SUBMISSION BY INTERNET SOCIETY CANADA CHAPTER IN THE PUBLIC SAFETY CANADA AND THE DEPARTMENT OF JUSTICE *CONSULTATION ON NATIONAL SECURITY*

15 DECEMBER 2016

Table of Contents

1.0 Introduction

1. Internet Society, Canada Chapter[1] ("ISCC") is hereby making its submission in the Public Safety Canada and Department of Justice consultation on national security. ISCC is a volunteer association that seeks to advance the cause of the Internet in Canada. ISCC is a chapter of the international Internet Society[2] ("ISOC"), which is a non-governmental organization that "engages in a wide spectrum of Internet issues, including policy, governance, technology, and development."[3] ISCC has prior and ongoing participation in other government initiated consultations including Global Affairs Canada's Canadian International Assistance Review Consultations, the Canadian Heritage consultation regarding Canadian content in a digital world and Public Safety Canada's cyber security consultation.

2. Some of ISOC's work, in which ISCC participates and that it supports, includes:

- "Championing public policies that enable open access;
- Facilitating the open development of standards, protocols, administration, and the technical infrastructure of the Internet;
- Organizing events and opportunities that bring people together to share insights and opinions."[4]

A complete list of ISOC's mission can be found at http://www.internetsociety.org/who-we-are/mission.

3. The policies that will be influenced by this consultation must strike a delicate balance between Canadian rights, values and freedom on one hand and the safety and security of the nation and its citizens on the other. Achieving the right balance for the year 2017 and beyond must start with meaningful input from all stakeholders. This consultation is therefore the appropriate first step towards laws and policies that reflect and protect what it is to be Canadian. For this reason, ISCC applauds Public Safety Canada and the Department of Justice's initiative to seek public input on national security laws and policies. Few areas of policy evoke stronger, more passionate

---

1 Internet Society, Canada Chapter, "ISOC Canada", <http://www.internetsociety.ca/>.
2 Internet Society, "Internet Society", <http://www.internetsociety.org/>.
3 Internet Society, "What We Do", <http://www.internetsociety.org/what-we-do>.
4 *Ibid.*

responses. ISCC therefore expects the present consultation to elicit diverse, thoughtful and innovative submissions that will assist our government in shaping balanced and effective policies.

4. ISCC has reviewed Green Paper entitled "Our security, Our Rights"[5] (the "Green Paper") and is encouraged by the approach that the government has taken in identifying the most prominent national security issues and challenges that need to be addressed going forward. The Green Paper served as background to frame a discussion that occurred at a conference that ISCC held on October 28, 2016 in Ottawa. Individuals from a variety of backgrounds attended the conference both in-person and remotely from across Canada. The conference was structured as a moderated discussion of the chapter of the Green Paper that was most relevant to ISCC's mandate: investigative capabilities in a digital world.[6] The discussion was divided into four parts and each part was dedicated to one of the four main problems, as identified by the Green Paper, that investigators face in a world characterized by a rapid pace of new technology and ever evolving threats:

1. Slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time;
2. The lack of a general requirement that domestic telecommunications networks maintain the technical ability to intercept messages;
3. The use of advanced encryption techniques that can render messages unreadable; and
4. Unreliable and inconsistent retention of communications data.

5. This submission synthesizes the input of conference participants on each of the above-listed topics. In some cases, participants were able to reach a general consensus on a position, idea or proposal. In other cases, the room was divided and unable to reconcile conflicting opinions and perspectives within the limited time assigned to the topic of discussion. ISCC submits that non-consensus positions at the conference described in this submission emphasize the need for a carefully nuanced approach to policy making.

---

5 "Our Security, Our rights", National Security Green Paper, 2016.
6 *Id.*, at p.18.

6. The balance of this submission is divided into four sections dedicated to each of the above-listed problems associated with investigative capabilities in the digital world. Part 6.0 of this submission sets out ISCC's conclusions and a summary of recommendations.

