

**JOINT SUBMISSION TO THE UNIVERSAL PERIODIC
REVIEW OF CANADA**

8 October 2012



APC



**TeleCommunities Canada
Alternatives**

Also endorsed by:

Leslie Regan Shade
Associate Professor, Faculty of Information, University of Toronto

Michael Gurstein, Ph.D.
Executive Director: Centre for Community Informatics Research, Development and Training
(CCIRDT); Editor in Chief: Journal of Community Informatics;
Adjunct Professor: School of Library and Archival Studies

Christopher Parsons, PhD Candidate
University of Victoria, Department of Political Science

Executive Summary

This joint submission has been prepared by the Association for Progressive Communications (APC)¹, the Canadian Internet Policy and Public Interest Clinic (CIPPIC)², OpenMedia.ca³, TeleCommunities Canada⁴, Alternatives⁵ and Web Networks⁶. APC has general ECOSOC consultative status and is concerned with recognition of human rights on the internet as we believe the internet can play a critical role to enhance social and economic development.

This submission focuses on the right to information, privacy and freedom of expression in relation to internet. It highlights areas where Canada is doing well and specific areas of concern. Eight recommendations are made for follow-up and implementation in the UPR process.

A Introduction

1. A special focus on the internet is a key element of this submission. The UPR process includes internet-related human rights issues, such as rights related to culture, information and expression. Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression confirms that Member States' existing human rights obligations⁷ extend to taking steps (including national plans of action) to ensure access to the internet.⁸
2. In July 2012, Canada, along with 84 co-sponsors at the UN Human Rights Council, confirmed the importance of the promotion, protection and enjoyment of human rights on the internet, and in particular, freedom of expression online⁹. We welcome this explicit support from Canada, and look forward to contributing to the continued promotion and protection of human rights in the context of new technology and legislation.
3. This joint submission includes comment on follow up to the first Canadian UPR and is structured as follows:
 - Section B discusses public oversight and transparency in the context of open government data and the *Access to Information Act*.
 - Section C highlights concerns about universal, equitable and affordable internet access; and online content diversity and language.
 - Section D highlights concerns about the right to privacy; online spying, and Bill C-30
 - Section E discusses issues relating to freedom of expression and discrimination online

¹ <http://www.apc.org>; Contact Shawna@apc.org

² <http://www.cippic.ca/>

³ <http://www.openmedia.ca/>

⁴ <http://www.tc.ca/>

⁵ <http://www.alternatives.ca>

⁶ <http://www.web.net/>

⁷ The matters on which they must report in the UPR: Human Rights Council, Institution-building of the United Nations Human Rights Council (18 July 2007, A/HRC/RES/5/1. Affirmed in Resolution A/HRC/RES/16/21).

⁸ Frank La Rue "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (26 April 2011, A/HRC/17/27).

⁹ <http://www.apc.org/en/news/un-recognises-freedom-expression-internet-human-ri>

- Section F makes recommendations for follow up and implementation.

B Public Oversight and Access to Information

4. In its first review, Canada accepted the recommendation made to create or reinforce a transparent, effective and accountable system that includes all levels of government and representatives of civil society, including indigenous people, to monitor and regularly report on the implementation of Canada's human rights obligations.¹⁰
5. Since then, the government has demonstrated an interest in increasing transparency and accountability in governance, through online consultations, engagement with initiatives such as the Open Government Partnership, and the Open Data Pilot Project.¹¹ The Canadian government has also announced plans for a new online pilot project for access to information requests.¹²
6. We commend Canada's efforts to implement this recommendation, using new technologies to reach a diverse group of stakeholders. However, we believe more work is needed to ensure that available information is used to effectively monitor human rights obligations.

B.1 Follow-up to first UPR

7. In its first review, Canada accepted the recommendations made by Portugal and Mexico to “*establish a mechanism that will meet regularly with the effective participation of civil society organizations and indigenous peoples, and have national reach to implement all Canada's international obligations*” and “*facilitate the acceptance of pending commitments and to monitor and publicly and regularly report on the implementation of Canada's human rights obligations.*”¹³ As of its mid-term assessment, Canada had not implemented either of these recommendations.
8. Despite Canada's commitment to transparency and oversight regarding its human rights obligations, very little work has been done to regularly report on the implementation of these obligations. Canada's website for the Universal Periodic Review welcomes comments and recommendations based on the first UPR, but does not report on the implementation of these recommendations.¹⁴

B.2 Freedom of information, transparency and accountability

9. Canada's open data portal, data.gc.ca, provides important datasets that enable analysis of a number of human rights issues, including violence against women and affordable housing. However much of this information is not readily accessible to the general public, and requires intermediary actors, such as media and civil society to summarize and contextualize datasets. It is necessary to examine how online data is being used in practice in order to determine its impact on Canada's wider commitment to transparency and accountability.

