



**CANADIAN MULTISTAKEHOLDER PROCESS**  
ENHANCING IOT SECURITY

# Final Outcomes and Recommendations Report



# Table of Contents

Definitions.....	3
Executive Summary.....	4
1. Introduction .....	16
2. Network Resilience Working Group (NRWG).....	19
3. Device Labeling Working Group (DLWG).....	28
4. Consumer Education and Awareness Working Group (CEAWG).....	38
5. Inter-Group Collaboration .....	43
6. Youth Perspectives .....	45
7. Appendices.....	48



# Definitions

ccTLD: Country Code Top-Level Domain

CEAWG: Consumer Education and Awareness Working Group

CIPPIC: Canadian Internet Policy and Public Interest Clinic

CIRA: Canadian Internet Registration Authority

CSA: Canadian Standards Association

CSIRT: Computer Security Incident Response Team

CTIA: Cellular Telecommunications and Internet Association, USA

CVP: Cyber Verification Program

DCMS: UK Department of Digital, Culture Media and Sport

DLWG: Device Labeling Working Group

DNSSEC: Domain Name System Security Extensions

DOTS: DDoS Open Threat Signaling

ENISA: European Union Agency for Network and Information Security

IETF: Internet Engineering Task Force

ISED: Ministry of Innovation Science and Economic Development

ISO/IEC: International Organization for Standardization/International Electrotechnical Commission

ISOC: Internet Society

ISP: Internet Service Provider

ITU: International Telecommunications Union

MUD: Manufacturer Usage Description

NCCoE: National Cybersecurity Center of Excellence

NIST: National Institute of Standards and Technology

NRWG: Network Resilience Working Group

OC: Oversight Committee

OSMUD: Open Source Manufacturer Usage Description

OWASP: Open Web Application Security Project

PIPEDA: Personal Information Protection and Electronic Documents Act

SDO: Standards Development Organizations

SIDN: *Stichting Internet Domain Namen* (registry for .NL)

SPIN: Security and Privacy for In-home Networks by SIDN

UPnP: Universal Plug and Play



# Executive Summary



The Internet of Things (IoT) carries enormous potential to change the world for the better. Projections for the impact of IoT on the Internet and the global economy are impressive, forecasting explosive growth in the number of IoT devices and their use in a wide variety of new and exciting applications.

At the same time, with billions of IoT devices, applications, and services already in use, and greater numbers coming online, IoT security is of utmost importance. Poorly secured IoT devices and services can serve as entry points for cyberattacks, compromising sensitive data, weaponizing data, and threatening the safety of individual users.

These risks and rewards are being carefully considered by many governments and global organizations. However, given the Internet's global reach and impact, it is critical that its security be addressed collaboratively. That is why the *Canadian Multistakeholder Process: Enhancing IoT Security* initiative was launched.

Recognizing the complexity of mitigating cyber security risks from the global proliferation of IoT and the resulting necessity for a made-in-Canada policy to address these risks, the Internet Society, in partnership with the Ministry of Innovation Science and Economic Development (ISED), the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), and CANARIE, undertook a voluntary multistakeholder process for the development of broad-reaching recommendations to enhance IoT security in Canada.



This initiative brought together a multistakeholder group — drawn from the Canadian Internet community — to explore both the scope of challenges and the range of promising solutions that could be pursued further to address them, guided by the following principles:

1. The complexity of IoT security necessitates a bottom-up, organic process to ensure the outcomes address all existing and potential challenges and issues.<sup>1</sup> The approach should be fluid in nature, defined and refined through discussion with stakeholders.
2. Internationally harmonized technical standards are key to enhancing IoT security in the long-term, but they are hard to get right and take time. It is reasonable for approaches to IoT security to start at a national level while working in collaboration with other national, regional, and international bodies.
3. Because of the immediacy of the risks and the extended time frame of long-term developments, such as improvements to framework policies and the development of international standards, it is important to start work on educating consumers and for businesses to begin adopting best practices that will reduce the risks of consumer IoT device adoption.

Within this context, the initiative was focused on consumer-level devices as opposed to those that are being utilized at the enterprise level.<sup>2</sup> Throughout 2018 and early 2019, the *Enhancing IoT Security* multistakeholder group engaged in a series of in-person multistakeholder meetings, focus groups, and webinars and conducted research to develop the following:

1. A shared set of definitions and benchmarks around the security of Internet-connected devices.
2. Shared guidelines to ensure the security of Internet-connected devices over their lifespan, including the development, manufacturing, communications, and management processes.
3. Recommendations to inform national policy related to IoT security in Canada.

A defining feature of the *Canadian Multistakeholder Process: Enhancing IoT Security* initiative was the use of the multistakeholder approach in its organization, governance, and decision-making. Oversight and guidance were provided by the initiative partners (the Oversight Committee<sup>3</sup>) and management was provided by the Internet Society. Appendix II explores the role the multistakeholder model played in this work and outlines key learnings from the process.

Three thematic working groups, Network Resilience, Device Labeling, and Consumer Education and Awareness, were established to inform the process and to develop specific recommendations. The recommendations of these Working Groups cover the technical, policy, and behavioural aspects of IoT security.

---

1 A multistakeholder process is particularly well adapted to discovering insights when the dimensions of the issue are not clear; when the solutions are undetermined; and when in general people do not have the answers, there is no consensus around the possible answers, or approach is lacking.

2 Participants reached near consensus to define IoT as “any network-exposed device not historically accessible, or any device transmitting data, via the Internet, which generally lack sufficient built-in security to protect themselves from causing or becoming a source of harm.”

3 See Appendix I



## Best Practices, Recommendations, and Next Steps:

Certain aspects of IoT security are so well-established that they were asserted as baseline actions that must be taken to enhance IoT security, including the following:

1. No universal or easily guessed pre-set passwords.
2. Data should be transmitted and stored securely using strong encryption.
3. Data collection should be minimized to only what is necessary for a device to function.
4. Devices should be capable of receiving security updates and patches.
5. Device manufacturers should notify consumers if there is a security breach.
6. Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.

Over the course of a year, the multistakeholder group and the Working Groups worked together to develop the following over-arching recommendations:

1. Elevate the focus on international-level standards. Standards can provide clear, testable, and credible guidance on implementing security and privacy by design across all jurisdictions.
2. Continue development and deployment of the Secured Home Gateway at CIRA and the Manufacturer Usage Description (MUD) standard at the Internet Engineering Taskforce (IETF) in order to provide network-level approaches to resiliency that can address the challenge of low-cost, foreign-made devices that do not adhere to security standards (which are designed for specific devices and firms).
3. Continue to develop a consumer friendly label alongside international-level standards. It is recommended that a label combine static “trustmarks” (such as for CE in Europe, Kitemark in the UK, CSA in Canada) with a live component such as a QR Code that can convey advanced and up-to-date product security information.
4. Leverage the multistakeholder group’s core content for consumer education and awareness (the Shared Responsibility Framework). This could be used in efforts or campaigns to raise consumer and industry awareness. With funding, a consumer education campaign could be organized by a multistakeholder group that leverages the network created by this Canadian IoT initiative. The Working Groups also developed more granular recommendations for specific stakeholder groups, identified in the following sections.



## On Internet-connected device labeling

### Recommendations:

1. Develop a security label for Internet of Things (IoT) and other digital products.
2. Adopt standards for testing and evaluation of IoT products to assist purchasing decision.
3. Promote consumer awareness programs for both product labels and testing.
4. Enact a regulatory framework that requires formal testing and evaluation of products.
5. Create a flowchart that could be used by manufacturers to determine requirements, and by users to determine label expectations.

An effective security label should combine the consumer trust factor of known “trust marks” (such as CE in Europe, Kitemark in the UK, and CSA in Canada) with advanced and critical product security information that can be updated. The label should convey the key information that formal testing and certification has been performed on the product, and how to access up-to-date critical information on product security features and installation/deployment considerations. Examples of security labels can be found in Section 3.3.

### Recommended Next Steps:

1. Approach and collaborate with organizations focusing on IoT security and privacy in an attempt to reduce the amount of fragmentation in the market for initiatives and labels to avoid consumer confusion.
2. Continue to influence the standards effort through the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) for international standards and standards developing organizations with similar projects and interests.
3. Collaborate with the Online Trust Alliance (OTA) to approach key vendors and solution providers to raise awareness on the need for security certification and device labels.
4. Determine the best organization to provide a formal specification of the “live label.” This could be Internet Engineering Taskforce (IETF) or similar, and includes further developing the live label (QR Codes) proposal through collaborating with other organizations such as OTA.
5. Elevate the proposed voluntary labeling framework as a model for consumer IoT device manufacturers to demonstrate their compliance with existing Canadian law and regulations in this space.
6. Further assess the certification and testing of applications that control devices and backend support services, in addition to focusing on the devices themselves.
7. The development of labeling concept should continue. Labeling can be incorporated as a ‘control’ as part of IoT security-related standards being developed at the national/regional (T200) and international (SC27030) level.

There is a need for a regulatory framework for required formal testing of standards and mutual recognition options between IoT standards, similar to the type of agreements that govern telecommunications equipment.



## The Device Labeling Working Group proposes that a security product label should include the following:

1. Identification of the organization overseeing/authorizing the certification and formal testing (e.g. BSI Kitemark, CE mark, CSA mark).
2. A machine-readable code that is linked to a website providing up-to-date product information (i.e., a live label). The website should include the following:
  - a. Product model and/or version number
  - b. Latest product firmware version number
  - c. Recent vulnerability information
  - d. Certification/testing framework
  - e. Security configuration guide
  - f. Information on data collection and sharing
3. Key information to be conveyed by the label:
  - a. Formal testing and certification have been performed on the product.
  - b. Where to get up-to-date critical information on product security features and installation/deployment considerations.

The next steps for implementation must be carried out by many stakeholders, including, but not limited to:

4. IEEE Data Port (free resource of large datasets to be fed into the process).
5. Vendors, security experts, consultants.
6. Civil society, to add consumer perspectives to the standards discussion.
7. ISED and government technical experts who can influence the standards discussion to provide public policy considerations, including implication legislation and enforcement.

## On consumer education and awareness

The Consumer Education and Awareness Working Group developed a Shared Responsibility Framework which recommends behaviours for consumers and industry. The Working Group recommends that the Implementation Working Group focus on how to take the content of the Framework, as well as related messaging in the other working groups, to further develop and ultimately raise consumers and industry awareness.



SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
Before Purchasing	Understand and consent to how the device is collecting, using, and sharing your data.	Improve accessibility and content of privacy policies (i.e., provide clear answers on how the device is collecting, using, and sharing data).
	Ensure that the device comes from reputable/certified manufacturers (i.e., low cost devices typically come with greater risks. Any smart devices that are connected to the Internet carries a risk of breach).	Clearly lay out the shared responsibility regarding the device's security (i.e., convey expectations of consumers' awareness/responsibility in the instructions/ToS/warning leaflet of the device).
	Check if there are any extra functionalities (i.e., is the device collecting unnecessary data that could create unnecessary risk? Can you opt out of future features without opting out of security updates?)	Clearly indicate/disclose all functionalities of the device and how to minimize unnecessary functions (i.e., develop a list of sensors in the device, provide information on how to turn off video and audio recording, clearly indicate if new/extra functionalities have been included in updates, and if/how it is possible to opt out of these functionalities).
	Check for user reviews, labels, and certifications (i.e., label and certification indicate that the device has been tested).	Use certification/adherence to laws, standards, and non-binding best practices as a publicized selling feature.
	Consider the lifecycle of the device and the support available to keep your device in use for as long as possible (i.e., verify availability and duration of security upgrades and patches).	Use availability/duration of patches, updates, and support as a publicized selling feature.
	Check that the device works even without Internet connection, and assess functionality in the event the device outlives the company (i.e., smart lock, camera, fridge still function even if the Internet is down or the company no longer exists).	Ensure the devices can still function without Internet connection, and if the company ceases to exist.



## SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
At Use/Issue	Know where to seek redress and address technical problems, including if your device has been compromised, and keep record of your purchase.	Provide transparent and accessible instructions on seeking redress.
	Follow best practices for network setup and configuration to help mitigate risk when using IoT devices.	Assist consumers to set up their IoT networks consistent with best practices (i.e., make the default setting consistent with best practices).
	Be considerate of the implications or impacts on guests or others who are in the vicinity of your device (i.e., consider notifying your guests when in proximity to your smart home devices, or turning devices off).	Remind consumers about the effects of their IoT devices on their guests (i.e., audio or video recording).
	Be aware that the security of your device is constantly being updated. Ensure that the device is able to receive updates.	Remind consumers to follow recommended security best practices (i.e., follow recommended upgrading and patching recommendations from the NTIA Multistakeholder Process). <sup>4</sup>
	Ensure that each device in your home is secured. The security of your home network is only as good as its weakest link.	Consider providing mechanisms to warn consumers when issues arise (i.e., assist consumers in monitoring their traffic to detect anomalies).
End of Life/Use	Remove data from your device before disposing or moving. Many guides are available to assist users with specific IoT devices (i.e., Nest Thermostat <sup>5</sup> ).	Clearly indicate the best method or provide consumer assistance to permanently remove data from device.
	Do not forget to revert back to factory default settings. Many guides are available to assist users with specific IoT devices.	Clearly indicate the best method or provide consumer assistance to revert the device to factory default settings.
	Check the resources that are available to help dispose of IoT devices responsibly. Retailers may provide this information.	Provide resources to help consumers dispose of their IoT devices responsibly.

<sup>4</sup> [https://www.ntia.doc.gov/files/ntia/publications/ntia\\_iot\\_capabilities\\_oct31.pdf](https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf)

<sup>5</sup> <http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/>



### Recommended Next Steps:

1. Task the Implementation Working Group with focusing on the delivery of these messages—i.e. convene interested civil society, consumer advocacy, educational institutions, outward-facing Canadian government departments such as the Office of Consumer Affairs (OCA), Canadian Centre for Cyber Security (CCSE), Public Safety Canada, and the Office of the Privacy Commissioner (OPC).
2. Task the Implementation Working Group with providing a multifaceted coordination function, including providing a network where stakeholders could:
  - a. Continue dialogue and networking to ensure consistency of messaging.
  - b. Share opportunities to input into relevant government processes (e.g., consultations, legislative reviews etc.).
  - c. Share their own ongoing IoT-related educational efforts.
  - d. Seek support on how to engage their own membership.
  - e. Coordinate engagement with industry.
  - f. Collaboratively develop an educational campaign (including pooling resources and distribution channels).



## On enhancing network resilience

### Recommendations:

1. The Secure Home Gateway code should be accepted by the core openWRT<sup>6</sup> project. Furthermore, the openWRT should be bundled by default with its IoT security framework, and/or that when manufacturers upgrade their openWRT software, it comes equipped with this framework.
2. Future work is needed regarding network resilience with regard to IoT security, including:
  - a. Security evaluation of any new security/user interaction mechanisms. New MUD-based access controls represent significant new attack surface and must be analyzed and tested.
  - b. Continued implementation of a security framework and the integration and development of:
    - i. Device fingerprinting
    - ii. Automated MUD profile generation
    - iii. MUD clearinghouse
    - iv. Access controls
    - v. User controls (visibility, permissions, notifications)
    - vi. Unified onboarding
    - vii. DDoS Open Threat Signaling (DOTS)-based DDoS filtering
    - viii. Quarantine and un-quarantine procedures
  - c. Standards development
    - i. Live labels: integration of live label with network onboarding, MUD, user-interaction
    - ii. Out of support notification/device management
    - iii. Credential management on IoT devices
    - iv. Quarantine/unquarantine
    - v. (MANRS<sup>7</sup>-inspired) MARIS: Mutually Agreed Norms for Internet Security
  - d. Continued global coordination towards standardization, implementation, and adoption.

---

6 "OpenWrt is an open source project for embedded operating system based on Linux, primarily used on embedded devices to route network traffic." From Wikipedia: <https://en.wikipedia.org/wiki/OpenWrt>

7 <https://www.manrs.org/>



### Recommended Next Steps:

1. In collaboration with partners, CIRA will continue developing a functional Secure Home Gateway prototype initiative and standard APIs on:
  - a. SHG onboarding
  - b. IoT device onboarding/management
  - c. Device quarantining
  - d. Device un-quarantining
2. In collaboration with partners, CIRA will attempt to get two distinct “running code implementations” that are based on the standard APIs.
3. CIRA, in collaboration with the two other Working Groups, will submit Internet drafts for MUD extension to support live labels, privacy notification, user space, IoT device management framework, instant management, and credential management.
4. CIRA’s Secure Home Gateway initiative will assess integration with Mozilla’s Web of Things initiative.
5. Ensure CIRA’s Secure Home Gateway code is available on GitHub, is open source and freely available to all.
6. Integrate the work of this group with the Labeling and Consumer Education and Awareness Working Groups.
7. This working group will reconvene to assess feasibility, new partners, resources required, and to adjust the plan as needed. It will create a mailing list for notification of updates to this work.
8. Raise awareness of stakeholder group recommendations and demonstrate to gateway developers, through the Secure Home Gateway initiative, that these recommendations are achievable, thus providing the larger industry with a framework for secure device development.



## Youth-focused recommendations and areas for further research

1. **Education:** For youth in particular, education policy is critical. Provincial/territorial and federal governments should work together with civil society organizations on curricula and programs that can offer forums for discussion and awareness of IoT and other tech-related issues across Canadian educational institutions.
2. **Conversation:** One of the strengths of social media as a medium of engagement is its ability to bring people into a conversation and generate widespread interest in specific topics or events through the multiplying effects of personal networks. Catalyzing authentic personal interest and curiosity through open dialogue which connects a specific issue like IoT security to broader social narratives or concerns is the most effective means of spreading awareness and inspiring action.
3. **Exploration:** Effective engagement and capacity building will also require a deeper dive into assessing the current state of young people's interaction with digital platforms and their knowledge of them.
4. **Improving diversity and multistakeholder access:** Engagement opportunities should be promoted, and not skewed to certain types of organizations over others.
5. **Embed participation:** Avoid requiring significant amounts of additional time from people by incorporating opportunities to learn about and engage with IoT and other emerging technologies, as well as to participate in policy making, into regular education or training activities.
6. **Policy changes:** Policymakers from around the world can use the best practices of existing and proposed regulation to inform and inspire the basis for an approach to data protection for IoT devices.
7. **Collaboration:** Internet governance and policy involves a variety of organizations from a myriad of backgrounds. The topic of IoT security spans multiple interrelated issue areas, each serving as the focus of a number of these groups. In order to prevent duplication of efforts, collaboration and harmonization must increase between these groups at both the community and international level.



## The Enhancing IoT Security Implementation Working Group

An Implementation Working Group, made up of members of the OC, WGs, and multistakeholder group, was formed at the sixth and final multistakeholder meeting to ensure the recommendations are implemented and to carry out next steps. Stakeholders will leverage this group to coordinate and contribute to:

1. A coordinated education and awareness campaign on consumer IoT that uses the Shared Responsibility Framework.
2. Canadian participation in national and international standards processes—with specific emphasis on engaging and facilitating the contributions of consumer organizations, civil society, and youth — in particular the development of T200 into a binational standard, the ISO/IEC 27000 series, and the IETF MUD standard.
3. Canadian participation in international IoT security initiatives, integrating or adapting the trajectory set out by the recommendations and input on the final report. This includes the Internet Society IoT Policy Platform,<sup>8</sup> IoXT,<sup>9</sup> IoT Alliance Australia (IoTAA),<sup>10</sup> EU's Cybersecurity Act implementation, etc.
4. The development of the Secure Home Gateway, binary security label, and related standards.

---

8 <https://www.internetsociety.org/iot/iot-security-policy-platform/>

9 <https://www.ioxtalliance.org/>

10 <https://www.iot.org.au/>



# Introduction



IoT carries enormous potential to change the world for the better. Projections for the impact of IoT on the Internet and the global economy are impressive, forecasting explosive growth in the number of IoT devices and their use in a wide variety of new and exciting applications.

