Canadian Multistakeholder Process: Enhancing IoT Security

Report on third multistakeholder meeting

Location: Toronto, Canada
Date: September 5, 2018
In-Person Attendance: ~35
Remote Attendance: ~15
Total Attendance: ~50
Livestream Link: https://livestream.com/internetsociety/iotsecurity2018-3

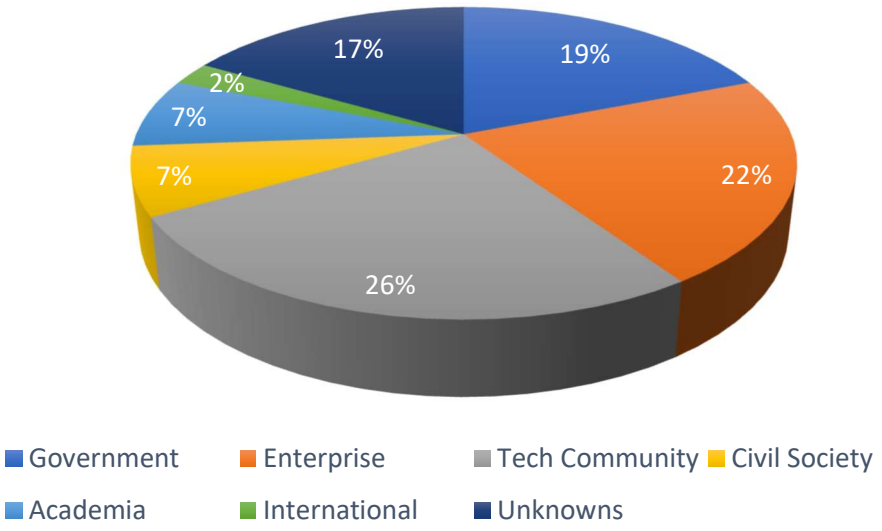
Overview:

The Canadian Multistakeholder Process – Enhancing IoT Security is a year-long process to develop recommendations for a set of norms and/or policies to secure IoT in Canada. Events throughout the year will serve as an opportunity to begin planning and implementing a bottomup, organic process to remedy existing and potential security challenges in Canada's national IoT ecosystem.

This initiative is a partnership between the Internet Society, Innovation, Science and Economic Development, the Canadian Internet Registration Authority, CANARIE, and CIPPIC. The Canadian Chapter of the Internet Society is also assisting in this effort.

The goal of the third multistakeholder meeting was to receive reports from the three working groups (on consumer education & awareness, labelling and network resiliency) created at the second meeting. To this end, the meeting was spent hearing short presentations from each working group, followed by a longer discussion aimed at identifying and refining key messaging within the group's research objectives. The results of this discussion will serve as the basis for the next meeting.

At this meeting, the following stakeholders were represented:



Opening Remarks (2:00 – 17:59):

The meeting opened with remarks from Dr. Ann Cavoukian, a distinguished expert-in-residence at the Privacy by Design Centre of Excellence and the former Information and Privacy Commissioner of Ontario. She developed Privacy by Design (PbD) in the late 1990's and it was unanimously passed as landmark legislation in 2010 by a gathering of international data protection and privacy commissioners.

Dr. Cavoukian emphasized that privacy is not synonymous with security, but allows the freedom to control personal security. PbD advocates for thorough, preemptive security measures to be embedded into the code of connected devices before breaches and subsequent lawsuits occur. Cavoukian advocated for ditching a zero-sum attitude towards privacy and explained that privacy and innovation are not mutually exclusive. "Privacy should be viewed as a business issue," she says, "not a compliance issue." In short, securing customer privacy also ensures customer retention.

Throughout the meeting, she also advocated for the burden of responsibility to be on the manufacturer and not the consumer, identifying a huge trust deficit with 91% of people polled admitting that they are concerned about their privacy.

Stakeholder Rules & Reminders (18:00 – 22:41):

Next, facilitator Martin Botterman, GNKS Consult, reviewed the multistakeholder rules of engagement as established at the first multistakeholder meeting on April 4. He also reminded stakeholders that the next in-person meeting is slated for November 20.

