Policy Toolkit on IoT Security and Privacy

August 2020

Internet Society

Table of Contents

Icons

Principle

Challenge

Recommendation

Example

Case Study

1. About the Toolkit

The *Policy Toolkit on IoT Security and Privacy* is a practical resource for policymakers and regulators to strengthen the security and privacy of IoT systems to protect individuals, businesses, and governments.

Many of the actions that are needed must be taken by IoT manufacturers and service providers. But these entities may not have the expertise or incentives to incorporate security, privacy, and data protection in IoT devices and services. Meanwhile, many consumers still lack awareness about the risks posed by IoT, and how to protect themselves and others.

There is a critical need for the public sector to **lead, guide, and support** the adoption of security and privacy standards, and of best practices in IoT. Governments can facilitate a collaborative approach[1] to tackling these challenges by engaging with the IoT industry and industry associations, the technical community, academic institutions, consumer protection organisations, and other stakeholders within and across national borders.

This toolkit is based on the following references from the Internet Society:

- Online Trust Alliance (OTA), IoT Security & Privacy Trust Framework, https://www.internetsociety.org/iot/trust-framework/
- IoT Security for Policymakers, April 2018, https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/
- IoT Privacy for Policymakers, September 2019, https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/
- The Economics of the Security of Consumer-Grade IoT Products and Services,
- April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

2. Introduction to IoT

2.1 What is IoT?

The Internet of Things (IoT) is the rapidly expanding network of devices, sensors, physical objects, services, and applications that are connected to the Internet.

Examples include wearable technology like smart watches and fitness trackers, self-driving cars, home automation that can control appliances, lighting and security systems, and smart cities.

By 2020, IoT devices are set to outnumber people globally by five to one.[2]

IoT devices generate vast quantities of data from their surroundings, including audio, images and videos, and environmental sensor data, which are then transmitted via the Internet and analysed to create insights for organisations and industries.

[1] See Internet Society, Collaborative Security: An Approach to Tackling Internet Security Issues, April 2015, https://www.internetsociety.org/collaborativesecurity/

[2] Internet Society, IoT Security Policy Platform Wants to Raise the Bar on Global IoT Security, 14 November 2019, https://www.internetsociety.org/blog/2019/11/iot-security-policy-platform-wants-to-raise-the-bar-on-global-iot-security/

The International Data Corporation estimates that over 40 billion connected IoT devices will be producing 80 zettabytes of data by 2025.[3]

The IoT market can be broadly divided into **consumer IoT** and **industrial IoT**:

Consumer IoT devices make up the largest share of the total IoT market. This segment (excluding smartphones and tablets) comprises a major share of the total installed base of IoT devices.[4]

The consumer IoT market falls into three main categories:[5]

1. **Home and residential** – e.g., smart TVs, smart appliances, voice-activated home assistants, home automation tools such as smart lighting, home monitoring and security products, wireless printers and scanners, baby monitors and smart toys.
2. **Transportation** – both in-vehicle and external systems linked to personal transport.
3. **Health, fitness and personal** – e.g., personal safety alarms, healthcare devices, and wearable technologies like smart watches and fitness trackers.

Home and residential IoT devices make up the largest segment of the consumer IoT market. Globally, the dominant consumer IoT device is the smart TV: Between 25% and 35% of consumers worldwide own a smart TV that can connect to the Internet.[6]

Industrial IoT includes the use of IoT by enterprises to optimise business processes (supply chain, inventory, maintenance), enhance user experience (retail, delivery) and resolve business challenges. For instance, enterprises use the data generated by sensors to monitor their systems in real time and make them more efficient.

Governments are also deploying IoT to enhance the efficiency of critical infrastructure through initiatives like smart grids for electricity, gas and water, smart cities and intelligent transportation.

2.2 Why is IoT important?

Rapid development and innovation in IoT provide enormous potential for economic growth and social advancement.[7]

IoT is a significant driver for big data analytics and machine learning projects because it allows businesses to create vast datasets from network-connected sensors and devices, often in real time. This data collection also

[3] International Data Corporation, The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, 18 June 2019, https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[4] Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, 7 February 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[5] Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[6] Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[7] Thierer, Adam/O'Sullivan, Andrea, Projecting the Growth and Economic Impact of the Internet of Things", MERCATUS Center Technology and Innovation Policy Briefs, June 2015, https://www.mercatus.org/publications/technology-and-innovation/projecting-growth-and-economic-impact-internet-things, Kranz, Maciej, IoT For Economic And Social Good: How The Internet Of Things Makes Our World Better", Forbes Magazine, 14 June 2018, https://www.forbes.com/sites/forbestechcouncil/2018/06/14/iot-for-economic-and-social-good-how-the-internet-of-things-makes-our-world-better/#8f8a79f100f6

poses significant threats to privacy, which are often not apparent to, nor within the control of, device users – or anyone venturing into proximity of these devices whether they know it or not.

It is also critical to the deployment of smart grids, smart cities and intelligent transportation initiatives. For example, connected sensors around a city can help planners improve traffic flows.

When IoT is combined with big data analytics and artificial intelligence, as well as developments in cloud computing and 5G, it can produce transformative impact on all sectors of the economy[8].

However, these opportunities come with significant security and privacy risks. Many of the IoT devices available now lack basic security features or adequate user interfaces, or ability to control them even if they are present, and compromised devices can be entry points for cyberattacks, jeopardising sensitive data and threatening the security and privacy of individuals, businesses and governments. Further, many IoT services do not apply best practices privacy standards.

An Internet Society study shows that while many governments have created strategies for developing the IoT industry, these have often not been accompanied by measures to address security and privacy challenges.[9]

2.3 Why do policymakers and regulators need to care about IoT security and privacy?

IoT-related cyberthreats will likely continue to rise at a rapid rate, at least in the short term – a trend that could have devastating effects on Internet users and the Internet's core infrastructure.[10]

There are two distinct security and privacy risks in IoT systems:

1) An IoT system can be attacked, exposing users to security and privacy risks. Examples include:

- Listening to conversations and watching you from a smart TV's built-in microphone and video camera[11]
- Controlling smart home appliances and systems or connected cars, and causing them to behave in unwanted and potentially dangerous ways[12]
- Tracking homeowners through home security systems[13]
- Obtaining private video feed from a baby monitor or connected home security devices[14]

[8] 5G for Smart Manufacturing – Insights on How 5G and IoT Can Transform Industry, GSMA report on 23 April 2020 https://www.gsma.com/iot/resources/pa-consulting-5g-iot-smart-manufacturing/, Tamsons, Asa, "How 5G and the Internet of Things can create a winning business", World Economic Forum Annual Meeting Article, 8 Jan 2020, https://www.weforum.org/agenda/2020/01/what-does-5g-and-the-internet-of-things-mean-for-business/

[9] Cullen International, International Comparison of Regulation of Consumer IoT: A study for the Internet Society, August 2018.