2.0 Basic Subscriber Information

7. The Green Paper sets the basic context for the challenges surrounding law enforcement access to basic subscriber information, such as phone numbers or Internet Protocol ("IP") addresses.[7] Fundamentally, these challenges stem from the tension between: (a) law enforcement's interest in obtaining timely and accurate information to assist in ongoing investigations and enforcement activities; and (b) the privacy rights of subscribers. As further explained by the Green Paper, Canadian courts have recently decided in favour of reinforcing the need for appropriate safeguards around basic subscriber information. Indeed, in 2014, the Supreme Court of Canada in *R v. Spencer*[8] imposed strict boundaries on law enforcement's general investigative powers under the *Criminal Code*[9] and the lawful authority exceptions provided under the *Personal Information Protection and Electronic Documents Act*[10] regarding the disclosure of basic subscriber information.[11] It bears noting the Court's precise finding that privacy rights are associated with basic subscriber information. Justice Cromwell, writing for the court stated:

> "In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search."[12]

8. In light of the *R v. Spencer* decision and in the absence of any clear laws articulating rules and process for obtaining access to basic subscriber information, it is not surprising that law enforcement is struggling to obtain such information in a timely and effective manner. Participants at the ISCC conference were sympathetic to the obstacles faced by law enforcement agencies and agreed that tools ought to be available to allow reasonable and timely access to basic subscriber

---

7 *Ibid.*
8 *R. v. Spencer*, 2014 SCC 43. (*"R v. Spencer")*
9 S. 487.014(1) of the *Criminal Code*, R.S.C., 1985, c. C-46.
10 S. 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5.
11 *R v. Spencer.* at paras 68-73.
12 *Id.* at para 66.

information that could meaningfully assist with an ongoing investigation. However, such tools should not come at the expense of the reasonable expectation of privacy of basic subscriber information that was recognized and protected in *R v. Spencer*. Accordingly, any tools and measures intended to improve timely access to basic subscriber information must be carefully calibrated to prevent potential abuses of such information by law enforcement agencies.

9. ISCC recommends the creation of a graduated scale that sets out different procedural and evidentiary requirements for access to basic subscriber information depending on factors including: the likelihood that a crime has been committed or will be committed, the severity of the alleged crime, time sensitivity and urgency of disclosure (i.e., is there a threat of imminent harm?) and other relevant considerations. Procedural and evidentiary requirements should be relaxed towards the end of the scale that is characterized by an urgent need for access to information. Conversely, stricter procedural and evidentiary requirements that are in line with traditional warrant applications should apply in situations where access to basic subscriber information in a timely manner is less of a concern. Overall, the basic idea of this scaled approach is to provide law enforcement with more expedited and streamlined access to basic subscriber information in situations where time is of the essence.

10. If the government decides to apply the model described in the preceding paragraph or any other measures intended to facilitate law enforcement access to information involving a reasonable expectation of privacy, safeguards must be imposed to prevent potential abuses. For instance, a law enforcement agency's use of basic subscriber information should be strictly limited to uses that are necessary to further the investigation that led to the collection of the information. For additional certainty, authorized law enforcement recipients of basic subscriber information must be prohibited from disclosing such information internally within their organizations or to other government organizations for purposes not related to the primary investigation pursuant to which the information was obtained.

11. Although participants at the ISCC conference were inclined to recommend carefully calibrated tools that could improve investigative capabilities, many in attendance were concerned by the public's general lack of trust towards government and law enforcement agencies. Participants referred to information leaks by Communications Security Establishment and the Canadian Security Intelligence Service as notable breaches of trust that have harmed public

perceptions dramatically. Such sentiments are also compounded by increasing incidence of racially charged conflicts involving police in the United States.

12. In light of the above, ISCC recommends that government deploy a strategy to regain public trust in authority and law enforcement. ISCC submits that an important pillar of this strategy must be improved oversight, transparency and accountability with regards to government and law enforcement's access to the private information of Canadians. Canadians need reassurance that an overseer is actively ensuring that reasonable expectations of privacy are protected in accordance with the law. Governments, law enforcement agencies and private companies that misuse information that is of a private nature, whether by reason of carelessness or otherwise, must be held publically accountable. In the interest of transparency, Canadians should also be entitled, subject to reasonable limitations, to a summary description of the information held by government organizations and law enforcement that is associated with their name.