Consumer Education & Awareness Presentation (22:42 – 1:13:20):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/06/Multistakeholder-Meeting-2-Report.pdf (Page 4)

Description:

Volunteer leader Rouba Alfattal (OCA—ISED) presented on the working group's current status. She reported that since the second multistakeholder meeting, the working group had met online on August 13 and had a number of communications in-person and on Slack. Based off of the input from those communications, the group narrowed their mandate to:

1. Leverage expertise to identify key messages and gaps; and
2. Provide an initial assessment and consolidation of the list of draft messages that may be useful to help educate consumers about the risks of IoT devices.

With this in mind, the group identified three priority areas, privacy, security, and functionality. These terms were defined across three time periods, before purchase, after purchase, and at-problem—or when an issue arises (*See Appendix B for the Messaging Matrix*). Key messages were developed for each of these areas, highlighting factors that consumers ought to be aware of or inquire about. She noted that these messages applied to what they called dumb consumer devices – vulnerable IoT devices that people would typically find in a home or small business.

Through the group's efforts, a number of gaps were identified throughout the course of creating the messaging matrix. The first was with respect to where the **At-Problem** column meets the **Security Dimension**. Rouba noted that these spaces are filled with different authorities depending on the the impact of the security event. For example, if the event has a financial impact, you would contact financial authorities; If it is related to privacy, users would contact the Office of the Privacy Commissioner of Canada, etc. However, there is no one authority that would serve as the contact in all cases.

Another gap was realized with respect to existing materials intended to educate consumers about cybersecurity related issues. In their research, the group examined a variety of sources including the Office of the Privacy Commissioner *Tips to Protect Privacy*, GetCyberSafe.ca, the PSC *Cyber Safe Tip Sheet*, and other materials. However, none of these were IoT specific. **This might be a gap which the group could incorporated into their evolving mandate.**

While there is still work to be accomplished, it was clear that the mulstakeholder group believes that a critical component to securing the internet of things is making strides to help change the public's understanding and behavior with respect to IoT devices, privacy and security.

Suggestions and Considerations:

1. There was a suggestion that an **end-of-use** dimension may be added to the **x-axis** of the matrix. This would cover privacy, security, and functionality issues related to when a user wants to

dispose of a device, when a device ceases to work properly, or when a user wishes to transfer a device to another user.

2. In terms of messaging, there were multiple suggestion to break down the **Privacy and Security - Before Purchase** section(s) into more granular components and include:
    a. The kind of data devices are collecting;
    b. What this data is used for;
    c. How the device manufacturer makes efforts to secure that information;
    d. Generally, how compromised devices can affect other people and devices around them;
    e. How to plan the device's location both in a physical space and on a network so that it minimizes the ability of that device to infringe on privacy and/or cause harm;
    f. What the device does from a functional standpoint;
    g. And information about the device's ability be repaired, patched, and upgraded.
3. Further to this was the question of how organizations acquire meaningful consent. There was a suggestion that this be broken down into the process of *collection, use, and disclosure.*
4. Faud Khan, the Labelling Working Group Lead, made mention of the fact that the **Before Purchase - Security Category** is mostly product-centric. However, he made the point that security begins with the organization itself and requires a certain process to be followed. This is where the CSA's Cyber Verification Program or other labelling/trustmark regimes could be useful (*see more in the labelling section*). With this in mind, there was consensus that the Labelling and Consumer Education Working Groups ought to work together more closely moving forward.
5. There was also a number of suggestions with respect to the **After Purchase - Security Category**, namely that consumers ought to know how to upgrade and patch devices. One participant stated that in ideal circumstances, devices will update automatically.
6. There were also multiple suggestions with respect to **after a device experiences** an issue, including:
    a. There was a suggestion that the **At-Problem** category should not only have an authority to turn to, but also some suggestions about how to seek redress;
    b. To that point, there was a suggestion to be a include instructions about how to erase, reset, or reimage IoT devices as needed to prevent or respond to breaches.
    c. There was also a question raised regarding where to place people who are affected by IoT devices who are not the primary users or consumers of those devices. There is still an outstanding question regarding what authority they would turn to for redress. There is the possibility that this, too, could in some way be built into a dynamic label which connects to online resources.
7. During the general discussion at the end of the day, there was a conversation about who are consumers are and whether or not it would be useful to divide them up by demography. This would allow messaging to be specifically tailored to those audiences. It was agreed that initial messaging will be developed using all consumers as the intended audience. However, future efforts may take place to develop messages aimed at various groups of consumers (e.g., youth, seniors, the tech-savvy, etc.).
8. There was a comment that the ordering and priority of the consumer education messaging is more important than necessarily the details or each area. This was compared to a newspaper style guide, where the priority information in news articles is in the first paragraph, followed by less important information, etc.