[10] According to a study by the Internet Society, it appears unlikely that market-driven security improvements will spread widely and quickly enough to offset the rapid growth of consumer IoT devices, at least in the short term. Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[11] Steven J. Vaughan-Nichols, How to keep your smart TV from spying on you, ZDNet, 8 March 2017, https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/

[12] Technology.org, 3 Risks of Smart Home Technology & How You Can Stay Safe, 6 June 2018, https://www.technology.org/2018/06/06/3-risks-of-smart-home-technology-how-you-can-stay-safe/

[13] Danny Palmer, 175,000 IoT cameras can be remotely hacked thanks to flaw, says security researcher, ZDNet, 31 July 2017, https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/

[14] Dan Goodin, 9 baby monitors wide open to hacks that expose users' most private moments, Ars Technica, 3 September 2015, https://arstechnica.com/information-technology/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/

- Monitoring children's location, eavesdropping on conversations and even communicating with children through their smartwatches[15]

For industrial IoT systems, the stakes are even higher: Potential threats include industrial espionage and destructive attacks on critical infrastructure.

2) Compromised IoT devices can be used to launch attacks against third parties or other systems.

Vulnerable devices like connected home appliances can be infected with malware to become part of a botnet – a network of thousands or millions of infected connected devices under the control of an attacker. A botnet can be used to send spam, steal user credentials, distribute malware, commit online advertising fraud, mine cryptocurrency or launch a distributed denial-of-service attack on a global scale.

IoT systems must therefore be secured against risks to direct users and their assets (inward security), as well as to other networks and users (outward security).

Several traits unique to IoT devices and systems present new security and privacy challenges that were not present in traditional computing systems:

- Deployment on a massive scale – The large number of devices, and corresponding interactions with other devices in the network increase the "surface" available for cyberattack.
- Volume of identical devices – Many IoT deployments consist of collections of identical or near-identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics.
- Connection between physical and digital worlds – Hacking into IoT devices can have dangerous real-world consequences, providing hackers access to confidential information or control over connected systems linked to critical infrastructure.
- Designed for long service life but no or limited upgradability or patching – Devices such as smart refrigerators or home routers may still be in use long after the manufacturer or service provider has stopped providing security updates to them, while some devices may not have been configured to accommodate upgrades at all.
- Limited user interfaces and control over devices – Many IoT devices collect data on individuals but often have no interface to allow users to adjust privacy preferences. This amplifies concerns about the potential increase of tracking and surveillance.
- The potential to re-identify de-identified data – The sheer scale of data that can be aggregated poses a great risk to privacy. IoT devices may collect data that is harmless on its own, but when collated and analysed with other data over time, it can reveal very accurate information about individuals' habits, locations, interests, and activities, resulting in increased user traceability and profiling. Already, these large datasets are being used by businesses to offer differential prices to consumers. It can also be used by those in positions of power to discriminate against specific groups, leading to denied access to services and employment, and to harassment and violence.
- Increased sensor scale and proximity – IoT allows close-up monitoring of people's faces, bodies and movements, and makes people more identifiable in public and private spaces. One of the most ubiquitous IoT sensors is the camera. Coupled with advances in facial recognition and other analytic technology, IoT devices allow people to be identified or singled out wherever these cameras are present. As a cloud service, facial recognition is likely to be cheaply available to many IoT manufacturers and service providers.

[15] Danny Palmer, Security flaws in children's smartwatches make them vulnerable to hackers, ZDNet, 18 October 2017, https://www.zdnet.com/article/security-flaws-in-childrens-smartwatches-make-them-vulnerable-to-hackers/

IoT is a complex system and involves many stakeholders. IoT is made up of sensors and devices, the apps and platforms used to manage them, and associated cloud and web services.[16] Security and privacy must be ensured in all parts of the connected system, as vulnerabilities in any given component can potentially compromise the entire system. The security of a system is only as strong as its weakest link. This means that entities in the IoT ecosystem need to work collaboratively to ensure that security and privacy are protected.

Relevant stakeholders include: device and sensor manufacturers, app developers, app services operators, platform developers, platform operators, protocol developers, network operators, retailers and resellers, policymakers and regulators, and users (these include individuals, businesses and governments). See Box 1 for an example of an IoT value chain.

Box 1: Petcafe's Value Chain[17]

PetCafe has designed a device that allows cat and dog owners to track their pets' movements.

For PetCafe's device to deliver its functionalities, the company engages with:

- Sens-data, a small business whose sensors are integrated into the device to capture information about the pet's movements.
- A specific IoT platform and application designed and run from AppMore. AppMore translates, processes and prepares the data captured from the sensors for transmission to the owner.
- Rolling Telecoms, a mobile network company that enables data connectivity, and establishes and manages the data exchange between the tracking device (which has a SIM slot) and the pet owner's smartphone.

As a result of the integration and cooperation of all these actors in the IoT value chain, pet owners are able to access the PetCafe application on their smartphone and track the location of their pets.

The sensors by Sens-data, IoT platform and application by AppMore, and the mobile network of Rolling Telecoms must all have strong security and privacy measures in place to minimize threats to the whole system.

Often, these components and the entities responsible for developing and maintaining them are in different jurisdictions (e.g., a server may be located in one jurisdiction, while the device may be manufactured in another, and in use in yet another), which means cross-border coordination and cooperation is crucial to solving IoT security and privacy challenges. Toward this goal, the Internet Society started the IoT Security Policy Platform[18] in early 2019. It is a collaborative body of government agencies and global organizations working to harmonize and promote best practices in IoT security among manufacturers, retailers, policymakers, regulators, and consumers, and to address key challenges to the ecosystem.

Individuals must be able to trust that the custodians of the data collected by IoT devices will treat their personal information respectfully. In the absence of trust, people will not embrace IoT devices, fearful that their data will be insecure or shared inappropriately.

[16] See IoTAA, IoT Reference Framework, November 2018, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf The IoTAA IoT Reference Framework shows all the layers where security, privacy and safety need to be considered in the IoT ecosystem.

[17] This example is taken from: Consumers International, Consumer IoT: Trust by Design 2019 – Guidelines and Checklists, 2019, https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf

[18] https://www.internetsociety.org/iot/iot-security-policy-platform/

IoT is poised to transform economies and societies worldwide. The technology brings enormous opportunities but also significant risks. We are at a critical juncture at which we need to collaboratively take steps to ensure that the benefits of IoT outweigh the risks.