## 1.1 Problem Statement

According to one estimate, “connected devices will number 38.5 billion in 2020, up from 13.4 billion in 2015.”<sup>11</sup> At the same time, with billions of IoT devices, applications and services already in use and greater numbers coming online every day, securing IoT is of utmost importance. Poorly secured IoT devices and services can serve as entry points for cyberattacks, compromising sensitive data, weaponization, and threatening the safety of individual users. Various studies have used empirical data to show that poorly secured IoT devices have been weaponized to assist perpetrators of domestic abuse to monitor and psychologically abuse their victims.<sup>12</sup> The use of poorly secured IoT devices in this manner poses human rights concerns, particularly for women and other vulnerable groups that are more likely to be victims of domestic abuse.<sup>13</sup>

These risks and rewards are being carefully considered by many governments and global organizations, but given the Internet’s global reach and impact, it is critical that its security be addressed collaboratively. That is why the *Canadian Multistakeholder Process: Enhancing IoT Security initiative* was launched.

For more than a year, this initiative convened six in-person, multistakeholder meetings and over a dozen virtual meetings in order to develop recommendations for a set of norms and/or policies to secure IoT in Canada. These events, as well as a comment period on the initial Draft Outcomes Report from this group<sup>14</sup>, served as an opportunity to begin planning and implementing a bottom-up, organic process to remedy existing and potential security challenges in Canada’s national IoT ecosystem.

<sup>11</sup> <https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020>

<sup>12</sup> The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT) - [ucl.ac.uk](http://ucl.ac.uk)

<sup>13</sup> <https://www.canada.ca/en/public-health/services/health-promotion/stop-family-violence/problem-canada.html>

<sup>14</sup> The comment period was open from February 27, 2019 until March 29, 2019 and ultimately resulted in the submission of comments from eight organizations representing five stakeholder groups.



The *Canadian Multistakeholder Process: Enhancing IoT Security* group reached near consensus to define IoT as “any network-exposed device not historically accessible, or any device transmitting data, via the Internet, which generally lack sufficient built-in security to protect themselves from causing or becoming a source of harm.” Within this context, the IoT group focused its activities on consumer devices as opposed to those that are being utilized at the enterprise level.

Though complete consensus was not achieved on a definition of IoT, participants agreed that any definition should be continuously updated as the technology develops. The group also agreed there is value in relying on the existing definitions rather than spending additional time reaching total consensus on its own.

At the first meeting of the *Canadian Multistakeholder Process: Enhancing IoT Security* and throughout subsequent meetings, participants frequently reiterated that there are some aspects of IoT security so well established that this group need not focus its

attention on them. Those items included, but were not limited to, the following:

1. No universal or easily guessed pre-set passwords.
2. Data should be transmitted and stored securely using strong encryption.
3. Data collection should be minimized to only what is necessary for a device to function.
4. Devices should be capable of receiving security updates and patches.
5. Device manufacturers should notify consumers if there is a security breach.
6. Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.

The objective of this report is to summarize the work of the multistakeholder group, provide insights gained throughout the process, and provide recommendations for policy on IoT security for Canada.



## 1.2 Methodology

The methodology used for this multistakeholder project was as follows:

1. An Oversight Committee (OC) was created to set the overall goals of the process, review outputs of individual working groups, oversee the development of reports and requests for comments, and approve any external communications. The OC includes representatives from Innovation, Science and Economic Development (ISED), the Internet Society (ISOC), the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), and CANARIE.
2. Decision-making within the Oversight Committee was based on consensus and norms established at the beginning of the process.<sup>15</sup>
3. A transparent multistakeholder group, drawn from government, civil society, academia, technical and security community, the private sector, and other relevant stakeholders was also convened to inform the process, identify appropriate working group members, select areas for research, review documents, and provide guidance to the development of the policy recommendations. Meetings of the multistakeholder group were open, public, and live streamed, with the live stream posted online following each meeting.
4. Reporting to the OC, the Internet Society managed the process.
5. The process was informed by three Working Groups, including on Network Resilience, Device Labeling, and Consumer Education and Awareness, as well as a report submitted to the process on Youth and IoT, focus groups, and research. The subject areas of the respective Working Groups were selected by the multistakeholder group.

6. Primary research was conducted through the expertise from members of the Working Groups and insights gained from participating in various forums.
7. Government participation in the multistakeholder process included activity across a dozen federal departments and agencies.
8. All resources from this project were posted on the initiative website in both English and French.

Efforts were also made to include individuals in these conversations from a variety of regions, languages, and backgrounds. Focus groups were held in both English and French, as well as those targeted at specific demographics, such as youth and Indigenous individuals.

For example, at the 2018 Indigenous Connectivity Summit<sup>16</sup>, the Internet Society hosted a roundtable on IoT security with participants of the conference. The roundtable discussion resulted in several insights including the view that devices should be built with security at the forefront, they should be tested, and they should utilize labeling similar to those for organic foods.

Participants further asserted that security training should be tied into digital literacy training and for many users, security and privacy are viewed as the same. Participants in this roundtable also suggested that messaging on a lack of security can lead to fear, which, in turn, leads the public to avoid using such devices without realizing their benefits. These and other insights from the focus groups held throughout the process were a valuable part of the initiative and directly contributed to the final outcomes of the process.

<sup>15</sup> See Annex IV for more information.

<sup>16</sup> <https://www.internetsociety.org/events/indigenous-connectivity-summit/2018/>



# Network Resilience Working Group (NRWG)



Large-scale attacks from consumer IoT botnets are one of the largest risks to many Internet-based organizations, including ones that provide critical Internet infrastructure.

## 2.1 Summary/Problem Statement

IoT devices are both the largest and fastest-growing type of Internet hosts. They are produced by a very wide range of vendors, most of whom have limited cybersecurity experience. Many of these devices are, by their nature, likely to have life spans that exceed their software support. For example, many first-generation Smart TVs are no longer provided with security patches by vendors. Though IoT devices generally do not generate high volumes of Internet traffic, the proliferation of gigabit-class home and business Internet provides IoT devices access to high throughput connections.

Given that IoT devices are vulnerable to compromise, rapidly proliferating, and have access to high speed Internet connections, they are attractive weapons for a multitude of uses by bad actors.<sup>17</sup>

The NRWG's central question was how to defend Internet infrastructure from this intensifying threat. While many initiatives address IoT security at a device level or address attack mitigation at the target end, the Working Group contends that, as valuable as these approaches are, they do not sufficiently address the threat. The group's central

thesis was that, in order to effectively address IoT-based attacks, the network should protect IoT devices from compromise. Ultimately, the main goal of the group was to develop an IoT security framework for the network to protect devices from being compromised, and to limit, from the network's edge, attacks from compromised devices.

The more limited connectivity needs of IoT devices, as opposed to the extensive connectivity needs of personal devices, provides a route for their protection: they facilitate deployment of fine-grained network-based security controls. The group's work explores how proactively protecting IoT devices can counterbalance the increase in scale of threat from IoT. This group worked to develop a set of recommendations and standards to protect the Internet from things and protect things from the Internet.

The NRWG focused on WiFi-enabled IoT devices. These include home devices, which connect to the home network via WiFi but do not support Internet-browsing by the user, such as phones, tablets, or personal computers. The NRWG calls the device that connects

<sup>17</sup> <https://www.Internetsociety.org/blog/2017/02/the-Internet-of-things-as-an-attack-tool/>



the Internet Service Provider's (ISP) access network to the home network the "home gateway." While the home gateway falls within its definition of an IoT device, its work focuses on protecting other IoT devices.

Appendix III outlines the research the NRWG carried out in their work.

## 2.2 Discussion

IoT devices are the fastest growing and largest class of consumer Internet-connected devices, eclipsing personal computers and smartphones. While the majority of smartphones and PCs feature a narrow range of operating systems, chip architectures, brands, and form-factors, IoT devices are built from hundreds of different software stacks and chip families, by thousands of manufacturers, in almost every shape and size imaginable. The number of manufacturers contributing to a single product is also raising concern over the security of the supply chain. While most smartphones and computers support many applications, most IoT devices serve a single purpose. These differences, and the scale of IoT device deployment, suggest that there is a need to re-examine how to mitigate threats to and connect consumer devices.

The physicality of IoT has elevated concerns around security in a range of domains. This concern and responses to it are documented in popular books (i.e. Bruce Schneier's "Click Here to Kill Everyone") as well as in domain-specific policy documents (i.e. NISTIR 8228) and standards (i.e. IETF MUD), with the focus on critical infrastructure, government systems, and, increasingly, enterprise users.

While IoT touches sensitive cyber-physical systems from medical devices to power infrastructure, a large portion of connected devices and device types are aimed at the consumer market and found within homes and small businesses. These devices pose privacy, if not safety, risks to their owners. Moreover, the scale and vulnerability of these consumer devices pose risks beyond the homes in which they are found. Large groups of compromised devices have been used together to attack and disable Internet-facing services

by forging large volumes of traffic; the most publicized case is the then-record-setting Mirai IoT botnet.<sup>18</sup> In 2016, Mirai exploited unsecure CCTVs whose default passwords had not been changed. The scale of such attacks continues to increase. The increasing scale of consumer IoT prompted the NRWG to be primarily concerned with the risk that such weaponization of IoT devices brings, both to the core infrastructure that provides Internet services, as well as to organizations that depend on maintaining an online presence.

The central question posed by the NRWG is how to defend against this threat. The group identified three approaches to defense that different actors can deploy and that are most valuable in combination. The first approach is to scale existing Distributed Denial of Service (DDoS) mitigation mechanisms. For core Internet infrastructure providers, this generally means scaling up infrastructure spending, but with IoT proliferation in the market outstripping revenue growth, scaling up for attacks is economically problematic.

While cloud service providers, content distribution networks, and DDoS mitigation specialists offer services able to protect a range of service types from a range of attacks, not every Internet organization is able to rent scale—or to afford it. While there are certain to be advances in DDoS mitigation approaches, there are no guarantees that they will keep pace. A qualitatively more dangerous Internet poses a real threat.

The second approach that the group identified is to directly address the insecurity of IoT devices through improved security design and lifecycle management practices, encouraged via standards, awareness, examples, and regulation. There was consensus within the Working Group that this was important, and members identified a range of initiatives aimed at promoting IoT security practices to manufacturers and the market, from security frameworks such as ETSI TS 103 645 to assurance programs such as a UL CAP<sup>19</sup> to IoT security-focused legislation.<sup>20</sup>

<sup>18</sup> <https://www.Internetsociety.org/blog/2018/11/we-need-to-do-something-about-iot-security/>

<sup>19</sup> <https://industries.ul.com/cybersecurity>

<sup>20</sup> [http://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=2017201805B327](http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=2017201805B327)



Promoting improvements in practices is central to the Consumer Education and Awareness and Device Labeling Working Groups of the multistakeholder process, and endorsed by all participants. As necessary and vibrant as these efforts are, the challenge to this approach is the diversity of manufacturers. For general computing and smart- phones, the relatively small vendor pool (Apple, Google, Microsoft) that produces the bulk of the software for the industry has developed, over many years, excellent software lifecycle practices. With thousands of manufacturers of IoT devices with diverse backgrounds and pervasive pressure to get products to market, many manufacturers will ship

products with little consideration or diligence placed on security and lifecycle management.