13. In ISCC's view, all of the above can be achieved by minimal legislative amendments. In fact, the core oversight functions described above are already within the mandate of the Office of the Privacy Commissioner ("OPC") and its provincial and territorial counterparts. Unfortunately, however, perhaps due in part to a lack of resources, these agencies have yet to make a meaningful impact in terms of preventing abuses and holding major parties, including government, accountable for misuses of information involving a reasonable expectation of privacy. Accordingly, ISCC submits that government should consider means to expand the powers and resources of these privacy oversight agencies so that they can fulfill the role of overseer and rebuild public trust and confidence. In particular, the government should ensure that these agencies are capable of acting proactively rather than reactively. Furthermore, where sanctions are warranted, these agencies must have the legislative authority to impose appropriate consequences that will promote deterrence.

14. Until public trust can be regained, even carefully calibrated investigative tools involving access to private information, like basic subscriber information, will be generally opposed due to the public perception that such tools are more likely to hinder rather than further justice. For this reason, ISCC urges Public Safety Canada and the Department of Justice to consider broader long term strategies that respond to the needs and concerns of Canadians. ISCC firmly believes that one

such forward looking strategy would be to empower the OPC and to encourage similar empowerment of provincial and territorial privacy oversight agencies.

3.0 Intercept Capability

15. The Green Paper describes the ability to intercept communications as "…a valuable tool in national security and criminal investigations".[13] However, the Green Paper also explains that this tool is sometimes unavailable to law enforcement agencies because communications providers do not maintain the technical capability to comply with court orders for interceptions of communications.[14] As a consequence, the Green Paper notes that key intelligence and evidence can be missed.[15]

16. Based on the above context, participants at the ISCC event explored whether it would be appropriate to require providers of communications services to deploy equipment to enable the capability of intercepting communications. Participants reached a general consensus that such a requirement would be acceptable pursuant to two conditions. First, providers of communications services must be compensated for the cost of acquiring and installing the equipment that is necessary to intercept communications that are transmitted on their networks and for engaging in interception activities. Second, communications providers must be subject to a strict set of requirements that are intended to ensure that interception capabilities are only utilized to comply with court orders. Both of these conditions are addressed in greater detail below.

17. Equipment that enables the interception of communications is extremely expensive. While this equipment and related processes might constitute a negligible expense for the national incumbent telecommunications service providers with annual revenues in the billions of dollars, the cost of interception equipment is prohibitively expensive for smaller telecommunications providers. If smaller providers are compelled to acquire such equipment at their own expense, even on a timeline of multiple years, many companies would be forced into bankruptcy. More broadly, all smaller providers would struggle to compete with larger companies that enjoy the size and scale to comfortably absorb significant and unforeseen operating costs. Furthermore, the costs that are

[13] Green Paper, at p. 19.
[14] *Ibid.*
[15] *Ibid.*

imposed by way of legislation are bound to be passed on to Canadian consumers by way of increased retail prices for telecommunications services.

18. All of the above consequences would substantially prevent and lessen competition in the Canadian markets for telecommunications services. For these reasons, any legislated requirement for communications providers to deploy interception equipment and processes to comply with court orders must be accompanied by a compensation regime to ensure that providers are compensated for one-time implementation costs and ongoing maintenance costs associated such requirements. Although ISCC is primarily concerned with the harms faced by smaller communications providers and the resulting consequences for competition and consumers, the government should be aware of the telecommunications Policy Direction which requires that the Canadian Radio-television and Telecommunications Commission apply regulatory measures in a manner that takes into account principles of technological and competitive neutrality.[16] Therefore, in accordance with principles of technological and competitive neutrality, it would be appropriate to compensate all communications providers for one time and ongoing equipment and process costs to enable compliance with court orders.

19. In addition to a compensation regime, a legislated requirement for communications providers to provide intercept capabilities must be accompanied by strict rules governing the use of such equipment. ISCC is concerned that communications providers will have strong incentives to utilize communications interception technologies for commercial purposes. In order to prevent this potential for misuse, a specific set of guidelines should be established by statute or regulation to prescribe the manner and circumstances in which interception capabilities can be utilized by a communications provider. Government might also wish to consult with the communications industry to explore technical means of preventing misuse of interception equipment.