3. Key Principles for IoT Security and Privacy

This section presents six key principles for improving IoT security and privacy protections while retaining flexibility for the market to innovate. There is a discussion on the challenges related to the principle, followed by recommended policy actions, and examples of adoption by various authorities.

The principles and recommendations are summarised, as follows:

Principle 1: Promote compliance with security-by-design and privacy-by-design standards.[19]

- Recommendation 1.1: Consider internationally accepted security and privacy best practices to guide the design, deployment and use of IoT devices and services.
- Recommendation 1.2: Promote a certification scheme and trustmark for IoT security and privacy.
- Recommendation 1.3: Require public procurement to only consider IoT devices and services that meet a set of specified security and privacy standards.
- Recommendation 1.4: Offer financial or other incentives to companies whose IoT products or services meet specified security and privacy standards.
- Recommendation 1.5: Participate in global forums and platforms on IoT security and privacy.

Principle 2: Empower consumers with choices, tools and capabilities to take control of their privacy and personal data.

- Recommendation 2.1: Review existing privacy, data protection and consumer protection policies, and ensure that individual users of IoT are adequately protected by law.
- Recommendation 2.2: Encourage data portability (i.e. work to preclude "vendor lock-in.")
- Recommendation 2.3: Promote and support the design of better privacy management and review interfaces for IoT devices and services.
- Recommendation 2.4: Ensure that IoT does not facilitate discrimination and unfair practices.

Principle 3: Protect consumers and small businesses from harm caused by IoT devices and services.

- Recommendation 3.1: Review existing liability frameworks to ensure these define clear responsibilities and consequences for companies across the IoT system and throughout the lifecycle.
- Recommendation 3.2: Ensure that children and other vulnerable consumers are not put at risk by IoT devices.
- Recommendation 3.3: Strengthen legal protections for security and privacy researchers.
- Recommendation 3.4: Have a mechanism in place for IoT product and service suppliers to notify authorities and affected individuals when there is a security or personal data breach.

[19] These terms can be applied to different frameworks, but useful references for this purpose are:
- Security by Design - https://www.owasp.org/index.php/Security_by_Design_Principles
- Privacy by Design - https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

Principle 4: Strengthen the capacity of relevant entities to respond to and mitigate IoT-based threats.

- Recommendation 4.1: Assess the needs of IoT stakeholders, and tailor capacity development plans to enhance their knowledge and skills to respond to and mitigate IoT security and privacy threats.

Principle 5: Support and engage in consumer awareness and education campaigns.

- Recommendation 5.1: Collaboratively develop awareness drives for relevant consumer segments, pooling resources and distribution channels when possible.

Principle 6: Adopt a multistakeholder approach to develop suitable policy interventions for promoting IoT security and privacy.

- Recommendation 6.1: Lead a multistakeholder process to identify policy interventions for promoting IoT security and privacy.
- Recommendation 6.2: Strengthen enforcement of relevant existing laws and regulations covering liability, data protection, and consumer protection before developing new ones focused just on IoT

3.1 Compliance with Standards and Best Practices

Principle 1: Promote compliance with security-by-design and privacy-by-design standards.[20]

Policymakers should encourage IoT manufacturers and service providers to adopt security and privacy standards from the outset, when new products or services are designed and developed, and throughout the full lifecycle of IoT products or services. Strong security and privacy features and protections cannot be effectively implemented as an afterthought.

Challenges:

Economics favour weak security and privacy.

Competitive pressures for shorter times to market and cheaper products drive many manufacturers and providers of IoT systems, including devices, applications and services, to commit less time and resources to security and privacy. Strong security and privacy can be expensive to design and implement, and it can lengthen the time it takes to get a product to market.

The commercial value of user data also means that there is an incentive to collect as much data for as long as possible, which runs counter to good data security practices.

There is no single set of IoT security and privacy standards that is universally recognised and adopted.

Numerous IoT security and/or privacy frameworks, standards, recommendations and guidelines have emerged in recent years, developed by professional bodies, standards development organisations and governments.

[20] Ibid.

One study identified about 30 such initiatives, most of them industry driven.[21] Annex 1 gives a sample of internationally-recognised frameworks for IoT security and privacy.[22] You will see that some focus only on IoT security but not privacy, while others focus on specific IoT segments.

With so many frameworks and standards for IoT security and privacy, manufacturers and suppliers may find compliance across different markets all the more burdensome. Hence the need for collaboration in harmonising frameworks and standards.

Recommendations:

1.1 Consider internationally-accepted security and privacy standards to guide the design, deployment and use of IoT devices and services.

Where there are no local standards in place, existing international standards should be explored to see what works best for local circumstances. They may also serve as incentive for enhancements to existing local standards.

For IoT, it is important to ensure that security and privacy measures are deployed across the IoT system and throughout the lifecycle of the IoT product or service.

Annexes 1 and 2 provides a selection of international and national frameworks, standards, guidelines, and codes of practice for IoT security and privacy.

When creating standards, adopt a principle-based approach, rather than a rigidly specified set of prescribed requirements (such as particular data security or password management methods that may eventually become obsolete). With this approach, standards are more likely to remain future-proof so that these will not need to be significantly changed with new technologies.

[21] Copper Horse, Mapping Security & Privacy in the Internet of Things, https://iotsecuritymapping.uk/

[22] For a list of IoT security and privacy standards and recommendations, see Copper Horse, Mapping Security & Privacy in the Internet of Things, https://iotsecuritymapping.uk/; and Cyber Security Agency of Singapore and Ministry of Economic Affairs and Climate Policy of the Netherlands, The IoT Security Landscape, September 2019, https://www.csa.gov.sg/news/publications/iot-security-landscape

IoT Trust Framework[23]

Consider using the OTA IoT Trust Framework to guide industry assessment.

The Internet Society's Online Trust Alliance developed an IoT Trust Framework in collaboration with over 100 stakeholders from industry, government and consumer advocacy

groups. The Framework is comprised of 40 actionable principles, and calls for collective responsibility to reduce security and privacy risk, strengthen trust and enable IoT innovation.

It stands apart from many other IoT-related frameworks with its comprehensive focus on security, privacy and lifecycle issues, and its holistic view of the IoT ecosystem. Although the Framework is focused on consumer IoT devices and services for the home and enterprise, it is also relevant and can be adopted for other IoT verticals such as agriculture, healthcare, transportation, smart cities, or industrial controls.

The IoT Trust Framework can be used to:

- Guide manufacturer and service provider design, along with business policy choices from initial design through the entire product lifecycle;
- Provide purchasers and distribution channels with the appropriate filters to assess security and privacy; and
- Give policymakers the necessary security principles for informed advocacy and economic policy.