The third direction the group identified is network-based defenses for IoT. While some of the vulnerability of connected devices may come from software flaws, these flaws require access to be exploited. The central thesis of the NRWG is that networks can protect IoT devices from compromise and weaponization to, in turn, protect themselves. Working Group members have active initiatives to develop these defenses, and identified and connected with those involved in a range of other network-based defenses.



To begin to develop a framework for defense, the group examined the threats against home IoT devices. These threats and the proposed mitigations are summarized as follows:

Pre-compromise threats (high to low)	Mitigation	Notes
Home gateway compromise.	Secure-by-design.	Home gateways are most-compromised “IoT” devices.
IoT device compromise via services exposed to Internet.	Prevent IoT devices from opening static ports in firewall without user approval.	UPnP-based firewall bypass allows device to act as Internet server. Needed by some games and P2P networks, but poses very high risk.
IoT device compromise via services exposed to home LAN.	Policy enforced at gateway limiting LAN access.	Policy can be signaled via IETF MUD or derived implicitly.
Backend compromise.	Private/limited access to backend.	Reduce reachability of backend to ISP domain or ISP and device class.
Post-compromise mitigation	Method	Notes
Reduce attack size.	Rate-limit policies.	Rate-limiting reduces total attack volume without requiring knowledge of which devices are or are not compromised.
Block in-progress attacks.	Identify and quarantine specific attacker device across NAT (IETF DOTS).	Denial of service attacks are most visible upstream, towards the victim. ISPs which identify attacks in progress can use assistance from the home gateway to identify the specific compromised devices within the home and quarantine them without affecting other home services.
Prevent “ID” theft: access control evasion & rogue AP attacks.	Provide each device with unique WiFi credential.	Provides cryptographically strong identity to facilitate access control. Also allows credential revocation.



The most exposed IoT device in the home is the device that connects the home to the access network: the residential gateway. This residential gateway is open to attacks directly from the Internet as well as from connected devices in the home. Due to their ubiquity, complexity, and exposure, residential gateways have compromised large proportion of the devices within IoT botnets, including Mirai. Hardening these devices is a first step towards hardening the home.

While the NRWG is not aware of security guidelines that are specific to residential gateways, general IoT-focused security considerations, such as those identified by the OWASP IoT project<sup>21</sup> and ETSI TS 103 645<sup>22</sup>, apply to these devices. Top threats to residential gateways include guessable passwords, insecure network services, insecure APIs, and poor software lifecycle practices.

## Residential Gateways

Residential gateways often act as firewalls (and for IPv4, Network Address Translators) for devices within the home, blocking inbound traffic that is not associated with an outbound connection and providing an important layer of defense between the untrusted public Internet and nominally more trusted home LAN.<sup>23</sup> The Universal Plug and Play (UPnP) framework includes a protocol that devices may use to tell the residential gateway to forward inbound traffic on particular ports to them. The second-largest category of IoT devices recruited to botnets have been those that have exposed open ports to the Internet as a whole—generally leveraging this feature.

IoT devices may also be attacked from other devices or applications on the local area network, including Internet browsers, or from Internet-based services to which they connect. Presently, these are seen as lesser threats, but as the number of devices in the home grows, so too does the importance of in-home segmentation. These attack vectors should be addressed within a comprehensive framework.

The NRWG also identified existing network-based defenses. Some Internet Service Providers (ISPs) scan their customers for open ports to detect vulnerabilities and look for connections between their customers and known command and control addresses to detect compromise. These ISPs are able to proactively notify customers of their security threats or breaches. Without cooperation from the home gateway, however, an ISP is not able to identify which device within the customer premises is affected, or to put in place protective controls.

The core of the NRWG's work centered on protecting IoT devices via the home gateway. The main tool is access control: preventing or allowing particular devices from reaching other devices on defined TCP or UDP ports. For example, if instead of allowing any device on the Internet to connect to an IoT device, the gateway only allows the device manufacturer's cloud service to connect to that IoT device, the threat to that device can be reduced while preserving all of its functionality. Similarly, if a gateway enforces that a home device may only talk to a particular service on the Internet with a maximum daily traffic volume, the home gateway can limit the capacity of that device to attack Internet-based services should it become compromised.

<sup>21</sup> [https://www.owasp.org/index.php/OWASP\\_Internet\\_of\\_Things\\_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)

<sup>22</sup> [https://www.owasp.org/index.php/OWASP\\_Internet\\_of\\_Things\\_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)

<sup>23</sup> Though usually placed in the home, there are alternate models where firewalling and other residential gateway features are provided by ISPs upstream from the home. Though there are different implementation considerations between the two models, most of the threats and mitigations are similar between them.



## Access Control Solution Prototypes

Access control is a mature security tool, but historically it has had limited application within the home, because PCs and smartphones support a rich application set with very few limitations. As the bulk of IoT devices are single-purpose devices, access controls around them should be tightened.

Fine-grained access controls are, however, challenging to specify for thousands of diverse IoT devices, and it wasn't immediately clear to the group how to do so. An emerging protocol for describing access controls is the IETF Manufacturer Usage Description (MUD) RFC 8520<sup>24</sup>. MUD provides a data-model for specifying access controls. In the original MUD concept, devices indicate to the network a URL to a MUD file describing the access profile for a device. The network may retrieve the file, validate its contents, and apply the profile.

This protocol is being proposed as a new way to signal the networking and security control characteristics of an IoT device in order to appropriately apply the correct security controls to ensure its safe operation.

MUD is useful in a world where an IoT device manufacturer takes time and care to define and manage MUD profiles. The challenge with MUD is its adoption: we live in a world where time to market requirements often take priority over security by design requirements. To address the case where manufacturers do not provide reasonable device profiles, an IoT device profiling/fingerprinting mechanism could be developed whereby MUD-like profiles are created for IoT devices and security controls are applied based on these discovered profiles.

However MUD profiles are created, if an IoT device's behavior deviates from its profile<sup>25</sup>, a gateway may presume it has been compromised and place it under quarantine to mitigate its potential malicious activities.

There are no current best practices for taking an IoT device out of quarantine mode. Further work is required to develop a best current practice (BCP) to define the processes for quarantining an IoT device and to restoring that IoT device back to normal operations. This remedy needs to address the 'who do we call' (the ISP, the

gateway manufacturer, the IoT device manufacturer, the country CSIRT) as well as the mechanism to restore the IoT device back to a normal state.

Fine-grained access controls are, however, challenging to specify for thousands of diverse IoT devices, and it was not immediately clear to the group how to resolve this problem. Again, MUD could be useful for describing access controls, as it provides a data-model for specifying access controls. In the original MUD concept, devices indicate to the network a URL to a MUD file describing the access profile for a device. The network may retrieve the file, validate its contents, and apply the profile.

Within an enterprise setting, MUD provides a way to automate access controls. The enterprise purchases large quantities of a limited set of device models, enterprise IT staff customize MUD files for each device type and have flexibility in choosing how the network associates a device to a MUD file—it can be through explicit signaling or by pre-associating device MAC addresses before deployment.

Within the home, there are no IT staff able to customize device profiles and deployment. MUD files may be maintained by the device manufacturer or by a third party the user trusts. To give the device's user control over permissions, software applying permissions from MUD files may allow a user to grant or revoke each permission present in the MUD file, much as smartphones provide a user the opportunity to deny permissions and app requests. As MUD file adoption by manufacturers is nascent, the NRWG examined options for signaling MUD URLs, generating MUD files, and curating manufacturer files: validating them, maintaining historical files should a manufacturer stop providing one, comparing versions to detect tampering, or allowing community or user-driven modifications.

As part of its Secure Home Gateway project, CIRA and its collaborators within the group demonstrated using a QR Code to deliver a MUD URL for a device to a home gateway and applying the access controls within that file to the device. Ideally, a single QR Code on a device would serve multiple roles, acting as a "live label" that guides the user to information and support for their device, as provisioning material for WiFi Easy Connect to

<sup>24</sup> <https://datatracker.ietf.org/doc/rfc8520/>

<sup>25</sup> There are many initiatives on IoT device profiling and fingerprinting. Netherland (NL) [SIDN.NL](https://www.sidn.nl/) and Italy IIT CNR (IT) are examples of country code top-level domains (ccTLDs) developing technology to profile, fingerprint, and detect anomalies in IoT devices.



allow the device to be on-boarded onto a network with a unique credential, and for MUD signaling.

To try to address the larger problem of creating and curating MUD files, CIRA and the group have been in discussions with a wide set of global collaborators, including authors of MUD and DOTS, SIDN (the .NL registrar) lab's SPIN team—who have built IoT connectivity surveillance and visualization tools as well as their own implementation of MUD access controls, the Canadian Centre for Cyber Security, and participants at NIST's MUD Open House—on working cooperatively to develop a full set of tools to deploy MUD and related threat mitigations at the residential gateway.

Many participants and collaborators suggested that when high quality MUD files are not available for a device from its manufacturer, machine learning might be used to construct one. To do this, the gateway may actively probe or passively observe a device in order to develop a large enough body of observations to (optionally: cluster that device with identical or similar models and, for that cluster) build a compact representation of normal behavior which may be used to build MUD files as well as to detect indications of compromise or other anomalies. The IoT Analytics Project at the University of New South Wales provides an implementation of such an automatic MUD-file generator.<sup>26</sup> There is an important user-interaction component to the Secure Home Gateway effort, as light cooperation with the user is viewed as critical for onboarding and incident response.

A second prototyping effort was aimed at onboarding and the shared key problem. For physical security, keys and badges are used for access control, and users with different sets of keys can be allowed into or locked out of different areas. In a hotel, for example, guests renting different rooms are given different keys. In the home, there is generally one WiFi password—one cryptographic key.