9. During the broader discussion at the end of the day, a participant commented that when considering SMART goals, copyright, contracts, or terms of service might be too broad for the Consumer Education Working Group.

Action Items:

1. During the Multistakeholder Meeting it became clear that there is complementarity between the work performed by the Labelling WG and the Education & Awareness WG; therefore, the two groups agreed to work together on key messages related to security and privacy specifically;
2. The Education & Awareness WG will continue to work with the privacy and security experts;
3. OCA will reach out to key stakeholders such as provinces, who will need to weigh in on the key messages related to IoT devices and Contract Law (including issues related to redress);
4. The Education & Awareness WG will incorporate the suggestions made by the majority of the stakeholder group into their work.

Labelling Working Group Discussion (1:13:20 – 1:59:08):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/06/Multistakeholder-Meeting-2-Report.pdf (Page 3-4)

Description:

Volunteer leader, Faud Khan (TwelveDot), began by outlining the broad goal of the Labelling Working Group, which is to scope out possible labelling regimes that could be applied and/or enhanced in the Canadian landscape. He then provided a brief overview of the progress made between our last multistakeholder meeting, when the group was established, and Sept. 5th. Most notably, the group hosted webinar on August 1, which brought together Jonathon Cave (University of Warwick), Maarten Botterman (GNKS Consult), Jonathon Kruse Brandao (NXP Semiconductors) and Faud himself to outline a variety of global perspectives around labelling and trustmarks.

In terms of work in progress, the Labelling Group White Paper draft is still being developed. However, in its current form, it focuses on four broad concepts: standards, testing and evaluation, regulations, and sector specific requirements. For the first point, Faud noted that there are two types of standards: international and national. If a product's manufacturer is trying certify a product for quality, performance, or safety in a way that is internationally recognized, Faud asserted that there are only two organizations which can accomplish this: The International Standards Organization (ISO/IEC) or the International Telecommunication Union (ITU). As noted in the draft document, other standards are bound to geographical regions and may require more self-assessment, rendering them less useful for other countries. In many cases there are labelling equivalencies, but this is determined on a country-to-country basis. With this in mind, there are a variety of international standards which may have applicability in Canada, including:

1. ISO/IEC 27000 series – Information Security Standards

2. IEC 62443 series – Industrial Network and Systems Security
3. ANSI/CAN/UL 2900 – Cybersecurity for Network-Connectable Devices

There are also two working groups, one being ISO/SEC SC 41 *Internet of Things*, which is creating a IoT device trustworthiness framework. Also, ISO/IEC SC 27, which has a project named ISO/SEC 27030 *Guidelines for Security and Privacy in Internet of Things*, is creating the product and organizational requirements for that framework.[1] When this has been complete, it may have applicability for a labelling regime in Canada. However, the timeframe on this is to be determined.

On a regional basis, the Canadian Standards Association (CSA) is creating a Cyber Verification Program (CSA CVP) that may be aligned with various international standards that could apply to the IoT. This program has multiple layers to it, including a self-assessment, an on-site audit, and end-to-end product security and privacy tests. This assesses the organization's security maturity, as well as the integrity of the product itself. If all the benchmarks are met, attestation would then be issued and the organization could adopt the CSA CVP label.

By the next meeting, it is the hopes of the Labelling WG to have an idea of the best route forward with respect to what certifications and trustmarks ought to enhanced or promoted by the Canadian Multistakeholder Process, as part of a larger effort to help create a more secure IoT ecosystem.

Suggestions and Considerations:

1. One participant noted that an issue with labels is that they can be forged. Considering ways that prevent that from happening will be critical to wide-scale adoption of any label or trustmark.
2. As noted in the consumer education discussion, there are no existing labels for security and/or privacy.
3. When considering the value of security-by-design, privacy-by-design, and the business case for improved security, Faud mentioned that many companies believe that this is something they cannot justify due to cost. However, he mentions that this is a falsehood because you save money in legal fees down the road.
4. It was suggested that we out to begin to thinking outputs, namely the **feasibility of piloting a label for this initiative**. This might help uncover some lessons learned with respect to how labels resonate with people of different cultural, knowledge, and accessibility differences.
5. A participant explained that there is a difference between security attestation and certification. Certification means the product is absolutely certified and secure. The person remarked that this does not exist because no product can be totally secure. Attestation, on the other hand, means that consumers ought to have a good indication that the product is secure when it comes out of the box. However, after enough time, any device can be compromised. **This distinction ought to be incorporated into a the white paper.**
6. There are still gaps with respect to non-ISO/IEC and CSA labels that ought to be incorporated into the Labelling White Paper.