¹⁰ A/HRC/11/17 http://www.pch.gc.ca/pgm/pdp-hrp/inter/wrk_grp-eng.pdf

¹¹ <http://www.open.gc.ca/open-ouvert/ap-pa02-eng.asp>

¹² <http://www.cbc.ca/news/politics/story/2012/10/07/access-to-information-online-pilot-project.html>

¹³ UPR-Info Mid-term assessment of Canada, Paras 65, 91

¹⁴ <http://www.international.gc.ca/rights-droits/upr-epu.aspx>

10. Canada's open data pilot project includes datasets from 21 of the more than 200 federal departments. As the project moves forward we hope to see a continued expansion of these datasets, and the number of departments reporting. In particular, publicly funded research data should be made available to ensure that Canada does not lag behind other countries in supporting open access to knowledge.¹⁵
11. In spite of the Canadian government's vocal commitment to transparency and open data, no substantial updates have been made to its outdated *Access to Information Act*¹⁶, which currently ranks 55 out of 92 countries.¹⁷ In recent years, ATI responses appear to have been steadily declining in quality. For example, in the last 5 years, there has been a 49.1% increase in the number of instances where no response was given to ATI requests.¹⁸
12. Canada's Information Commissioner recently launched a dialogue with stakeholders and Canadians on updating the *Access to Information Act*, calling for comprehensive rather than piecemeal changes to the law¹⁹, and periodic, mandatory parliamentary review of the access law.²⁰
13. The Canadian government should consider Comment 34 of the Human Rights Committee on Article 19 of the ICCPR²¹, and update its access to information legislation to take into account the impact and opportunities provided by information and communication technology, including access to the internet, proactive disclosure and two-way communication with citizens.

B.3 Access to online information and community networks

14. As Canada moves towards online government data and services, low broadband access in rural and First Nations communities is a serious concern.
15. Recent research suggests that community networks are important distribution sites for government information, with 64.7 percent of respondents from community networks searching for government information at least a few times per month. This is significant when compared to the Canadian Internet Use Survey, in which only 52 percent of respondents indicated that they had searched for government information during the year.²²
16. We strongly urge the Canadian government to re-launch the Community Access Program (CAP), and support existing community networks in rural and First Nations communities.

C Universal, equitable and affordable internet access

17. The Canadian government should be commended for signing the 2003 Geneva Declaration of Principles, including: "Building the information society: a global challenge in the new millennium which includes commitments to work

¹⁵ <http://theyee.ca/Mediacheck/2012/09/18/Public-Funded-Research-Access/>

¹⁶ R.S., 1985, c. A-1

¹⁷ http://www.oic-ci.gc.ca/eng/modernization-atia_2012_open-dialog-dialogue-ouvert.aspx

¹⁸ <http://www.cbc.ca/news/canada/story/2012/07/06/pol-access-to-information-30th-anniversary.html>

¹⁹ http://www.oic-ci.gc.ca/eng/media-room-salle-media_news-releases-communiques-de-presse_2012_7.aspx

²⁰ <http://www2.macleans.ca/2012/09/28/info-czar-kicks-off-review-of-federal-access-to-information-law/>

²¹ CCPR/C/GC/34 Human Rights Committee 102nd session General comment

²² Clement et al. 2012, p.71; Statistics Canada, 2006

together to improve access to information, infrastructure and knowledge.”²³

18. The key access issues in Canada are: limited access (low internet penetration particularly outside main centres), high costs, inadequate broadband infrastructure, and the absence of an integrated strategy for harnessing the potential of the internet for social, cultural, economic and political development.

C.1 Internet penetration in Canada

19. Canada has one of the highest rates of internet usage in the world, and has seen marked improvement in internet penetration over the last decade²⁴. However, while Canada has improved its penetration rates since 2000, it has dropped quite dramatically in global rankings over that same period of time. In 2002, Canada ranked 2nd globally in penetration rates - by 2011 it had dropped to #13 globally with only 32 subscriptions per 100 households.²⁵
20. The coalition commends the Government of Canada's Broadband Program for bringing internet access to a total of 218,000 new Canadian households between 2009 and 2012, many of which are in rural communities.²⁶ However we are concerned because funding has ended for both this program, and the Community Access Program (CAP), as of March 31, 2012.²⁷ CAP operated in over 3,000 sites across Canada, offering computer literacy trainings and Internet-user skills for youth, seniors, members of low-income communities and residents of rural and remote regions²⁸.
21. Industry Canada stated that in the context of “challenging fiscal times,” \$15 million in funding for CAP was terminated because the program had “successfully achieved its objective.”²⁹ However, the digital divide persists in Canada, particularly among First Nations communities.