Granting the same key to different devices prevents the gateway from enforcing differential access control. To overcome this, TELUS and Algonquin College illustrated giving each device in the home a different password,

locked to its MAC address, while still having all home devices share a single WiFi network (SSID) and use the normal WPA2-PSK authentication that all consumer devices support. Handing out different keys facilitates applying access control, and pairing keys with MAC addresses provides a cryptographic root to conventional MAC-based filtering techniques.

The participants validated the technique on a single home gateway using the popular HostAPd open source WiFi Access Point software, in a multiple access point setting with RADIUS authentication from HostAPd to a FreeRadius backend, and with web and app-based user interfaces to hand out passwords and assist in device onboarding.

The main outcome of this work is that popular existing tools are able to support device on-boarding techniques which facilitate applying access controls at the home gateway. The new Wifi Device Provisioning Protocol and Wifi Easy Connect certification offers a streamlined process for onboarding compliant IoT devices and provisioning them with unique credentials. The group has investigated ways to integrate Easy Connect and MUD provisioning, and believes that a single QR Code may function as a live label while performing Easy Connect onboarding and MUD provisioning.

## 2.3 Conclusions

The NRWG believes that insecure home IoT devices pose a large present and future threat to Internet-based services as well as to home users. This threat should be partially addressed by improvements to existing denial of service mitigations and maturation of IoT device security practices, but may also be partially addressed by improved security frameworks within the home that can place appropriate access controls onto IoT devices and allow users visibility into and control over IoT device behavior. The NRWG has outlined such a framework, and continues to work with global partners to develop, implement and standardize it.

26 <https://GitHub.com/ayyoob/mudgee>



## 2.4 Recommendations

The goal of the NRWG was to develop a security framework, running code that implements that framework, and to develop and refine user-centered onboarding and support tools for that framework.

### The key outputs of the group to date are:

1. A high-level threat list against IoT devices in the home.
2. A high-level framework for protecting IoT devices against these threats.
3. A demonstration of discovering and applying access controls using MUD.
4. A demonstration of onboarding WiFi devices with unique credentials in a way that strengthens the application of access control rules.
5. Work in progress to design and implement a fuller demonstration of the protection framework.
6. Global collaborations towards this work.

The NRWG's primary recommendation is that the Secure Home Gateway code be accepted by the core openWRT project. In the future, the NRWG aims to ensure openWRT is bundled by default with its IoT security framework, and/or that when manufacturers upgrade their openWRT software, it comes equipped with this framework. Having this group's framework as a standard means it is core to the base openWRT package.



The NRWG also created a set of recommendations for future work, including:

1. Security evaluation of any new security/user interaction mechanisms. New MUD-based access controls represent significant new attack surface and must be analyzed and tested.
2. Continued implementation of a security framework. Integration/development of:
  - a. Device fingerprinting.
  - b. Automated MUD profile generation.
  - c. MUD clearing house.
  - d. Access controls.
  - e. User controls (visibility, permissions, notifications).
  - f. Unified onboarding.
  - g. DOTS-based DDoS filtering.
  - h. Quarantine and un-quarantine procedures.
3. Standards development
  - a. Live label and their integration with network onboarding, MUD, and user-interaction.
  - b. Out of support notification/device management.
  - c. Credential management on IoT devices.
  - d. Quarantining/un-quarantining.
  - e. (MANRS<sup>27</sup>-inspired) MARIS: Mutually Agreed Norms for Internet Security.
4. Continued global coordination towards standardization, implementation, and adoption.

---

27 <https://www.manrs.org/>



# Device Labeling Working Group (DLWG)



The Device Labeling Working Group's objective was to ensure the safe use of connected devices and associated data streams through labeling that clarifies how they will protect privacy and mitigate against cyber threats.

## 3.1 Summary/Problem Statement

Labels can help consumers make smart choices when it comes to acquiring, using, and disposing of IoT devices. Consumers need to be able to rely on the information provided through a product security label, and the information needs to cover the key aspects for buyers to consider. An effective label should provide information to help consumers make well-informed decisions when purchasing and using an IoT device.

This working group asserted that through consumers making smart choices, the Canadian IoT environment will develop in a safer, more secure way, taking privacy and security into account from the outset. Consumers making smart choices results in manufacturers and businesses offering better and more secure solutions. Ultimately, this process will lead to a higher level of network resilience, both from a societal and from a personal perspective. Consumer education at all levels will need to empower consumers to make the best use of the information provided through the labels. As such, the Device Labeling Working Group worked closely with the Consumer Education and Awareness Working Group to ensure their work was complementary.

This section of the report presents the primary findings for product labeling and the need for more joint efforts, not just in Canada, but globally on security and privacy requirements for IoT. This work included cooperation and evidence sharing between the Canadian multistakeholder process and the UK Department for Digital, Culture, Media and Sport (DCMS).

When a buyer, either consumer or business, purchases an IoT product or solution, they must consider specific characteristics, including at a minimum aspects of user functionality, security, privacy, and safety. The key aspects of effective labeling are as follows:

1. **Content:** providing reliable, relevant, and useful information when it is needed.
2. **Coverage:** ensuring that all consumers of all competing products see the information.
3. **Uniformity:** using a single simple and recognizable design to facilitate comparison.

Appendix IV outlines the research into existing labeling formats and standards carried out by the DLWG.



## 3.2 Discussion

### The Need for a Labeling Scheme for Consumer IoT devices

In October 2018, PETRAS IoT Hub, the Dawes Centre for Future Crime at UCL, and the United Kingdom as part of its “Secure by Design Review” for consumer Internet of Things products, published the report “Rapid evidence assessment on labeling schemes and implications for consumer security.”<sup>28</sup>

The report found that consumers cannot distinguish between devices that offer good and inadequate security when making purchasing decisions. Instead, they must investigate the security features and capabilities of the product themselves before purchasing. This would involve evaluating technical information such as security standards compliance, what data is collected by the device and how it is shared, the length of support, and default password configuration. Default passwords can often be easily obtained from vendor sites and other sources, and therefore must be changed by the consumer.

Awareness campaigns and behavior change interventions can encourage consumer behavior and motivate consumers to routinely assess the security of IoT devices they consider purchasing. Research has shown, however, that such intervention will not be sufficient to have a real impact on consumer decisions when buying an IoT product.<sup>29</sup> A key reason is that manufacturers do not systematically communicate information about the security features that devices possess and need to be evaluated to assess their level of security. The average consumer does not have the expertise required to evaluate this information, and typically is inclined to avoid such demanding tasks, as per relevant research.<sup>30</sup> A label that consumers can relate to and that would inform

their decision-making in a meaningful way is a more achievable intervention that could influence their choices.

As mentioned, manufacturers often do not currently provide correct or accessible information to inform consumers and retailers about the level of security their devices offer. A labeling scheme would encourage manufacturers to compete on security as a form of market differentiation. It would also hold manufacturers to account by directing their attention to the security of devices according to clear criteria and guidelines. Finally, a labeling scheme would allow market oversight and consumer protection authorities to assess compliance to IoT security in a more consistent and transparent approach.<sup>31</sup>

### Labeling Formats

This group considered three primary varieties of labeling formats:

1. Descriptive information label, which details security-related information.
2. Binary seal of approval labels in which a product is certified to a certain standard.
3. Graded scheme labels that allow more critical comparisons of security-related compliance.

In order to provide more insight into the relative merits of the different types of labeling, the Device Labeling Working Group referred to critical research performed on established labeling schemes, particularly on food and energy efficiency labels.<sup>32</sup>

28 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/747296/Rapid\\_evidence\\_assessment\\_iot\\_security\\_oct\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_iot_security_oct_2018.pdf)

29 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/747296/Rapid\\_evidence\\_assessment\\_iot\\_security\\_oct\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_iot_security_oct_2018.pdf)

30 Kahneman D, Egan P. Thinking fast and slow. New York: Farrar, Straus and Giroux. 2011.

31 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/747296/Rapid\\_evidence\\_assessment\\_iot\\_security\\_oct\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_iot_security_oct_2018.pdf)

32 See Appendix VI for more information and background research.



## IoT Device Security Labeling

As possible IoT device security label formats, each of the dominant three labeling schemes has its strengths and weaknesses:<sup>33</sup>

1. The colored graded scheme would attract the attention of consumers and help them compare the security of different devices. For this implementation to be effective, the display of the graded label must be mandatory for manufacturers.
2. The binary or “seal of approval” label is typically preferred by consumers due to its simplicity, but is less effective in guiding attention and informing consumer choice.<sup>34</sup> The use of the binary label may lead consumers into a false sense of security or to assume that no intervention is required to keep them secure.
3. The descriptive information label communicates critical information to consumers and may provide helpful indicators of a device’s security readiness. The label needs to communicate the most relevant information only and not burden consumers with unnecessary information. This type of label is more suitable for the voluntary label introduction.

## Mandatory versus Voluntary Labels

The Department of Digital, Culture Media and Sport (DCMS) of the UK released their policy review for Secure by Design for consumer IoT products in March 2018<sup>35</sup> as well as a final report in October 2018.<sup>36</sup> A key measure in the report is a voluntary code of practice for manufacturers to ship products with features that make them “Secure by Design.” The report also proposed exploring the role of a voluntary labeling scheme to communicate important information to consumers that is otherwise invisible to them, or

difficult to find, such as how data collected by devices is shared and the support period for the product.<sup>37</sup>

More recently, the DCMS announced a consultation process on the government’s regulatory proposals regarding consumer IoT security.<sup>38</sup> In this consultation process, initiated in May 2019, a proposal was made for the “top three” guidelines of the Code of Practice, to become mandatory in the UK. These critical guidelines are: all IoT device passwords shall be unique and not be resettable to any universal factory default value; that the manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy; that manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

A voluntary labeling scheme would be useful as an initial step. However, for sustainable market growth and to ensure manufacturers’ adherence, as well as to maintain consumer awareness, the label must be mandatory in order to be effective, especially given some manufacturers unwillingness to display a label that indicates poor security of a product.

## QR Codes

A Quick Response (QR) code is a type of matrix bar code or two-dimensional code that can store data and is designed to be read by smartphones. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL, or other data.<sup>39, 40</sup> The popularity of QR Codes is growing all around the world. Now, mobile phones with a built-in camera are widely able to recognize the QR Codes.

33 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018,

34 Koenigstorfer J, Wasowicz-Kirylo G, Styško-Kunkowska M, Groeppel-Klein A. Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! *Public Health Nutr.* 2014;17:2115–21.