[1] Note that these standards are a combination of what was mentioned at the Sept. 5th meeting and on the Labelling webinar on August 1st.

Action Items:

1. To continue to build out the white paper/working document draft for comment and input by the end of October.
2. To work more closely with the Consumer Education Working Group to broaden the component of labelling which speaks to what consumers and business need to convey before purchase, after purchase, and when there is an issue.
3. The Labelling WG will incorporate the suggestions made by the stakeholder group into their work.

Network Resiliency Group Discussion (2:28:24 – 3:08:00):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/06/Multistakeholder-Meeting-2-Report.pdf (Page 4-5)

Description:

For the Network Resiliency Working Group, volunteer leader, Dr. Jordan Melzer (TELUS), began by reiterating the security challenge that IoT devices pose to the network – scale, vulnerability and longevity – and gave an example of the impact these devices could have when compromised and weaponised: the MIRAI security camera botnet that broke DDoS attack size records in 2016. He noted the workgroup's consensus on the need to break the cycle of devices being compromised via the Internet and then used to cause harm elsewhere, and offered two approaches:

1. Building more secure IoT devices and lifecycle management processes
2. Restricting network access (*See Appendix A for Secure Home Gateway Workflow*)

As other groups have focused on 1, the Network Resiliency Working Group has focused on 2. They have been implementing access controls into a home gateway to help it secure IoT devices in the home. Their prototypes are using open source code (OpenWRT) and standards (Manufacturers Use Description – MUD) and they will contribute their lessons learned back to the broader internet community.

He described two implementation efforts that were in progress:

1. Unique WiFi Keys – WiFi networks primarily implement access control through encryption. In a home network, though, a single WiFi encryption key is generally shared across devices, making it impossible to link per-device access control to this key. Instead of this "key to the home" model, TELUS and Algonquin implemented a "hotel key" model, where each guest is given a different key. The gateway can provide different access to the holder of each key, or revoke access entirely. (WIP code: https://github.com/noahburrell)
2. Access Controls – As part of CIRA's Secure Home Gateway project, CIRA and Twelvedot are implementing access controls into a home gateway. In their prototype, the policies derive from MUD (Manufacturers Use Description), which is a specification being created by the IETF

(Internet Engineering Task Force). This specification will allow the gateway to receive information regarding what typical data traffic patterns coming from IoT devices ought to look like. If patterns deviate from the MUD, the gateway can limit the device's access. In cases where there are no MUD files, there would be secondary repositories that could be referenced. After the gateway does an initial assessment of what the device requires, users could then give it permissions based on what is needed (LAN vs. full internet access, etc.). To this point, Jordan noted that there are lessons which can be gleaned about user experience from permissions controls given by smartphones. (WIP code: https://github.com/CIRALabs)

Through this prototyping effort, the group is developing and making available viable options for implementing access controls for IoT devices that can help protect IoT devices and reduce the scale of future IoT-based attacks.

Suggestions and Considerations:

1. Faud Khan made note of the fact that the Labelling Working Group has been working closely with the Network Resiliency Group. He made note of an ideal scenario, where a user would scan a device label, giving the gateway access to the MUD file. This would not only attribute a unique WiFi password to the device once it has received the file, but also take the user to a web portal that would outline everything needed to understand the aspects of the device related to security and privacy. If this works in practice, the intent is that the members of the working group will submit an IETF draft specification which would make this a requirement.
2. It was noted that there is the intent to submit another IETF draft specification, different from the one described in point 1, which would outline specifications related to the MUD QR code or other ways which devices can retrieve MUD files. Again, this would only occur if the efforts of this working group are validated by a successful prototype. **This has applicability for both after a purchase has been made, allowing a user to configure the device after has been purchased, but also prior to purchase, helping consumers make informed decisions while the device is still on the shelf – so to speak**.
3. One participant noted that despite industry interest, there are no public MUD files available, and wide-scale adoption has an uncertain timeline and future. In light of this, it was proposed that the group consider approaches with lower time to market and fewer actors. Working group members generally agreed that this was valuable and worth working on.
4. There was discussion of how to treat devices that don't implement MUD, and a suggestion to limit their access to force adoption. The challenge with only allowing devices that do not have MUD files limited access to networks is that it may constrict their functionality or ability to be updated. However, this diminishes the attack surfaces that could be exploited.
5. There was some discussion related to out-of-support devices, and a suggestion that the gateway could restrict a device to LAN access once its software support is over.