C.2 Digital Divide: First Nations communities

22. Broadband internet penetration is particularly low among First Nations communities. In 2007, 64% of Canadian urban communities and small towns and close to 50% of remote communities had access to some form of broadband service (DSL, cable or wireless). In comparison, only 17% of First Nations communities had broadband access in 2007.³⁰
23. Cost is a major obstacle to internet access in First Nations communities, with recent research suggesting that costs to access broadband in Nunavik and Nunavut are up to three to five times higher than in urban centres in southern Canada, with download capacity only a fraction of what is available in the urban south.³¹

²³ <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

²⁴ <http://www.internetworldstats.com/am/ca.htm>

²⁵ 10.2 subscriptions per 100 households, behind only S. Korea at the time: OECD, “Six Year Historical Time Series: Penetration” December 2011, Broadband Portal:

<http://www.oecd.org/internet/broadbandandtelecom/oecdbroadbandportal.htm>

²⁶ <http://www.ic.gc.ca/eic/site/719.nsf/eng/home>

²⁷ <http://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/03127.html>

²⁸ <http://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/03127.html>

²⁹ <http://www.cbc.ca/news/technology/story/2012/04/06/ns-cap-funding-cut.html>

³⁰ <http://www.cli-ica.ca/en/about/about-cli/indicators/be-internet.aspx>

³¹ McMahon et al., 2011 Digital Divides and the 'First Mile'.

24. Failure to adequately reach First Nations communities is in part the result of non-inclusive policy by the Canadian government. In 2009-10, the Canadian government announced the development of a national digital strategy, but did not refer to the specific contexts of on- and off-reserve First Nations, Inuit, and Métis communities in its formal consultations.³² Research from First Nations communities in Northern Ontario suggests that community-based online network development is essential for effectively increasing access and use of the internet in these areas.³³
25. As the Working Group report from the 2009 UPR of Canada discusses, violence against women in First Nations communities is a serious concern.³⁴ Access to the internet is also an important tool in addressing women's human rights issues, including violence against women. Research from India, Pakistan and the Philippines suggests that online tools such as blogs and social networking sites provide a much needed space for women who have experienced domestic violence to share their experiences, and develop a support network. Access to social networking sites allow women to push the boundaries of cultural and social barriers that place intense scrutiny on the sexuality and mobility of women and girls.³⁵ In Canada, programs have been developed to provide support for digital storytelling by women in First Nations communities, including experiences of Residential Schools.³⁶
26. We recommend that the government support and expand existing social network and digital story telling programs for women in First Nations communities.

D Right to privacy and Bill C-30

27. According to George Radwanski, former privacy commissioner of Canada, “the fundamental right of privacy in Canada is under assault”³⁷ - and has been for over a decade. Internet and new technologies have made way for unprecedented surveillance of individuals. Under the pretext of fighting terrorism and cybercrime, Canadians have seen their right to privacy of personal information consistently decline.³⁸
28. In 1971, the Government of Canada acknowledged the right to communicate and the right to privacy as a basic human right, and consensus that a legal concept of “invasion of privacy” should be introduced in provincial and federal law, granting Canadians the right to communicate privately, and to disconnect at will. Today, Canadians have the right to physical privacy, freedom from surveillance, freedom from monitoring or interception of their private communications and freedom from the collection, use and disclosure

³² McMahon et al., 2011 Digital Divides and the 'First Mile'.

³³ Bell et al. 2012 in *Connecting Canadians? Investigations in Community Informatics*, eds. A. Clement, M. Gurstein, G. Longford, M. Moll, L.R. Shade (Edmonton, AB: Athabasca University Press):250

³⁴ Final report of Working Group A/HRC/11/17. Paragraph 11

³⁵ SM Kee, Moolman, 2011. Sexuality and women's rights <http://www.giswatch.org/en/2011>

³⁶ http://www.pwhce.ca/program_aboriginal_digitalStories.htm

³⁷ 2008. Reconsidering the Right to Privacy in Canada. *Bulletin of Science, Technology & Society* 28(1): 80-91.