The IoT Alliance Australia (IoTAA) IoT Security Guideline version 1.2[24] for the IoT industry and the forthcoming Security Trust Mark Scheme for the certification and labelling of IoT products and services are both based on the IoT Trust Framework.

In Canada, a multistakeholder process that yielded policy recommendations for enhancing the security of consumer IoT products and services proposed using the IoT Trust Framework to test and assess IoT products and services—this is provided as a case study in Annex 3 of this toolkit.[25] Similar multistakeholder processes have been completed in France[26] and Uruguay.[27]

1.2 Promote a certification scheme and trustmark for IoT security and privacy.

A certification, by which a device manufacturer or an independent body asserts or verifies that a product, service or system has passed a set of quality or performance tests, can be a powerful and visible signal of compliance to internationally recognised best practices.

An associated trustmark that communicates important security and privacy information to users, such as the support period for the product and how data collected by devices is used, would enable users to distinguish between devices that have adequate and inadequate protections at the point of purchase.

[23] Internet Society, OTA IoT Trust Framework, https://www.internetsociety.org/iot/trust-framework/

[24] IoTAA, IoT Security Guideline version 1.2, December 2016, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

[25] Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/

[26] https://www.isoc.fr/services/groupe-iot/

[27] Security in IoT Process in Uruguay, September 2019 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Security%20IoT.pdf

It could also create demand for products and services that bear the trustmark, which would in turn apply market pressure on manufacturers and providers to improve security and privacy.

Certification Scheme and Trustmark for IoT: Voluntary or Mandatory?

Australia, Canada, the EU, UK and USA are in the process of developing a certification scheme and trustmark for IoT. These are currently voluntary, but the UK and USA are considering requiring manufacturers to have their products certified by an independent body or testing agency.

In the UK, the Department of Digital, Culture Media and Sport (DCMS) published in 2018 a voluntary code of practice for manufacturers to release IoT products with secure-by-design features. In 2020, the DCMS set out plans for its top three guidelines to become mandatory in the UK. These will require that:[28]

1. IoT device passwords must be unique and not resettable to any universal factory setting;
2. Manufacturers of IoT devices need to provide a public point of contact as part of a vulnerability disclosure policy; and
3. Manufacturers of IoT devices need to explicitly state the minimum length of time for which the product will receive security updates.

The IoTAA (an industry body) in Australia is planning to roll out a voluntary industry-operated scheme called the Security Trust Mark (STM). This will use market signals to drive vendor and user behaviour, focusing on consumers awareness to spur demand for more secure devices, which in turn will drive vendors to voluntarily meet the requirements for the right to carry the STM.[29]

In November 2019, Finnish Transport and Communications Agency Traficom has launched a Cybersecurity label for smart devices if the devices meet the certification criteria, which are based on EN 303 645. With the label, Traficom aims to raise consumer awareness of information security and the safe use of connected devices.[30]

Some research has shown that voluntary self-certification for Internet-based technologies (especially in the area of privacy) has not been particularly successful, yet mandated testing and certification may increase the cost of producing devices, which could increase prices and reduce IoT adoption.[31]

A certification scheme and trustmark must consider the need to continually monitor and improve the security and privacy of IoT products and services, not just at the point of sale, and to provide ongoing support to protect users throughout the device's (and the data's) lifecycle.

[28] GOV.UK, Secure by Design, 6 June 2019, https://www.gov.uk/government/collections/secure-by-design ; and GOV.UK, Government to strengthen security of internet-connected products, 27 January 2020, https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

[29] IoTAA, IoTAA Submission to Department of Home Affairs consultation on: Securing the Internet of Things for Consumers Draft Code of Practice, 1 March 2020, https://www.iot.org.au/wp/wp-content/uploads/2020/03/IoTAA-Submission-to-IoT-Security-Code-of-Practice-1-Mar-2020-Final.pdf

[30] https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

[31] Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/.

Canada: Exploring Static Labels with QR Code[32]

Canada is exploring the development of a trustmark that combines static labels with a live component such as a Quick Response (QR) code linking to a website that can convey advanced security and privacy information.

The static label could represent the formal testing and certification process performed, while the QR code will allow users to access up-to-date information on the product's security and privacy. As a live component, a QR code could also be used to determine the authenticity of the static label.

A drawback is that users must have access to a smartphone or tablet to scan the QR code, and to an Internet connection to access the website with security and privacy information.

In promoting a certification scheme and trustmark– whether voluntary or mandatory – government agencies and industry groups should work with other organisations focusing on IoT security and privacy to reduce fragmentation in the market for certification initiatives and labels, thus avoiding consumer confusion. A good example of this is the Internet Society-led IoT Security Policy Platform.[33]

A government considering mandatory requirements could take a staged or sector-by-sector approach, making trustmarks mandatory first in areas where personal privacy and safety are most at risk, and allowing voluntary approaches elsewhere.

1.3 Require public procurement to consider only IoT devices and services that meet a set of specified security and privacy standards.

Governments could develop stronger procurement policies that emphasise adherence to accepted security and privacy standards for IoT devices, platforms, and services. These will spur companies to meet the demand, improving the overall IoT market.

Where available, they should also require IoT vendors to obtain certifications or trustmarks as part of procurement policies. Governments should also use industry-accepted tools, such as privacy impact assessments, for testing IoT in their evaluation processes for procurement.

USA: Minimal Cybersecurity Operational Standards for Internet-Connected Devices Purchased by Federal Agencies[34]

A bill introduced in the US Senate in August 2017, and re-introduced in March 2019,[35] proposes "minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies," which includes an obligation for government agencies to procure only IoT devices that comply with specific security requirements. US government agencies would also accept third-party certification of compliance with industry security standards.

[32] Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/

[33] See Footnote 16

[34] Congress.gov, S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?r=1.

[35] Congress.gov, S.734 - Internet of Things Cybersecurity Improvement Act of 2019, https://www.congress.gov/bill/116th-congress/senate-bill/734

1.4 Offer financial or other incentives to companies whose IoT products or services meet specified security and privacy standards.

Incentives and financial support for industries to develop and implement IoT security and privacy can help drive investment and improvements in IoT security and privacy.

Japan: IoT Tax System[36]

From 2018 to 2020, the Japanese government incentivised industry investments in IoT by reducing companies' corporate tax if they can prove their investments in IoT devices increase productivity and cybersecurity.

1.5 Participate in global forums and platforms on IoT security and privacy.

Governments are encouraged to collaborate with industry standards and certifying bodies, the private sector, researchers and others at national, regional and international levels to align frameworks and standards to stimulate global acceptance and adoption.