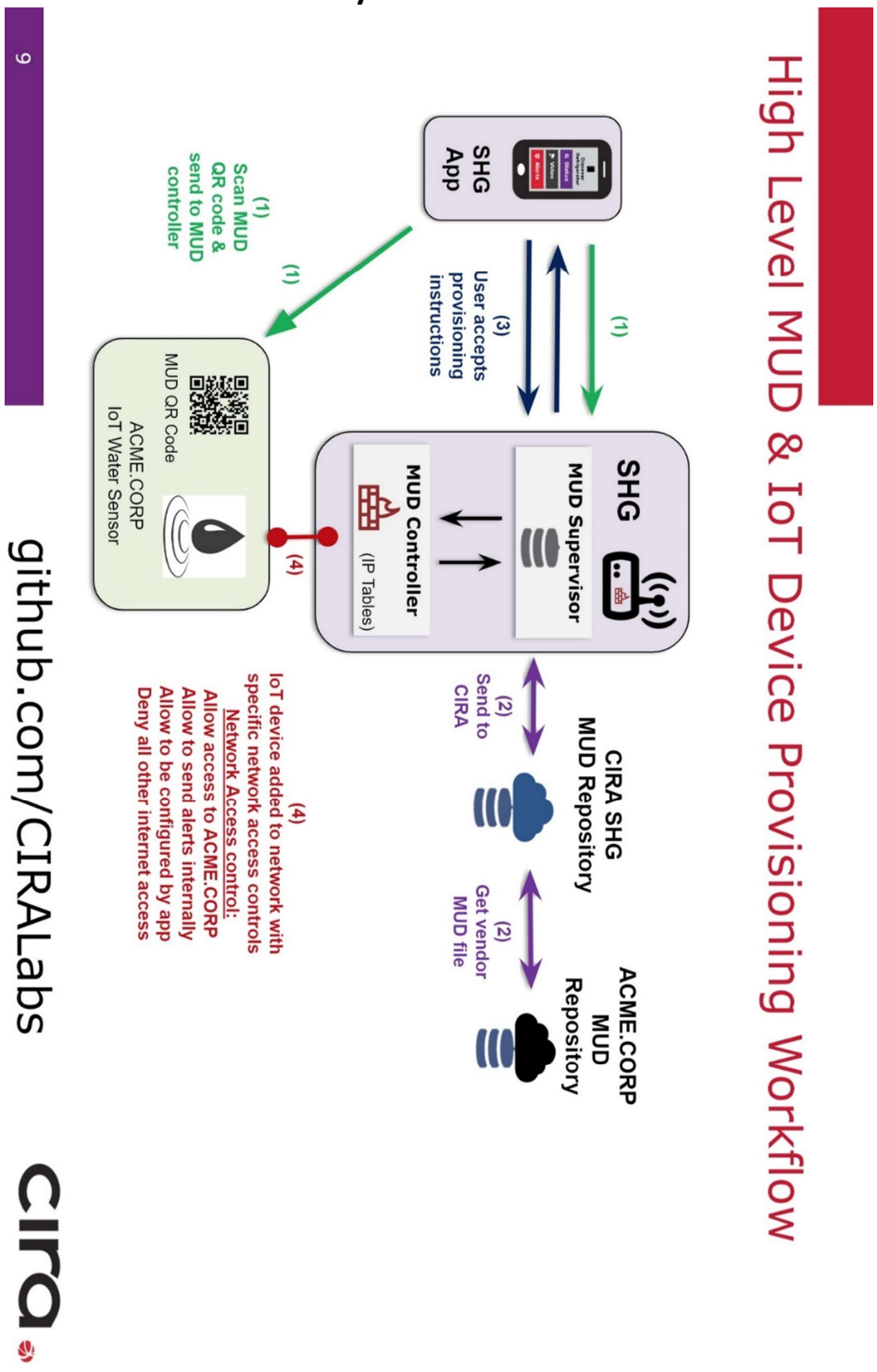
Action Items:

1. Have a demonstrable prototype working by the November 20th multistakeholder meeting.
2. The Network Resiliency WG will incorporate the suggestions made by the stakeholder group into their work.