20. ISCC also recommends the introduction of substantial statutory damages associated with a communications provider's use of interception capabilities in a manner that is not authorized by court order or in accordance with the prescribed guidelines. Doing so will send a signal to the industry that the misuse of interception capabilities is not acceptable. Statutory damages are a

[16] Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives, P.C. 2006-1534, 14 December 2006, SOR/2006-355, Canada Gazette Part II, Vol. 140. No. 26, 27 December 2006 ("Policy Direction").

particularly strong deterrent given that they clearly set out a range of liability for parties that otherwise face strong incentives to breach the law.

4.0 Encryption

21. Many participants at the ISCC event were concerned by the tone and focus of the paragraph of the Green Paper[17] dedicated to the topic of encryption. For ease of reference, the Green Paper stated the following:

> "Encryption technology is a tool that can be used to avoid detection, investigation and prosecution. After investigators get the proper legal authorizations and make a successful interception or seizure, the information obtained may be indecipherable due to encryption. And there is currently no legal procedure designed to require a person or an organization to decrypt their material."[18]

22. Evidently, the Green Paper takes the position that encryption is simply an inconvenience for investigations and prosecutions. This is a one-sided perspective that overlooks the many critical applications of encryption in today's digital world. Indeed, the intent of encryption is to prevent unauthorized access to sensitive data. For instance, encryption is vital to the protection of personal information on electronic devices and in the cloud. Encryption also lies at the foundation of the digital economy and enables the online transactions which sustain it. Without encryption, all our voice, video, email and text communications would be exposed to eavesdroppers.

23. Encryption has become essential to our daily lives. As a result, industry and government should collaboratively seek to innovate and improve encryption standards rather than weaken them. Notwithstanding, the concern articulated in the Green Paper is also valid. It is true that encryption can sometimes impede an investigation that requires access to encrypted information. It is also true that access to such decrypted information can also be required on a time sensitive basis.

24. The challenge therefore becomes finding a way to continue to strengthen encryption while providing authorities with timely access to decrypted information, without circulating decryption keys, embedding backdoors or using other measures that could be exploited by third parties. Unfortunately, a clear solution has yet to present itself. Participants at the ISCC event were unable

[17] Green Paper, at para 19.
[18] *Ibid.*

to reach consensus on whether the progressive improvement of encryption or the interests of law enforcement should take priority in the interim.

25. Ultimately, the ISCC recommends that the government commission research towards a technical solution that enables law enforcement to access decrypted information pursuant to a court order, without undermining the level of protection afforded by the encryption. In particular, ISCC recommends funding research programs through the University of Waterloo's Centre for Applied Cryptographic Research.

5.0 Data Retention

26. According to the Green Paper, the fact that there is no general requirement for communications providers to retain phone and Internet records is yet another obstacle to investigators and prosecutors.[19] The Green Paper goes on to explain that some communications providers delete such information almost immediately while others use it for their own commercial purposes, and then destroy it.[20]

27. Much like the Green Paper's perspective on encryption[21], its perspective on data retention practices is attuned to the concerns of investigators and prosecutors but overlooks opposing interests which favor minimal data retention requirements. There are indeed very legitimate reasons supporting little or no data retention requirements. Most notably, data retention obligations increase the likelihood of a security breach or misuse of sensitive information. By their very nature, data retention requirements subject sensitive information to the risk of unauthorized access or accidental data leaks for set periods of time that extend far beyond what most communications providers would accept in the absence of data retention laws.

28. Anonymizing or deleting customer data when there is no longer a legitimate commercial purpose for that information are measures that are very effective at protecting customer privacy. Any data retention obligations would therefore undermine an important tool that communications providers apply to protect their customers and also themselves from major sources of liability.

---

[19] Green Paper, at para 19.
[20] *Ibid.*
[21] *Ibid.*

29. ISCC is also concerned that data retention requirements will provide communications providers incentives to commercialize data throughout the applicable retention period. For example, a communications provider that is required to keep data might attempt to offset the cost of retaining the information by selling related metadata to an advertising company or data mining agency. In ISCC's view, the government should avoid statutory requirements that encourage ulterior uses of customer information.