UK, AU, US, CA and NZ Collaborate with Others in Promoting IoT Security[37]

In October 2019, Ministers from the Five Countries (UK, AU, US, CA and NZ) issued a Statement of Intent Regarding the Security of IoT, agreeing to collaborate with industry and standards bodies to provide better protection to users by advocating for IoT devices to be secure by design, and to engage with industry partners and other nations to encourage international alignment on IoT security.

Governments should consider joining the IoT Security Policy Platform[38] which is working to harmonise IoT security frameworks and promote best practices by using existing guidelines to identify common themes, goals, and opportunities.

In 2019, following an analysis of many existing regional and national frameworks, platform members identified the following shared recommendations:39

- Ensure that security is incorporated in all stages of the design, development, and lifecycle, including risk assessments, security testing and evaluation;
- Ensure that personal and critical data is protected; and
- Make it easy for users to delete personal data.

[36] Eurasia Review, Japan's New Cybersecurity Strategy: Plugging The IoT Gap – Analysis, 19 July 2018, https://www.eurasiareview.com/19072018-japans-new-cybersecurity-strategy-plugging-the-iot-gap-analysis/; and Japan External Trade Organization, Incentive Programs: Connected Industries Tax System (IoT Tax System), https://www.jetro.go.jp/en/invest/incentive_programs.html#b4

[37] Five Country Ministerial Communiqué, Statement of Intent regarding the security of the Internet of Things, 23 October 2019, https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

[38] Internet Society, IoT Security Policy Platform, 14 November 2019, https://www.internetsociety.org/iot/iot-security-policy-platform/

[39] Ibid, linked from page and available in multiple languages.

3.2 Consumer Choice and Control

Principle 2: Empower consumers with choices, tools and capabilities to take control of their privacy and personal data.

Challenges:

IoT devices, by their nature, can make it harder for consumers to be informed and have control over their personal data.

From the data collected by IoT, it is possible to extract information about a person's appearance, behaviour, habits and more.

Traditionally, privacy and data protection policies have focused on informing users about the collection and use of personal data and obtaining consent.

But as IoT devices are often small and resemble the connectionless devices they replace, they may not have screens or other user interfaces to display privacy policies or terms of service (ToSs), obtain consent from users, and give them the ability to manage or opt-out of data collection.

Some devices may be connected to apps on smartphones for this purpose, but typically users would have already opened and installed the device before being able to review privacy policies, ToSs, or give or withhold consent. Other devices may have a privacy policy in their packaging but may not have a means to interact with users to obtain consent and provide choices and controls.

The IoT industry needs to be held accountable for protecting consumers' rights and their data.

The reliance on the concept of "notice and consent" alone to provide information and choice is problematic in the IoT environment as it is for other services that collect and use personal data. Meeting the criteria for informed consent--a legal requirement imposed by many data protection and privacy laws worldwide--becomes more difficult due to the lack of a user interface in IoT devices that consumers are used to have on their personal computers and smart phones. It is important to emphasise other privacy and data protection principles to ensure consumers are adequately protected, such as data minimisation and data security. This might entail focusing on accountability for the appropriate collection, use and protection of users' data.

Since the EU General Data Protection Regulation (GDPR) came into force across the EU in 2018, consumers are becoming more aware of the need for data protection and their right to have control over their personal data. GDPR started a global trend, prompting other jurisdictions to enact or strengthen their own privacy and data protection laws. Some of these apply to the IoT industry or introduce specific provisions on IoT privacy, such as California's Consumer Privacy Act and the US Senate Bill No. 327 on information privacy in connected devices.

The GDPR prescribes seven individual rights for EU citizens or residents: The (1) right to be informed about collection and use of personal data; (2) right to access and obtain a copy of personal data; (3) right to rectification; (4) right to erasure (right to be forgotten); (5) right to restriction of processing of personal data; (6) right to object to the processing of personal data, including objecting to their data being used for direct marketing; and (7) right to data portability.

Data portability entitles users to obtain and reuse their personal data for their own purposes across different services – allowing them to copy or transfer personal data from one service to another securely without affecting its utility. Data portability is a technical and organisational challenge for the IoT industry, requiring cooperation to develop open standards and interoperability in IoT products and services.

However, not all jurisdictions have data protection laws and policies, and for those with data protection laws and policies, not all include the same rights for users to control the collection and use of their personal data, and the ability to transfer or delete data upon discontinuing use, loss or sale of IoT devices or services.

Moreover, not all jurisdictions enforce data protection principles such as purpose limitation, data minimisation and storage limitation – these are foundational principles in the GDPR and other privacy frameworks. IoT will generate massive amounts of data, tempting companies to collect and mine everything they can.

Industry regulation, whether through legislation or voluntary codes of conduct, could reflect users' interests by limiting collection, use and retention of data to the minimum necessary to deliver the service the user expects. Safeguards that limit the amount of data collected and the time it can be kept can reduce the risk of personal data breaches.

Recommendations:

2.1 Review existing privacy, data protection and consumer protection laws and policies to ensure that individual users of IoT are adequately protected by law.

Existing laws and policies should be reviewed and updated as needed to address IoT-related challenges. This would ensure that:

- Individuals are informed about the security, privacy and support policies for their IoT devices or services prior to purchase, activation, download or enrolment, and throughout their lifecycle. This includes making available easy to understand information about what data is collected, how it is used and shared with others, and how long it will be kept, as well as the duration of support/security patching.
- Individuals have control over what data is collected by their IoT devices or services, including the ability to blind and mute devices, as well as how IoT data is analysed and shared with third parties.
- Individuals have control over how identifiable they are when undertaking online and offline activities – there should be options for pseudonymous or anonymous use.[40]
- Individuals are able to transfer or delete their personal data upon discontinuing use, loss or sale of a device or service. IoT manufacturers, developers and service providers should offer the ability to reset a device, and accompanying applications to factory settings, including the ability to delete user data, so that devices can be safely decommissioned at their end of life.
- Personal data collected and stored in sensors, devices and across the IoT ecosystem is protected using security and privacy standards and best practices such as authentication, encryption, purpose limitation,[41] data minimisation[42] and storage limitation.[43]
- Individuals are able to seek redress if their rights are not respected.

[40] Anonymisation is the process of removing personal identifiers that may lead to an individual being identified. Pseudonymisation replaces any identifying characteristics of data with a pseudonym or a value that does not allow the individual to be directly identified without having access to additional information. The latter does not remove all identifying information from the data but merely reduces the linkability of a dataset with the original identity of an individual.

[41] Purpose limitation ensures that data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Companies must understand where, how and why they use personal data, and the GDPR requires that these be documented internally and communicated to the end user.

[42] Data minimisation requires companies to demonstrate that they have processes in place to ensure that they only collect and hold the personal data needed to fulfil the purposes stated. If a company wishes to collect or use personal data for a purpose for which they do not have consent, new consent must be sought from the users, and users should have the ability to withdraw their consent to data collection at any time.