Broader Discussion (3:08:00 – 3:46:45):

1. There was a suggestion that the sub-groups have more face-to-face meetings.
2. There was a comment that there ought to be more effort put into discussing the goals of each sub-group and considering ideal outcomes and outputs. This participant noted that the network resiliency group appears to have that goal in mind, whereas the others might still be too broad. When prompted to provide a suggestion about what the goals of the Consumer Education group may be, they said that perhaps this group could focus on education the population generally about IoT, not focusing on what is on devices or packaging. This part could be made more explicit by the Labelling Working Group. In response, another participant commented that the group is focusing mostly on behaviors as opposed to anything else.
3. With respect to consumer education, the delivery component has not been discussed yet.
4. It was proposed that another working group/agenda item for each working group created that will focus on adoption.
5. A question was asked about what happens after March/April, when the project is completed. There seems to be some desire at this point in the process to begin thinking about outcomes/adoption of the project's outputs. Tom Stark, the Project Manager for this Initiative, suggested that this be tabelled for our next multistakeholder meeting in November.
6. It was suggested that it might be useful to form another working group that would consider how the components of the Canadian Multistakeholder Process would mesh with other international initiatives.

Appendix A: Secure Home Gateway Workflow



Appendix B: Consumer Education Messaging Matrix

Instruments	Categories	Stages		
		Before Purchasing	After Purchasing	At Problem
Potential Key Messages	Privacy	• Read privacy information before purchasing. • Understand meaningful consent. • Check whether it is possible to not provide some information and still use the product as intended.	• Learn about the privacy settings in your browser and keep it up to date. • Let the manufacturer know if you are not comfortable with your information being shared. • Remove all your personal information Before disposing of your connected device.	• OPCC
	Security	• What are the security measures put in place by the company? (i.e. will communications between the connected device and my phone be encrypted? • Investigate the level of security provided with the IoT device. • Ask about the availability and duration of security upgrades and patches, etc.	• Create a guest WiFi network just for IoT devices to keep them separate from your computers and other more secure devices. • Ensure the network is password protected — and choose WAP2 when prompted. • Change the default password on the device. • Make sure your passwords are strong and don't re-use the same password across multiple devices or services. • Ensure your home network is secured, for example, with virus protection and firewalls. • update the computer program that runs the device (known as the firmware) if you receive a notification do to so.	
	Functionality	**Copyrights:** • Are there TPMs on the software that will limit how the consumer can use the device, e.g. limit their ability to tinker with it or to ensure interoperability? • Will software updates be available free of charge? • Are there restrictions on consumers' ability to use services of a third party to repair the device? • Is the software part of a closed ecosystem that will not function with the software in other IoT devices? **Contracts:** • What are the policies with respect to returns, refunds and exchanges? • Does the device/software come with a manufactures warranty? If so, for how long? Does the warranty cover software? • Does the company offer post-sale customer support? • Is the product functional without internet connectivity?		• Provinces

Appendix C: Agenda

12:30 p.m.	**Registration Opens**
1 p.m.	**Welcome and overview of the Securing the Internet of Things Canada Project** Tom Stark, Internet Society
1:05 p.m	**Remarks on Privacy and Security by Design** Dr. Ann Cavoukian, Ryerson University
1:20 p.m.	**Review of rules of engagement and project recap** Maarten Botterman, GNKS Consult
1:25 p.m	**Consumer Education Working Group Discussion** • Presentation of Group Progress (10 mins) – Rouba Alfattal, OCA • Questions and/or Facilitated Discussion
2:15 p.m	**Labelling Working Group Discussion** • Presentation of Group Progress (10 mins) – Faud Kahn, TwelveDot • Questions and/or Facilitated Discussion
3:00 p.m.	**Break**
3:30 p.m.	**Network Resiliency Working Group Discussion** • Presentation of Group Progress (10 mins) – Jordan Melzer, Telus • Questions and/or Facilitated Discussion
4:15 p.m.	**Broader Discussion** Does the group believe we are still addressing priority areas? In the context of what has been happening in the three working groups, does anyone have any outstanding issues they would like to discuss?
4:45 p.m	**Any Other Business** Are there any needs that ISOC and the Planning Committee can provide support for?
5:00 p.m.	**Adjourn** Reception from 5 to 7 p.m.