³⁸ Diebert, 2011. Towards a cyber security strategy for global civil society? <http://www.giswatch.org/en/2011>

of their personal information.³⁹ Although qualifications on these rights are permitted under the Canadian Charter of Rights (where justifiable in a free and democratic society), current technological advances have led to discussions about the tension between privacy and protection of public security. New legislation, namely Bill C-30 could give the Canadian government carte blanche to overlook the fundamental right to privacy in its varying expressions.

D. 1 Bill C-30 – Lawful access legislation

29. On February 14th 2012, the Canadian Government introduced Bill C-30.⁴⁰ This bill enhances Canadian authorities' capacity to "lawful interception of communications and the lawful search and seizure of information, including computer data."⁴¹ This bill gives law enforcement agencies the power to legally obtain names, unlisted phone numbers and IP addresses from internet and telecommunications service providers (ISPs and TSPs) without a warrant,⁴² and imposes gag orders on TSPs who comply with lawful access powers.⁴³ There is huge potential for this to be used in a manner that expands the State's surveillance capacity: enabling authorities to more intimately understand the relationships between Canadians.²⁰ It also allows police to identify any anonymous online activity, posing a direct threat to anyone expecting non-conventional comments made on blogs, online newspaper articles, etc., to remain private.⁴⁴
30. Bill C-30 is still vague as to what "prescribed identifying information" is, and would be developed after the legislation was passed. This is particularly concerning with regards to legislation affecting citizen's privacy, and surveillance in general. "Deferring what constitutes 'prescribed identifying information' to the regulation phase prevents citizens from knowing what identifiers the state wants to use to track and identify citizens."²⁰ As the Bill will permit police to match any 'prescribed information' to identifiers such as name and address at will, what is ultimately included in this general category can have dramatic implications for the privacy of citizens. For example, if mobile phone identifiers are included, police will, without a warrant, be able to track the location and movements of Canadians.⁴⁵
31. The obligation to disclose identifiers such as IP addresses and email addresses without a warrant is troubling. Identifiers such as these are left behind like traceable footprints as a natural by-product of most online activity. The ability to link this data with other personal data could open the door to detailed profiling of identifiable individuals. Given its potential sensitivity, the decision to require disclosure without any oversight should raise concerns within the Canadian privacy community.⁴⁶

³⁹ Shade, Leslie Regan. "Reconsidering the right to privacy in Canada", 2008, p.83

⁴⁰ <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=5375610>

⁴¹ <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>

⁴² <http://www.cippic.ca/en/lawful-access-faq>

⁴³ <http://www.christopher-parsons.com/blog/technology/the-issues-surrounding-subscriber-information-in-bill-c-30/>

⁴⁴ http://www.cippic.ca/sites/default/files/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf

⁴⁵ <http://blog.privacylawyer.ca/2012/02/what-lawful-access-is-all-about.html>

⁴⁶ <http://www.michaelgeist.ca/content/view/6320/125/>

32. The bill requires ISPs to dramatically re-work their networks to allow for real-time surveillance and establishes new requirements for all Canadian ISPs, such as the power to intercept communications, to isolate the communications to a particular individual, and to engage in multiple simultaneous interceptions. In addition to ISPs, the bill seeks to apply these obligations to a broad range of online services, including Facebook, Twitter, and others. The bill establishes reporting requirements - all within six months of the bill taking effect. The bill also establishes numerous reporting requirements including mandating that all Internet providers disclose their technical surveillance capabilities within six months of the law taking effect. Follow-up reports are also required when providers acquire new technical capabilities.
33. Implementing the bill will also cost some 80 Million dollars (CAD)⁴⁷, which will ultimately be taken on by the Canadian public, either through increased service costs by the ISPs and TSPs, or, should the Canadian government offer financial assistance to the service providers, through taxpayer dollars. Providers will likely also be able to charge fees for complying with law enforcement requests.⁴⁸

E Freedom of Expression

34. Freedom of expression is an enabling right and a cornerstone of democracy. We commend the Canadian government for its work in protecting freedom of expression online, including its recommendation to Kyrgyzstan to take measures to ensure the right to freedom of expression, including guaranteeing unhindered access for independent media to airtime and the internet.⁴⁹ However the proposed Bill C-30, and new tensions around hate speech online require Canada to demonstrate its strong commitment to freedom of expression domestically as well as internationally.