[43] Storage limitation requires companies to justify how long they retain personal data, and delete or de-identify personal data when it is no longer required.

Where a single, overarching privacy/data protection law is not in place, consider developing and passing one. A general privacy/data protection law without reference to a specific sector or technology gives a consistent level of protection and defines a common baseline for all organisations participating in the digital economy.

In the interim, other measures can be adopted to protect the privacy and data of individuals. For example, by integrating privacy and data protection principles in IoT regulations, policies and licensing schemes.

Saudi Arabia: Adoption of Privacy and Data Protection Principles

In Saudi Arabia, there is no general or telecommunications-specific privacy law. However, the country has adopted a specific category of telecommunications licence for IoT virtual network operators (VNOs), which are IoT service providers that do not own network or spectrum resources but provide IoT services to their customers using leased capacities from existing network operators. The IoT-VNO licence requires service providers to maintain their customers' privacy and apply non-discriminatory practices.[44]

Saudi Arabia also adopted in 2018 a cloud computing regulation that applies to all cloud service providers in the country,[45] prohibiting any party other than the customer from accessing the customer's content, and providers from using or processing the content for purposes other than those set in the contract signed with the customer.

2.2 Encourage data portability.

Data portability enables individuals to request and obtain a copy of their data from the organisation holding this information in a structured, commonly-used and machine-readable format, and for the organisation to transmit the data to another organisation or the user.

To encourage data portability, governments need to promote open and interoperable specifications and architectures. IoT manufacturers should be encouraged to publish interfaces to their devices, controllers and servers, and increase the interoperability of data generated by their devices.

This will allow users more control over their data. It will also open up markets for value-added services and increase user choice.

[44] Saudi Arabia Communications and Information Technology Commission, Approval of the "Rules and Conditions for MVNO Services and IoT-VNO Services Provision, 28 October 2018, https://www.citc.gov.sa/en/Decisions/Pages/399-1440.aspx

[45] Saudi Arabia Communications and Information Technology Commission, Cloud Computing Regulatory Framework version 2, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

Several Jurisdictions have Introduced the Right to Data Portability

Several jurisdictions, including Australia, China, the EU, India, Japan, Philippines, New Zealand and the US (State of California) have either implemented or are considering introducing the right to data portability in their domestic laws.

Australia recently passed its Consumer Data Right Act 2019,[46] that gives Australians greater control over their data, allowing customers to transfer their data to trusted recipients for the purposes that they have authorised. The Consumer Data Right is being implemented in the banking, energy and telecommunications sectors, before being rolled out economy-wide on a sector-by-sector basis.

Singapore intends to introduce a data portability requirement.[47] It issued an update to its 2019 discussion paper this year, developed through a collaboration between the Singapore Personal Data Protection Commission and Competition and Consumer Commission of

Singapore. Data portability has an overlap between competition law and data protection law, and both perspectives need to be taken into consideration when implementing a data portability requirement.

2.3 Promote and support the design of better privacy interfaces for IoT devices and services.

IoT devices can and should do more to help users see and control the data their devices generate, but this takes careful design. Controls that are too detailed may offer greater protection, but if they reduce convenience and are hard to use, users are likely to ignore them.

Designers devote great ingenuity to making IoT devices useful and convenient – they should apply the same creativity to the design of privacy controls.

Governments could stimulate research into IoT user interface designs and notification practices and encourage the provision of guidance on how companies can offer different ways of informing users and providing privacy controls.

2.4 Ensure that IoT does not facilitate discrimination and unfair practices.

Governments should explore legislative and regulatory methods to restrict certain kinds of IoT data from being seen or used by specific parties for unauthorised purposes, for example, to prevent insurance companies from using IoT-derived data as a factor in insurance rates, unless explicit, informed consent has been given.

[46] The Treasury of the Australian Government, Consumer Data Right, http://treasury.gov.au/consumer-data-right

[47] Singapore Personal Data Protection Commission and Competition and Consumer Commission of Singapore, Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions, 20 January 2020, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Response-to-Feedback-for-3rd-Public-Consultation-on-Data-Portability-Innovation-200120.pdf?la=en

3.3 Liability and the Protection of Consumers and Small Businesses

Principle 3: Protect consumers and small businesses from harm caused by IoT devices and services.

Challenges:

Regulations may not be sufficiently protecting consumers and businesses from harm caused by defective IoT devices and services.

Harm arising from the use of IoT is generally regulated through existing laws, such as product safety laws and standards, but the extent to which they fully protect individuals and businesses varies across the world. The EU Product Liability Directive (85/374/EEC) and California SB 327 for example, covers products only, and not services.

Most jurisdictions have not yet addressed the issue of liability in the IoT ecosystem.

The complex ecosystem of IoT, with a range of manufacturers, developers and service providers, make it much harder to establish who is liable under existing laws and regulations when something goes wrong.

As IoT-based initiatives such as smart cities, smart grid and intelligent transportation are developed and scaled, there will also be a blurring of roles and responsibilities between the public and private sectors, including in the collection, storage and use of personal data. For these IoT initiatives, it will be a complex challenge to figure out which data protection rules would apply, who owns the data, and who bears the liability for any damage or harm caused to the user of an IoT technology or to third parties (e.g. victims of an IoT DDoS attack).[48]

Unclear legal liability mechanisms may lead to uncertainty among individuals and organisations involved as to who is responsible and what remedies (including compensation) are available when something goes wrong. Further, when liability is known in advance, IoT manufacturers, suppliers and retailers may have stronger incentives to enhance IoT security and privacy.

In IoT systems, different components may be under the control of different organisations in different jurisdictions, which may present challenges in cross-border enforcement.

Recommendations:

3.1 Review liability frameworks to ensure it defines clear responsibilities and consequences for companies across the IoT system and throughout the device's lifecycle.

Policymakers and regulators play an important role in strengthening accountability through well-defined responsibilities and clear consequences for those that are most able to exercise control over the security and privacy of IoT devices and services. Clear liability could be an incentive for stronger security and privacy of IoT devices and services.

Governments should consider the following when reviewing liability frameworks:[49]

- As new risks arise, tort law or other rules governing safety and liability standards should be introduced, replaced, or updated, where necessary.
- Liability rules should cover all types of products and services that comprise the IoT ecosystem.

[48] Internet Society, "Asia-Pacific Bureau Issue Paper: Internet of Things," November 2017.