35 Department of Digital, Culture, Media and Sport (DCMS), Secure by Design Report, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/686089/Secure\\_by\\_Design\\_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report.pdf)

36 <https://www.gov.uk/government/collections/secure-by-design>

37 Id.

38 <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

39 Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang “The psychology behind QR Codes: User experience perspective”, *Science Direct, Computers in Human Behaviour* 28 (2012) pp 1417-1426.

40 Phaisarn Sutheebanjard, Wichian Premchaiswadi, “QR Code Generator”, *IEEE 2010 8th International Conference on ICT and Knowledge Engineering* (24-25 Nov. 2010) pp 89-92.



## QR Code Usage Statistics

The use of code scanning has increased during the past few years as awareness and adoption of QR Codes has grown exponentially. QR Code stats done by ScanLife show that 23 million QR Codes were scanned during the first quarter of 2015, which is nearly 10 million more than during the first quarter of 2012. Moreover, the first quarter of 2012 had posted a 157 per cent increase as compared to the first quarter of 2011.<sup>41</sup>

The age group with the highest percentage of people scanning QR Codes was 34 to 44 years in 2015. Since then, apps popular with the younger generation, such as Snapchat, Pinterest, and WeChat, have added QR Code scanning features. Therefore, the age distribution is likely to shift towards the younger generation moving forward.<sup>42</sup>

Twenty-seven million Canadians are online, representing eighty per cent of the population. Ninety-three per cent of them go online to view and verify product information. These figures have changed the way Canadian marketers and retailers engage their audience. To strike a chord with the young generation, marketers, retailers, manufacturers, and even the police have adopted QR Codes in Canada.

## Code of Practice for Consumer IoT Security

Recent research, including research by the Internet of Things Security Foundation,<sup>43</sup> as well as the UK's Department for DCMS report titled "Code of Practice for Consumer IoT Security",<sup>44</sup> have identified critical information and best practices to be followed and documented by manufacturers, service providers, retailers, and consumers. The DLWG considered each of these inputs in the development of its labeling schema.<sup>45</sup>

## Certification

Currently, there is no one single standard or recommendation that can provide product or solution assurance to security. However, there are some that will indicate that a product has undergone some evaluation and testing to get a mark. The DLWG carefully considered these schemes when evaluating its proposed solution.<sup>46</sup> Regional efforts currently underway in the UK, EU, Australia, USA, and Canada were also considered.

41 ScanLife.com, "QR Code Adoption: Trends and Statistics", [www.scanlife.com](http://www.scanlife.com)

42 QR Code Statistics 2018: Latest Numbers On Global QR Code Usage, (<https://scanova.io/blog>)

43 IoT Security Foundation, Establishing principles for IoT Security, <https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSE-Establishing-Principles-for-IoT-Security-Download.pdf>

44 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/747977/Mapping\\_of\\_IoT\\_Security\\_Recommendations\\_Guidance\\_and\\_Standards\\_to\\_CoP\\_Oct\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT_Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf)

45 See Appendix VI for more information.

46 See Appendix VI for more information.



### 3.3 Conclusions

#### Comparison of Types of Labels for IoT Device Security

This table provides a comparison between the different types of labels, focusing on their suitability as a label for IoT device security:

Type of Label	Pros	Cons	Notes
Graded/ Color Graded	<ul style="list-style-type: none"> <li>• Attracts the attention of consumers.</li> <li>• Helps consumers compare the security of different devices.</li> </ul>	<ul style="list-style-type: none"> <li>• To be effective, the display needs to be mandatory for manufacturers.</li> </ul>	<ul style="list-style-type: none"> <li>• Could be introduced at a later stage in a mature IoT Security market.</li> </ul>
Binary (Seal of Approval)	<ul style="list-style-type: none"> <li>• Easy for customers to interpret.</li> <li>• Preferred by consumers.</li> </ul>	<ul style="list-style-type: none"> <li>• Less effective in guiding consumer choice.</li> <li>• Gives (false) sense of security and belief that no additional action from consumer is needed.</li> <li>• Does not automatically reflect current security status or new product vulnerabilities.</li> </ul>	<ul style="list-style-type: none"> <li>• Example is BSI Kitemark in the UK.</li> <li>• Combine binary/seal of approval label with another informative label (e.g. live label).</li> </ul>
Informative	<ul style="list-style-type: none"> <li>• Communicates critical information to consumers.</li> <li>• Provides helpful indicators of a device's security readiness.</li> <li>• More suitable for voluntary label introduction.</li> </ul>	<ul style="list-style-type: none"> <li>• Need to limit display to most relevant information.</li> </ul>	<ul style="list-style-type: none"> <li>• Suitable for market introduction and to help build consumer understanding and trust.</li> </ul>
Live label (e.g. QR Code)	<ul style="list-style-type: none"> <li>• A form of informative label.</li> <li>• QR Codes are gaining adoption from manufacturers as marketing tools</li> <li>• Provides link to current information on product security.</li> <li>• Allows consumer to get information beyond security compliance, e.g. deployment recommendations, data collection/sharing information, latest vulnerabilities.</li> </ul>	<ul style="list-style-type: none"> <li>• Requires consumer to scan QR Code and spend time going through relevant information.</li> </ul>	<ul style="list-style-type: none"> <li>• Suitable for market introduction and to help build consumer understanding and trust.</li> </ul>



## Live Label Requirements and Structure

As many of the labels represent a static view of a product at a specific time within the product lifecycle, there is a need to ensure that a dynamic view of the product is available to users. The concept of a “live label” is not new; however, based on the discussions within the multistakeholder process, it became clear that a different approach to labeling is required.

A live label will provide a near real-time view of any product’s security risks. As many products undergo formal testing and evaluation, there will be aspects of the software components that could provide no risks one day but, due to a zero-day discovery and/or malware, the components and possibly the product will be prone to compromise. The need to be able to provide a single source of information for product buyers is becoming more critical. As many vendors do currently offer support sites, the additional elements recommended are not a far reach to meet the necessary requirements to offer a comprehensive view of an IoT product’s risks.

### Requirements:

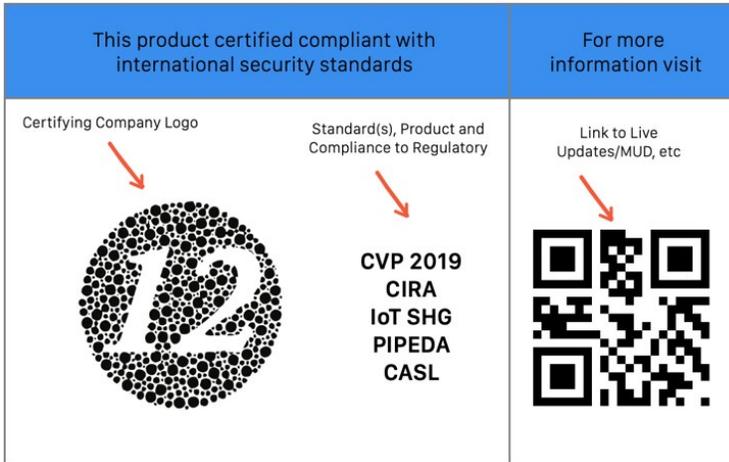
1. A web page accessible by secure means (such as https and encryption) containing specific details of each product or a group of products provided by the vendor, including:
  - a. Product firmware updates.
  - b. Product security alerts and announcements, including any CVEs and CVSS registrations.
  - c. Policies for privacy and vulnerability disclosures, including any recent changes to data collection policies or practices.
  - d. Contact details for either phone, web, or email support that will result in a minimum response of seventy-two hours.
2. The web page should contain additional details, such as:
  - a. “How To” and user guides for secure setup and configuring the IoT device(s).
  - b. References to updated certifications and/or attestations obtained.
3. The web page may contain supporting details, including:
  - a. Third party organizations who conducted formal testing and assessment to recognized standards and attestations.
  - b. Alert levels for cloud hosting and online system availability.
4. Use an electronic coding scheme that will allow users to quickly find the “live label” website.
5. Additional fail safes that will prevent the counterfeiting of labels placed on products.

### A security product label should also have the following structure:

1. Clearly identify the organization that performed the formal testing and assessment.
2. Clearly identify the standard and product being tested and assessed.
3. Include a holographic, embedded RFID tag or other means to prevent counterfeiting.
4. Provide a machine-readable code that can be used to provide updates to date and live information on the specific instance of the product. This can be hosted on the current company or product website and should include the following:
  5. Product model and/or version number.
  6. Latest product firmware version number.
  7. CVEs or CVSS references.
  8. Security configuration guide.
9. Proposals for IoT Device Labeling



## Proposal One of IoT Device Security Label



Reference Sample ONLY

## Label Proposal One

The reference example above indicates what a proposed “live label” might look like. This indicates the three key elements, including the name of certifying company, product, standard, compliance, and link to live site. While not completely fool-proof, it does provide additional information that a user can use to validate a label. If the vendor attempts to falsify all of these details it would clearly indicate a liability situation.



## Proposal Two of IoT Device Security Label



### Label Proposal Two

Following the comparison between the benefits of the different label formats, the proposed approach is to combine the consumer trust factor of known “trust marks” such as for CE in Europe, Kitemark in the UK, or CSA in Canada, with advanced and critical product security information that is difficult to display on a label, and have the nature to change over time.

Key information to be conveyed by the label should include:

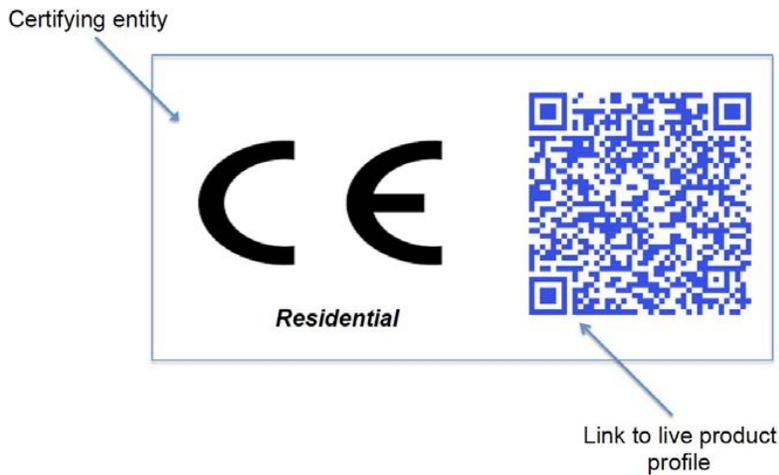
1. Formal testing and certification have been performed on the product.
2. Where to get up-to-date critical information on product security features and installation/deployment considerations.