E.1 Bill C-30

35. Although already discussed in the context of right to privacy, the proposed bill also has implications for freedom of expression online. By allowing Canadian authorities to easily access Canadians' online activities, the Bill C-30 places limitations on the internet as a space for open expression of ideas and opinions, debate and criticism. The ability to identify anonymous online speakers at will poses a particularly poignant threat to non-mainstream political and other online discussion forums.

E.2 Hate speech and discrimination online

36. Recent cases of hate speech and religious intolerance online have sparked increased debate in many countries over appropriate restrictions to freedom of expression online. In September 2012 an anti-Muslim YouTube video sparked violence in Libya and Egypt. In response, Google blocked access to the video in the two countries, claiming exceptional circumstances.⁵⁰

⁴⁷ <http://www.cbc.ca/news/politics/story/2012/02/22/pol-lawful-access-costs.html>

⁴⁸ <http://www.michaelgeist.ca/content/view/6316/125/>

⁴⁹ A/HRC/15/2 Report of the Working Group on the UPR of Kyrgyzstan, Paragraph 76.82

⁵⁰ <http://www.nytimes.com/2012/09/14/technology/google-blocks-inflammatory-video-in-egypt-and-libya.html>

37. In its first review, Canada accepted the recommendation made by Pakistan to “Apply provisions of its hate-speech law in a non-selective manner to cover all acts and incidents that may lead to incitement to racial and religious hatred and violence”.⁵¹ We encourage Canada to note recent statements made by the Special Rapporteur on Freedom of Expression on this issue, including the importance of protecting human rights online and offline.
38. With regard to technical measures taken to regulate types of prohibited expression, such as the blocking of content, the Special Rapporteur on Freedom of Expression has reiterated that “States should provide full details regarding the necessity and justification for blocking a particular website and that the determination of what content should be blocked must be undertaken by a competent judicial authority or a body that is independent of any political, commercial or other unwarranted influences in order to ensure that blocking is not used as a means of censorship.”⁵²

E.3 Defamation and copyright as limits to online speech

39. . The Special Rapporteur has similarly warned against the potentially harmful effects on free expression that can result from overly aggressive use of online intermediaries as tools of enforcing private rights:

*[...] given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by over-censoring potentially illegal content. Lack of transparency in the intermediaries’ decision-making process also often obscures discriminatory practices or political pressure affecting the companies’ decision [...] The Special Rapporteur emphasizes that censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals’ human rights*⁵³

40. The Supreme Court of Canada’s recent decision in *Crookes v. Newton*⁵⁴ with regards to online hyperlinking to defamatory material, suggests that Canadian courts recognise this risk, and support maintenance of an open internet. We recommend that the federal government adopt the approach taken in the judicial decision of *Crookes v. Newton* to protect freedom of speech of downstream users, and ensure that internet intermediaries do not engage in online censorship.⁵⁵

⁵¹ A/HRC/11/17 Report on Working Group for the UPR of Canada, Para 86.23

⁵² Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression <http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf>

⁵³ http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

⁵⁴ <http://www.canlii.org/en/ca/scc/doc/2011/2011scc47/2011scc47.html>

⁵⁵ <http://www.slaw.ca/2011/11/02/crookes-v-newton-speculations-on-intermediary-liability/>

F Recommendations

We recommend that the Government of Canada:

F.1 Access to Information and Public Oversight

41. Follow up on its commitment to regularly report on the implementation of human rights obligations, including updating online information on the Government of Canada website.
42. Update the federal *Access to Information Act* in consultation with civil society and First Nations communities, taking into account the impact of new technology.
43. Provide specific support for the uptake and dissemination of online government data by citizens, media and civil society, and continue to develop the federal Open Data project by releasing new datasets and expanding the number of departments reporting.

F.2 Universal, equitable and affordable internet access

44. Acknowledge the critical importance of universal access to the internet as a facilitator of civil and political and economic, social and cultural human rights.
45. Provide funding and support for community networks and access programs in order to complement new online government services and to ensure fairness and equality in access to online services for all Canadians.
46. Work with local communities to expand internet access in rural areas, and develop a national digital strategy that refers to specific contexts of on- and off-reserve First Nations, Inuit, and Métis communities, including expansion of existing social network and digital story telling programs for women in First Nations communities.

F.4 Freedom of expression, the right to privacy and regulation of interception of communications

47. Continue to uphold freedom of expression in Canada by withdrawing the proposed Bill C-30, and any proposed legislation that jeopardises the privacy and security of online users.
48. Develop and implement best practices in domestic response to hate speech and discrimination online, on the basis of recommendations made by the Special Rapporteur on Freedom of Expression.