9%20Interim%20Report%20Protection%20of%20Privacy.pdf>. Note that current Canadian legislative initiatives aimed at enacting data breach notification obligations have not yet followed these proposals.

[13] The White House, "Data Breach Notification Legislative Language", May 2011, <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf>. See also: White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

The absence of a 'droit d'oubliette' is not material. CIPPIC notes that it is not aware that such a right raises free expression concerns (although the means of its enforcement might). Regardless, CIPPIC is of the view that the right to be forgotten overlaps completely with limits on data retention, the right to withdraw consent (which, in turn, is inherent in the right to consent) and the right of opposition. As each of these subsidiary rights is included within Convention 108 or is proposed in this modernization initiative, there remains little reason to adopt a distinct 'droit d'oubliette'.

With respect to the right to opposition proposed in Article 8(d), CIPPIC retains concerns, again, over the proposed standard. Proposed Article 8(d) restricts a citizen's right to refuse consent to a specific data process to scenarios where that citizen can marshal an 'overriding legitimate reason' to object. Consent-based privacy regimes aimed at empowering users to determine how their data will be processed put citizens' subjective preferences at the core of data processing. This is fitting, given that in most contexts users will be interchangeable to data controllers and will be best placed to determine whether a specific process is desirable or not (based on meaningful consent and non-viscous decision-making). In keeping with this theme, users should be able to refuse most data processing activities that are not essential to provision of the service being sought. There should not be a need for 'overriding legitimate reasons' to refuse consent. Rather, data controllers should have 'overriding legitimate reasons' for obligating specific data processing activity.

PIPEDA adopts this stance by preventing organizations from requiring users to consent to non-legitimate purposes as a condition of service.[14] This obligation has proven critical in preventing tied selling and in ensuring the over-arching principle of data minimization, as it prevents organizations from over-collection by means of packaging non-essential processing with essential services in a 'take it or leave it' approach. A clear right of refusal would also be beneficial in addressing scenarios where changes to the character and nature of entire privacy regimes are imposed on an entrenched user base.

Article 9 – Exceptions and Restrictions

Article 9 proposes the adoption of an important and beneficial overarching 'necessary measure in a democratic society' qualifier that limits any exception to the general data protection regime to proportionate measures adopted to address legitimate needs aimed at addressing pressing social needs.

In addition to this over-arching qualifier, the Article 9 exceptions could benefit from greater specificity in articulating specific contexts where an exception might be appropriate. Of greatest concern in this respect is the seeming expansion of section 3 of Article 9, which permits exceptions to elements of the data protection regime undertaken for statistical purposes or for the purposes of scientific research where there is 'no risk of an infringement of the rights and freedoms of data subjects.' The removal of 'personal' from the provision, which now applies only to '~~personal~~ data processing', suggests this provision aims at facilitating statistical and research activities based on anonymized data. If this is the case, it should be state much more explicitly than is currently the case. As currently drafted, the provision suggests the opposite, as non-personal or identifiable data would not be subject to the regime in the first place. Currently, the purpose of this provision appears aimed at facilitating so-called 'big data' benefits while bypassing the need to provide citizens with transparent details regarding such

[14] *Personal Information Protection and Electronic Documents* Act, , S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principles 4.3.3: "*An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.*"

practices (Article 7bis), without regard to the sensitivity of the information to be processed (Article 6) and, perhaps most critically, without a right of opposition (Article 8). In place of these critical protections is a more amorphous obligation not to infringe the 'rights and freedoms of data subjects' although, presumably, this obligation already exists. This should be avoided. It is not at all clear that the public benefits of such data processing outweigh the costs in personal privacy. Of greatest concern is the potential inclusion of 'statistical purposes', which is clearly inclusive of commercial analytics and can facilitate a significant amount of online/offline tracking with little clear public benefit.

Second, blanket exceptions in the name of 'public security', 'economic/financial state interests', and 'prevention of criminal conduct', may lead to excessively broad voluntary information disclosures of a type that is not consistent privacy protection in a democratic society. The proposal refers to added clarification that will come in the explanatory report, but in the case of exceptions, it may be better to consider clear and express limits within the scope of the Article itself. As noted in the OECD Privacy Guidelines, exceptions to privacy protection principles, "including those relating to national sovereignty, national security and public policy", should be "as few as possible".[15] As drafted, the proposed amendments would allow data processing for such purposes without regard to the sensitivity of the information (Article 6) and, perhaps most importantly, without the obligation to notify citizens of such processing leads to unauthorized processing (Article 7.2). The latter is critical. Without it, there is no obligation on organizations to notify users or the public of data processing undertaken in the *name* of public security or prevention of criminal conduct, but which is later revealed to have been unauthorized. Finally, it is concerning that data controllers will be permitted to ignore restrictions on retention of citizen data (Article 5.3(d)) in order to facilitate 'public investigations' and in the absence of specific legislative obligations to do so.

Third, the proposed blanket 'freedom of expression' exception raises similar concerns with respect to its scope. It is important to ensure that data protection does not unduly impact on freedom of expression, but it must be kept in mind that in many cases, the parameters of this exception will be determined by organizations without guidance from an objective decision-maker. Private organizations are ill-equipped to make such determinations. The possibility of extending the regime to recognize rights beyond those of 'natural persons' to include those of 'legal persons' (Article 3) is particularly concerning in this context, as it could permit commercial organizations to avoid elements of the data protection regime in the name of 'freedom of expression' even though the expressive value of their commercial expression is low. A more effective approach may be to follow the example in Article 3, which exempts specific private household conduct. Additional contexts that raise specific free expression concerns (such as journalism/news reporting) can be identified.

***** END OF DOCUMENT *****

[15] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Council Recommendation, September 23, 1980, <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>, Part One, paragraph 4.