Main aspects to be covered by a security product label are:

1. Identification of the organization overseeing/authorizing the certification and formal testing (e.g. BSI Kitemark, CE mark, CSA mark).
2. A machine-readable code that is linked to a URL providing up-to-date product information (i.e. a live label). The website should include the following:
  - a. Product model and/or version number.
  - b. Latest product firmware version number.
  - c. Recent vulnerability information.
  - d. Certification/testing framework.
  - e. Security configuration guide.
  - f. Information on what data is collected and how it is shared.



## Proposal Three of IoT Device Security Label



### Label Proposal Three

In the Label Proposal Two, the entity overseeing/authorizing the product certification and testing is the CTIA, while the device tested is the Amazon Alexa smart home assistant. The testing and assessment are performed against the Online Trust Alliance (OTA) framework v2.5.<sup>47</sup> The QR Code (i.e. live label) points to the product site with up-to-date product information.

The Label Proposal Three presents a simpler label format, focusing on the CE label<sup>48</sup> (the European Certification) and the QR Code of the product being certified (e.g. Amazon Alexa). Information regarding the standard used in the testing and certification is available on the product site, accessed by scanning the QR Code, instead of being explicitly mentioned on the label. Potentially the word "Residential" could be added in the label to indicate the intended usage of the product.

We believe Label Proposal Three qualifies as a simpler and easier to understand label.

<sup>47</sup> [https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework6-22.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf)

<sup>48</sup> It should be noted that in the UK DCMS "Consultation process on the government's regulatory proposals regarding consumer IoT security", a proposal for a labeling scheme is introduced. The label is based on a combination of a binary label that indicates if "Essential security features are included", and a label for the length of time security updates are provided by the manufacturer.

## 3.4 Recommendations

3. Approach and collaborate with other organizations focusing on IoT security and privacy such as the NIST, ENISA, IoT Security Foundation, IoXT, IoTAA, UK DCMS, ETSI and EU in an attempt to reduce the amount of fragmentation in the market for initiatives and labels to avoid consumer confusion.
4. Continue to influence the standards effort through the ISO/IEC for international standards and SDOs with similar projects and interests.
5. Collaborate with the Online Trust Alliance (OTA) to approach key vendors and solution providers to raise awareness on the need for security certification and device labels.
6. Determine the best organization to provide a formal specification of the “live label.” This could be IETF or similar, and includes further developing the live label (QR Codes) proposal through collaborating with other organizations such as the OTA.
7. Elevate the proposed voluntary labeling framework as a model for consumer IoT device manufacturers to demonstrate their compliance with existing Canadian law and regulations in this space, including but not limited to the *Canada Consumer Product Safety Act*, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, and the *Canadian Anti-Spam Legislation (CASL)*. This also reveals that the ‘gap’ is the lack of a clear and consistent way for manufacturers to indicate that they complete the certification with certain standards, and provide additional information that makes them compliant with these laws. This in turn situations the proposed voluntary labeling framework as a flexible, user-friendly framework to apply in order to advertise their compliance and effort put towards reducing risks associated with IoT devices.
8. Further assess the certification and testing of applications that control devices and backend support services, in addition to focusing on the devices themselves.

### The key findings for this working group include:

1. Security labels need rules for appearance and what information to include.
2. Consumers need more education on types of labels and what they actually mean for security and privacy implications.
3. Canada needs to find ways to work globally to eliminate duplication of effort for security and privacy labeling.
4. We need to consider compliance to Canada laws for PIPEDA and CASL for vendors and how this is reported to consumers or integrated into a label.
5. While labeling for most products should be voluntary, in some sectors it should be mandatory where personal safety could be at risk.

National and international standards will continue to be improved by members of this group, including the T200 and the SC27030.



# Consumer Education and Awareness Working Group (CEAWG)



As more consumers adopt IoT solutions in the home, their role in the overall security and privacy of IoT increases. Consumers are also required to take a more active role in purchasing and in their home security and privacy.

## 4.1 Summary/Problem Statement

Well-informed and empowered consumers are more likely to trust and engage with the IoT industry; demanding consumers also place pressure on businesses to be more innovative and competitive in order to earn their business. Educating consumers about IoT risks and opportunities has the potential to be beneficial for consumers, businesses, and the economy.

The focus of the Consumer Education and Awareness Working Group (CEAWG) is on household and business IoT devices. Systems that include many connected devices and complex systems, such as autonomous vehicles and smart cities, were not included in its analysis.

### Shared Responsibility Framework

A Shared Responsibility Framework (below) is used to illustrate how demand and supply sides of IoT devices can collaborate to bridge the gap between the ideal situation/behaviours that are outlined for consumers and the status quo by engaging the diversity of actors (expertise/stakeholders/forces/incentives/trusted authorities). This Shared Responsibility Framework broadly organizes the ideas into the demand side and the supply side, which can work collaboratively over the lifecycle of the device:

1. Demand side: The expectations of the consumers who are active users of the IoT device.
2. Supply side: A broader category of stakeholders who are either directly or indirectly involved in the supply chain of the device.

Appendix V includes an evaluation of existing educational resources carried out by the CEAWG.



## 4.2 Discussion

The approach taken by the working group was to involve all stakeholder groups, including consumers. IoT consumer device manufacturers are the main targets of the CEAWG. The principal output of this working group is the Shared Responsibility Framework of key messages about behaviours and recommendations that need to be communicated to consumers, manufacturers, retailers, service providers, governments, civil society, educational institutions, and others. A list and evaluation of existing educational products is included in Appendix V.

A website/repository with the information below and relevant links will be available on the Enhancing IoT Security initiative website.<sup>49</sup>

The CEAWG first focused on reaching consensus on the content of key messages, then turned its attention to how this content will be translated into a full-scale Consumer Education and Awareness Campaign. Throughout the process of creating the content, several issues and considerations arose. In rough chronological order, the considerations for future work are as follows:

### Evaluating the Varying Elements of Key Messages<sup>50</sup>

1. **Scope of application:** General messaging was adopted instead of instructions for specific device/systems. The impact of this scoping of the content of the messages needs to be further considered.
2. **Product range:** How do the messages differ when applied to high-security products (i.e. vehicles) vs. low-security (home appliances)?
3. **Audience:** Target seniors, youth, newcomers, low tech literacy, or all IoT consumers? One approach to consider the audience perspective is to run a thought exercise for a consumer's use of devices (i.e., imagine scenario of device setup and assess which key messages will be most relevant and salient).
4. **Link to Smart Cities:** Consider the application of the WG's conclusions/key messages to educate citizens on smart cities (i.e. traffic lights, smart sidewalk, etc.)

### Linking Consumer Education and Awareness Messaging with Labeling Options<sup>51</sup>

How does the message promote use of the label by businesses and consumers and how can the label serve as a link to the content? For example, if the delivery of these messages relies on the QR Code model as proposed by the labeling WG, this assumes the users have access to a smartphone, which may affect use.

### Options for Information Dissemination

Awareness activities will largely need to be tailored to various audiences (e.g., youth, elderly, etc.), recognizing how to best convey the content to them. Resource requirements and delivery mechanisms (e.g., social media campaigns vs. traditional advertising, etc.) also need to be tailored to each audience.

---

49 The Consumer Education and Awareness Working Group will provide links and relevant information for inclusion on this webpage, which will be maintained by the Internet Society: <https://iotsecurity2018.ca/consumer-education-and-awareness/>

50 We wish to note that the CEAWG agreed that initial messaging will be developed using all consumers as the intended audience. Future efforts may take place to develop messages aimed at specific groups of consumers such as youth, seniors, and more tech-savvy demographics.

51 See also the information in the Device Labeling Working Group section above.



## Campaign Evaluation

In order to properly assess the effectiveness of the campaign message, a process must identify and validate consumer behaviour and reaction to key messages. Indicators of impact will be important to consider, including changes to consumer behaviour, complaints, the impact on purchasing (brands, types of devices, and devices with labels vs. devices without labels). Metrics showing the popularity of websites or other channels that deliver the content of the key messages will also be important.

Additional tools that can be explored to support consumers include a) redress mechanisms and consumer support beyond this educational campaign and b) ongoing development of the Canadian Cyber Centre's one stop shop and point of contact for reporting cybercrime.<sup>52</sup>

---

52 <https://www.cyber.gc.ca/en/>



## 4.3 Recommendations

All the messaging contained in the Shared Responsibility Framework (below) are considered recommended behaviours for consumers and industry:

### SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/Civil Society/Educational Institutions
Before Purchasing	Understand and consent to how the device is collecting, using, and sharing your data.	Improve accessibility and content of privacy policies (i.e., provide clear answers on how the device is collecting, using, and sharing data).
	Ensure that the device comes from reputable/certified manufacturers (i.e., low cost devices typically come with greater risks. Any smart devices that are connected to the Internet carries a risk of breach).	Clearly lay out the shared responsibility regarding the device's security (i.e., convey expectations of consumers' awareness/responsibility in the instructions/ToS/warning leaflet of the device).
	Check if there are any extra functionalities (i.e., is the device collecting unnecessary data that could create unnecessary risk? Can you opt out of future features without opting out of security updates?)	Clearly indicate/disclose all functionalities of the device and how to minimize unnecessary functions (i.e., develop a list of sensors in the device, provide information on how to turn off video and audio recording, clearly indicate if new/extra functionalities have been included in updates, and if/how it is possible to opt out of these functionalities).
	Check for user reviews, labels, and certifications (i.e., label and certification indicate that the device has been tested).	Use certification/adherence to laws, standards, and non-binding best practices as a publicized selling feature.
	Consider the lifecycle of the device and the support available to keep your device in use for as long as possible (i.e., verify availability and duration of security upgrades and patches).	Use availability/duration of patches, updates, and support as a publicized selling feature.
	Check that the device works even without Internet connection, and assess functionality in the event the device outlives the company (i.e., smart lock, camera, fridge still function even if the Internet is down or the company no longer exists).	Ensure the devices can still function without Internet connection, and if the company ceases to exist.



DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/Civil Society/Educational Institutions
At Use/Issue	Know where to seek redress and address technical problems, including if your device has been compromised, and keep record of your purchase.	Provide transparent and accessible instructions on seeking redress.
	Follow best practices for network setup and configuration to help mitigate risk when using IoT devices.	Assist consumers to set up their IoT networks consistent with best practices (i.e., make the default setting consistent with best practices).
	Be considerate of the implications or impacts on guests or others who are in the vicinity of your device (i.e., consider notifying your guests when in proximity to your smart home devices, or turning devices off).	Remind consumers about the effects of their IoT devices on their guests (i.e., audio or video recording).
	Be aware that the security of your device is constantly being updated. Ensure that the device is able to receive updates.	Remind consumers to follow recommended security best practices (i.e., follow recommended upgrading and patching recommendations from the NTIA Multistakeholder Process). <sup>53</sup>
	Ensure that each device in your home is secured. The security of your home network is only as good as its weakest link.	Consider providing mechanisms to warn consumers when issues arise (i.e., assist consumers in monitoring their traffic to detect anomalies).
End of Life/Use	Remove data from your device before disposing or moving. Many guides are available to assist users with specific IoT devices (i.e., Nest Thermostat <sup>54</sup> ).	Clearly indicate the best method or provide consumer assistance to permanently remove data from device.
	Do not forget to revert back to factory default settings. Many guides are available to assist users with specific IoT devices.	Clearly indicate the best method or provide consumer assistance to revert the device to factory default settings.
	Check the resources that are available to help dispose of IoT devices responsibly. Retailers may provide this information.	Provide resources to help consumers dispose of their IoT devices responsibly.

#### Additional information

For more information on the Consumer Education and Awareness Working Group, please see their draft report on the Enhancing IoT Security website.<sup>55</sup>

53 [https://www.ntia.doc.gov/files/ntia/publications/ntia\\_iot\\_capabilities\\_oct31.pdf](https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf)

54 <http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/>

55 <https://iotsecurity2018.ca/consumer-education-and-awareness/>



# Inter-Group Collaboration



When the multistakeholder group first selected its three working groups—Consumer Education and Awareness, Device Labeling, and Network Resilience—they were treated as separate, but interrelated, entities.

As the project moved forward and the working groups developed their resources and outputs, they also became more tightly interwoven. Continuing to foster the ties between all three groups and encourage their collaboration will be critical.

The Network Resilience Working Group’s primary recommendation is to ensure that all home gateway open source software has a Secure Home Gateway (SHG) framework as part of the core software. The SHG is made up of two parts: (1) the secure router and (2) an application on users’ phones or tablets that allows them to see the MUD files of all the IoT devices connected to that router. If and when an IoT device begins to malfunction by sending unusual amounts of data, or sending data to unusual places, or another security breach indicator, the application will notify the user and allow them to simply quarantine the device through their application until the problem is resolved.

The SHG is an excellent step toward a more secure network of things. However, when the SHG is produced, users will need a way to understand whether the devices they have already connected to the router are secure.

If a certification label were included in or alongside the MUD files in the user’s application, even the most basic users would understand whether the devices they have connected in their homes are secure. A label that meets both national/regional (T200) and international (SC27030) levels will allow users to easily understand the impact their devices may have on their network and which devices are most or least likely to have a security problem.



Together, the Network Resilience Working Group's SHG and the Device Labeling Working Group's label and standards development can create a more secure, easier to understand landscape for consumers, which will directly affect the way they interact with the devices in their homes.

However, without consumer education about the importance of SHG and labeling, it will be significantly more challenging for these to be widely adopted. That is why the Consumer Education and Awareness Working Group will need to focus their attention on supporting the other two Working Groups by sharing the message of the work they have carried out and the impact it can have on consumers in the context of the Shared Responsibility Framework.

Through the creation of their dynamic coalition in the implementation phase of this process, the Consumer Education and Awareness Working Group will be able to rapidly respond to new developments from both the Network Resilience and Device Labeling Working Groups and assist in all public-facing outputs. They will have a direct window to consumer needs and can also report back to the other two groups if any developments are inaccessible or difficult for consumers to understand.

Though all three working groups are independently focused on their own priorities, they all have an intertwined role to play in securing the Internet of Things. Without any one group, the other two would limit their success.



# Youth Perspectives



This report explores the IoT security and privacy climate by examining existing digital literacy pedagogies and interventions as well as youth attitudes, beliefs, and behaviours toward IoT and privacy.

EXCERPT IS DRAWN FROM “YOUTH AND THE INTERNET OF THINGS IN CANADA: PERSPECTIVES ON PRIVACY, SECURITY, AND ENGAGEMENT IN THE DIGITAL AGE.”<sup>56</sup>

While the survey conducted for this report has a limited scope, the work is important because it is the first of its kind. It lays the groundwork and offers recommendations for a future survey engaging Canadians with IoT security issues, and features a lengthy discussion section on this particular area. The youth report authors believe that policy should be backed by evidence, and thus they advocate for a large-scale, representative, and nationwide survey, building upon their findings and limitations, in order to adequately assess attitudes toward IoT and how best to engage youth in understanding its implications.

<sup>56</sup> “Youth and the Internet of Things in Canada: Perspectives on Privacy, Security, and Engagement in the Digital Age,” prepared by the Youth Internet Governance Forum for the Canadian Multistakeholder Process of Enhancing IoT Security. <https://iotsecurity2018.ca/wp-content/uploads/2019/01/Youth-and-IoT-in-Canada-Report-1.pdf>.



## 6.1 Methodology

### Survey

The aim of this online survey was to provide an overview of IoT device usage by young people in the context of both at-home and wearable use; to document youth awareness of IoT security issues; and to understand how individuals in this demographic consume media. In order to achieve this, the youth reporters circulated a survey through their networks, as well as through social media channels to garner responses from youth internationally. The data obtained from the survey was supplemented by insights from the 13th Internet Governance Forum (IGF), the ICANN63 Public Meeting, and the 2018 GovTech Summit.

### Survey Development and Pilot Testing

The survey was developed with the intention of collecting both quantitative and qualitative responses, as the researchers were interested in acquiring both statistical understandings and more subjective exploratory perspectives. To this end, the survey is comprised of a variety of question types including multiple choice questions, open-ended written responses, and Likert scales. To build the survey, they used Google Forms, primarily for its simplicity, ease of use, and visualizations. In developing the survey, careful attention was paid to the verbiage and wording in order to minimize bias and ensure neutrality. This process involved consulting members of the Youth IGF at an IGF session, and revising aspects of the survey based on their feedback. Data was anonymized as much as possible so that participants would feel comfortable providing truthful responses. Further, the length and time to complete the survey were carefully considered in order to ensure participants would complete it. Overall, thirteen questions were included, with the survey taking roughly two to three minutes to complete.

## 6.2 Summary of Findings

### IoT Use

The survey generated some novel insights into the use of IoT technologies by young people. Perhaps unsurprisingly, wearable devices such as smartwatches and fitness trackers (e.g. Apple Watch or Fitbit) and smart speakers (e.g. Amazon Alexa or Google Home) are the two leading IoT uses among youth. Several individuals stated that they interacted with multiple IoT devices, due to both their own ownership and their family's usage of IoT devices at home. However, the majority of youth do not identify themselves as frequent IoT users. About one-third considered themselves to be daily or weekly users; nearly one-third stated that they used it occasionally; and over one-third of youth indicated that they 'rarely' use IoT. Interestingly, these results match those of a 2017 survey by the Association of Energy Services Professionals (AESP) and Essense Partners which showed that millennials do not use IoT as much as older age groups.<sup>57</sup>

### Awareness of Security and Privacy Issues

On a scale of one to five, with five being 'Completely Aware,' the majority of respondents identified as having a mid-range (three or four) awareness of security and privacy issues related to IoT devices. But when asked to identify their level of concern, with five being 'Very Concerned,' the majority indicated a higher range (four or five). Despite enjoying the benefits of IoT usage that the majority of responses seem to exhibit, the attitudes towards IoT devices are decidedly more mixed. Many responses showed awareness of the security and privacy issues around these devices across a variety of contexts, specifically surveillance and tracking and associated data (mis)use.

Participants demonstrated a high-level of awareness regarding the ecosystem of these devices and their functions, but admitted that they lacked specific knowledge of the technical considerations of IoT device insecurities.

57 Research, Navigant. "IoT and Millennials." Forbes. March 24, 2017. Access January 1, 2019



## Engagement

Much like engaging other groups, engaging youth requires not only understanding where they are most reachable but also how best to reach them. It is no surprise that engagement is now often digital by default, leveraging the reach of various platforms online to enable more widespread information dissemination and interactivity.

### 6.3 Areas for Additional Research and Recommendations

1. **Education:** For youth especially, education policy is critical. Provincial and federal governments should work together with civil society organizations on curricula and programs that can offer forums for discussion and awareness of IoT and other tech-related issues across Canadian educational institutions.
2. **Conversation:** One of the strengths of social media as a medium of engagement is its ability to bring people into a conversation and generate widespread interest in specific topics or events through the multiplying effects of personal networks. Catalyzing authentic personal interest and curiosity through open dialogue which connects a specific issue like IoT security to broader social narratives or concerns is the most effective means of spreading awareness and inspiring action.
3. **Exploration:** Effective engagement and capacity building will also require a deeper dive into assessing the current state of young people's interaction with digital platforms and their knowledge when it comes to not only IoT security but other topics in the tech sphere such as data and privacy rights.
4. **Improving diversity and multistakeholder access:** Engagement opportunities should be promoted, and not skewed to certain types of organizations over others.
5. **Embed participation:** Avoid requiring significant amounts of additional time from young people by incorporating opportunities to learn about and engage with IoT and other emerging technologies, as well as to participate in policy making, into regular education or training activities.
6. **Policy changes:** European-style privacy laws such as the General Data Protections Regulation (GDPR) can inform and inspire the basis for regulatory and legislative approaches towards data protection reform with respect to IoT devices.
7. **Collaboration:** Internet governance involves a variety of organizations from a myriad of backgrounds. The topic of IoT security spans multiple interrelated issue areas, each serving as the focus of a number of these groups. In order to prevent duplication of efforts, collaboration and harmonization must increase between these groups at both the community and international level.