[49] Consumer International, Securing Consumer Trust in the Internet of Things: Principles and Recommendations, 2017, https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf

- It should be clear which entity is responsible for performance and security at each point of product or service delivery, and during the full lifespan of the IoT product or service.
- Liability time limits should be avoided or at least extended to cover the expected lifespan of the IoT product or service.
- Compensation thresholds should be avoided to enable flexible application of awards.
- Where a service provider shares or outsources data to another entity, it should not dilute the security and privacy obligations of either of them.
- Retailers should share the responsibility and not sell IoT products with critical safety and security defects that are known or they reasonably ought to have known.
- Where complaints or problems involve multiple providers and/or sectors, it should be clear where a consumer should go for assistance.

Canada: Personal Information Protection and Electronic Documents Act

The Canadian Personal Information Protection and Electronic Documents Act has made service providers responsible for protecting personal data under their control, including personal data that they transfer to third parties for processing, for which they must ensure a comparable level of protection through contractual or other means.

Addressing the Liability Challenge in IoT

- The EU has mapped liability issues related to emerging technologies such as IoT,[50] and established an expert working group to further analyse these concerns.[51] It issued a report on the safety and liability implications of IoT and other emerging technologies in February 2020.[52]
- China has started research on liability issues related to artificial intelligence.[53]
- The UK's Automated and Electric Vehicles Act, passed in 2018, deals with the attribution of liability for damages caused by connected cars.[54]
- France aims to modify its liability regime with a view to allowing the roll out of connected cars by 2022.[55]

3.2 Ensure that children and other vulnerable consumers are not put at risk.

Connected toys, virtual in-home assistants, and smart televisions all collect children's personal data. But while parents and guardians should take charge of managing their children's privacy, anticipating, and coping with IoT threats should not fall entirely on users. The primary responsibility for managing IoT security and privacy risks should be transferred to the IoT industry.

[50] European Commission, Staff Working Document: Liability for emerging digital technologies, 25 April 2018, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018SC0137

[51] European Commission, Expert Group on Liability and New Technologies (E03592), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1

[52] COM(2020) 64, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, 19.2.2020, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf

[53] Cullen International, International Comparison of Regulation of Consumer IoT: A study for the Internet Society, August 2018.

[54] legislation.gov.uk, Automated and Electric Vehicles Act 2018, http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted

[55] Cullen International, International Comparison of Regulation of Consumer IoT: A study for the Internet Society, August 2018.

Ensure tighter regulatory scrutiny of child-specific products (like baby monitors, smart toys, and smart watches).

Regulators should prosecute manufacturers, developers or service providers who make misleading or deceptive representations about the security and privacy of their IoT products or services.

Republic of Korea: Network Act and Location Information Act Amended to Protect Children

In the Republic of Korea, the Network Act and Location Information Act was amended in 2018 to account for the processing of personal data and personal location data of individuals under the age of 14.

It requires service providers to use easily understandable formats and language when providing notice of matters related to personal data, and service providers seeking to process the personal (location) data of individuals under the age of 14 must obtain consent from, and verify the consent, of their legal guardians.

3.3 Strengthen legal protections for security and privacy researchers.

Governments should ensure that security and privacy researchers are not put at legal risk for investigating vulnerabilities and responsibly disclosing information on vulnerabilities they have discovered.

They should also allow security and privacy researchers to communicate their knowledge, expertise, and findings with their counterparts in other economies.

3.4 Have a mechanism for notifying authorities and affected individuals when there is a security or personal data breach.

Not all jurisdictions mandate breach notification. However, the "name and shame" effect caused by the need to report and, in some cases, make personal data breaches public, can make IoT providers more vigilant in securing their products and services. Just as important, it means data protection authorities and users know when their personal data has been compromised and action to remedy the effect of the breach can be taken.

Breach Notification Schemes

Many countries or economies have recently amended their privacy and data protection laws, mandating service providers to report security and personal data breaches to data protection authorities and to affected individuals. These include Australia, Canada, China, Japan, Republic of Korea, the EU, the UK and the US.

In case of security incidents or personal data breaches, services providers are subject to timely and adequate notification obligations, liability and compensation rules, and sanctions in case of neglect.

Some economies do not have a mandatory breach notification scheme but have guidelines on handling security and data breaches and breach notifications.

For example, in Hong Kong, breach notification is yet to be a legal requirement,[56] but the Privacy Commissioner for Personal Data has published relevant guidelines[57] to encourage voluntary notification.

3.4 Capacity Building

Principle 4: Strengthen the capacity of actors in the IoT ecosystem to respond to and mitigate IoT-based threats.

Challenges:

Addressing security and privacy risks requires particular expertise

Implementing strong security and privacy measures takes expertise and experience that new players in the IoT ecosystem may not have.

Recommendation:

4.1 Assess the needs of IoT stakeholders and formulate a capacity development plan to enhance their knowledge and skills to respond to and mitigate IoT security and privacy threats.

Resources need to be allocated to awareness-raising and capacity-building on IoT security and privacy across the IoT supply chain.

Policymakers and regulatory authorities, as well as consumer protection bodies, must also have the knowledge and skills to understand and deal with IoT-based threats.

3.5 Awareness and Education

Principle 5: Support and engage in consumer awareness and education campaigns.

Challenges:

Consumers usually do not have the expertise to assess security and privacy features of IoT devices and services, and to protect themselves from IoT-based threats.

Studies have shown that consumers are increasingly concerned about the security and privacy of IoT but generally do not know how to assess the features of IoT devices and services, and to protect themselves from IoT-based threats.[58]

[56] Hong Kong has released a discussion paper reviewing its Personal Data Ordnance, with a proposal to make breach notifications mandatory. Legislative Council Panel on Constitutional Affairs: Review of the Personal Data (Privacy) Ordnance, January 2020, https://www.legco.gov.hk/yr19-20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf

[57] Hong Kong Privacy Commissioner for Personal Data, Guidance on Data Breach Handling and Giving of Breach Notifications, second revision, January 2019, https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

[58] Consumer International and Internet Society, The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things, May 2019, https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/; and Internet Society, Survey on Policy Issues in Asia-Pacific 2018: IoT Security and Privacy, November 2018, https://www.internetsociety.org/resources/doc/2018/the-internet-society-survey-on-policy-issues-in-asia-pacific-2018/

Awareness activities need to be tailored to relevant segments in the IoT consumer market (e.g., youth, elderly, etc.), and studies need to be conducted on 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.

Campaigns must provide sufficient information to allow consumers to make informed choices without overloading them with technical detail. This may be a difficult balance to strike.

Recommendation:

5.1 Collaboratively develop awareness and education campaigns, pooling resources and distribution channels when possible

Regulators, companies, industry bodies, consumer protection bodies and consumer organisations should work together to formulate and roll out consumer awareness campaigns to enhance IoT security and privacy.