30. If, despite the concerns raised above, government determines that data retention requirements are necessary, ISCC recommends the adoption of short retention periods. Data retention requirements should also stipulate different retention periods for different categories of information, based on the sensitivity of that information. More specifically, retention periods should be reversely proportionate to the sensitivity of a category of information. For example, Germany recently passed new data retention laws that prescribe a retention period of 10 weeks for call detail records and metadata and a retention period of 4 weeks for cell phone location data.[22] A similar targeted approach in Canada could be applied to limit the aforementioned exposure to exploitation that is associated with mandatory retention periods.

31. ISCC expects that other streamlined investigative capabilities, such as the recommended approach for access to basic subscriber information detailed in Part 2.0 of this submission, will expedite the process for accessing information that is pertinent to an ongoing investigation. Consequently, improved timeliness of investigative access will obviate the need for unnecessarily long retention periods.

32. If any mandatory data retention periods are implemented, ISCC reiterates the need for effective oversight. Fully resourced privacy oversight agencies could ensure that both law enforcement and communications providers stay onside of privacy laws. These agencies could also collect data over time to assess the appropriateness of prescribed data retention periods for various categories of information. For example, it would be helpful to understand to which extent data retention periods have furthered investigations that led to a conviction. Conversely, it would also be helpful to understand any linkage between mandatory retention periods and data breaches.

[22] https://lawfareblog.com/german-bundestag-passes-new-data-retention-law.

Based on the assessment of these agencies, data retention periods could be adjusted as necessary on an annual or biennial basis.

6.0 Conclusion

33. As noted at the outset of this submission, the policies that will be influenced by this consultation must strike a delicate balance between Canadian rights, values and freedom on one hand and the safety and security of the nation and its citizens on the other. The Green Paper accurately pinpoints several areas where investigative capabilities are frustrated by technology and / or the company policies and business practices of communications providers. ISCC would like to remind Public Safety Canada and the Department of Justice that there are often very legitimate and important reasons underpinning these perceived obstacles to investigations and prosecutions. The federal government must be aware and responsive of the public interests at play.

34. Investigative capabilities could be enhanced by a graduated scale that relaxes procedural and evidentiary requirements needed to support an application for access to basic subscriber information in proportion to time sensitivity considerations and other factors. However, access to basic subscriber information should be subject to strict controls and oversight. Enhanced oversight is particularly important to restore public trust in government and law enforcement. ISCC recommends providing the OPC and its provincial and territorial counterparts with the resources and tools needed to be proactive and impose real consequences upon parties who breach privacy laws.

35. If communications providers are compelled to implement interception capabilities on their networks, a compensation regime must be implemented to allow providers to recover onetime and ongoing costs related to interception. Otherwise, smaller communications service providers will be disproportionately affected by increased operational costs. In turn, competition will be substantially lessened and prevented in Canadian markets for retail telecommunications services. The absence of compensation would also inevitably lead communications providers to pass on the cost of interception capability to consumers via price increases to retail services and products. Finally, strict rules should govern the use of interception technology and statutory damages should apply to breaches of such rules.

36. Encryption is essential. Industry and government should collaboratively seek to innovate and improve encryption standards rather than weaken them. However, authorities also need access to decrypted data to further investigations. ISCC recommends that the government commission research towards a technical solution that enables law enforcement to access decrypted information pursuant to a court order, without undermining the level of protection afforded by the encryption. To this end, a funded project with the University of Waterloo's Centre for Applied Cryptographic Research should be considered.

37. While data retention might assist investigations, it also exposes sensitive information to various risk factors. Anonymizing or deleting customer data when there is no longer a legitimate commercial purpose for that information is a crucial tool for protecting customer privacy. If, notwithstanding, it is determined that data retention periods are necessary, short retention periods should be applied. Even shorter retention periods for particularly sensitive data should also be considered. Fully resourced privacy oversight agencies would have an important oversight role with respect to data retention. They could also be tasked with collecting data that could be used to adjust data retention periods on an annual or biennial basis, as necessary.

38. ISCC thanks Public Safety Canada and the Department of Justice for the opportunity to participate in this consultation.