Consider collaborating with educational institutions and civil society organisations to integrate IoT security and privacy in digital literacy or school safety programmes. Specifically, enhance awareness on the security and privacy risks of smart toys, wearables and other gadgets and apps that make use of IoT, and how children can protect themselves from these risks.

A well-implemented awareness campaign could motivate consumers to assess the security IoT products and services prior to purchase. It could also stimulate market demand for IoT security and privacy.

Awareness campaigns are also a good mechanism to familiarise consumers with any trustmarks or certification schemes (see Recommendation 1.2) that have been put in place.

This can lead to better security and privacy being viewed by consumers as a market differentiator, which can justify higher pricing for adequately secure products.

Awareness and Education on IoT Security and Privacy

Several governments around the world have launched campaigns on cybersecurity and online privacy for consumers and small businesses, incorporating IoT security and privacy awareness. Examples include Australia's Stay Smart Online,[59] Canada's Get Cyber Safe,[60] and the UK's Cyber Aware Campaign.

Shared Responsibility Framework[61]

The multistakeholder process in Canada to enhance IoT security came up with a Shared Responsibility Framework, which contains behaviours that need to be communicated to consumers, manufacturers, retailers, service providers, governments, civil society, educational institutions and others, and could be used in IoT-related awareness and education campaigns.

[59] Australian Cyber Security Centre, Stay Smart Online: Smart Devices in Your Home, https://www.staysmartonline.gov.au/protect-yourself/protect-your-stuff/smart-devices-internet-enabled-appliances-gadgets-and-toys; and Australian Cyber Security Centre, Stay Smart Online: Smart Devices in Your Office, https://www.staysmartonline.gov.au/protect-your-business/protect-your-assets/smart-devices-internet-enabled-devices-and-gadgets

[60] Government of Canada, Get Cyber Safe: The Internet of Things, https://www.getcybersafe.gc.ca/cnt/rsks/ntrnt-thngs/index-en.aspx

[61] See pages 9 and 10 of the Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/

3.6 Multistakeholder Process

Principle 6: Adopt a multistakeholder and collaborative approach to develop suitable policy interventions for promoting IoT security and privacy.

Challenges:

There's an urgent need for collective action because it is unlikely that market-driven security and privacy improvements will spread widely and quickly enough to offset the rapid growth, particularly of consumer IoT devices, at least in the short term.[62]

No single stakeholder can solve this alone. An inclusive and consensus-based approach can help create long-lasting, efficient, and flexible solutions, and foster collective responsibility among actors in the IoT ecosystem.

IoT security and privacy is complex. A bottom-up multistakeholder process can provide a broader view to sufficiently address existing and potential challenges and issues.

Recommendation:

6.1 Lead a multistakeholder process to identify policy interventions for promoting IoT security and privacy.

Current global discussions about governing, managing, and regulating digital technologies, including IoT, are largely dominated by economically advanced nations and might not support developing economies' contexts and needs. International and regional partners can support and participate, and will be crucial to assisting policy implementation, but countries and economies must craft their own IoT security and privacy strategies.

A multistakeholder process allows participating individuals and organisations from different sectors to look at issues from different perspectives, and to develop consensus-based solutions.[63]

Governments should consider partnering with organisations that have expertise in facilitating multistakeholder processes and in IoT security and privacy. Engaging an independent institution can also bring balance and credibility to the policymaking process.

The Internet Society has identified four key attributes of a multistakeholder process:[64]

1. **Stakeholder-driven** – Stakeholders determine the process, scope, and direction.
2. **Open** – Any stakeholder may participate, and the process includes and integrates the viewpoints of a diverse range of stakeholders.
3. **Transparent** – All stakeholders and the public have access to deliberations, creating an environment of trust and accountability.
4. **Consensus-based** – Outcomes are consensus based, delivering positive value to the greatest number of stakeholders.

[62] Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[63] Internet Society, Internet Governance – Why the Multistakeholder Approach Works, April 26, 2016, https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

[64] Larry Strickling, A Call to Action: Get Involved with Multistakeholder Internet Policy Efforts, Internet Society, July 3, 2018, https://www.internetsociety.org/news/speeches/2018/a-call-to-action-get-involved-with-multistakeholder-internet-policy-efforts/

4. Priority Actions

With countries and economies at different stages of development with respect to IoT, as well as to cybersecurity and privacy protections, priority actions have been divided into three categories:

- **Early stage development** – Economies that have started to take an interest in IoT security and privacy but have yet to have cybersecurity and data protection regulations in place.
- **Intermediate stage development** – Economies that have cybersecurity and data protection regulations in place, but these do not specifically address IoT. Enforcement mechanisms may also be in place but may not be fully functioning.
- **Advanced stage development** – Economies that have cybersecurity and data protection regulations in place that specifically address IoT challenges, with strong enforcement bodies.

4.1 Early Stage Development

Characteristics:

Economies have started to take an interest in IoT security and privacy. Some groups have developed IoT or cybersecurity strategies that mention the need to address IoT security and privacy risks but there are no national-level policies or guidelines on IoT security and privacy, and no cybersecurity and general data protection laws enacted yet.

Priority Actions:

- Develop an overall IoT strategy that includes security and privacy considerations.
- Conduct a mapping of laws and policies that need to be updated or created in light of the security and privacy risks of IoT and of the overall strategy. This mapping study can be used to catalyse legislative and policy changes.
- If a cybersecurity policy or law is being drafted, ensure that it covers IoT security risks. Does it consider security measures across the IoT system (including the devices manufactured, the data generated and distributed, and the services that use them) and throughout the entire lifecycle of IoT devices and services?
- If a privacy or data protection law is being drafted, ensure that it covers IoT privacy risks. Does it include the rights of users to control the collection and use of their personal data, including the ability to transfer or delete data upon discontinuing use, loss or sale of IoT devices or services? Does it enforce data protection principles such as purpose limitation, data minimisation and storage limitation?
- Raise consumer awareness about IoT security and privacy risks to stimulate market demand for IoT security and privacy. Collaborate with industry bodies, consumer organisations and schools.
- Organise a multistakeholder process to identify IoT security and privacy policy recommendations. Since IoT is very broad and complex, economies may want to focus at this stage on consumer IoT security and privacy and develop working groups to undertake research on specific aspects of consumer IoT security and privacy (see Case Study on the Canadian multistakeholder process).

4.2 Intermediate Stage Development

Characteristics:

Economies have a national strategy for IoT. Economies also have some cybersecurity and data protection measures in place, but these do not specifically address IoT. Existing enforcement authorities may require strengthening. The IoT industry is seeking guidance on IoT security and privacy.

Priority Action:

- Review existing cybersecurity, privacy, data protection and consumer protection laws and policies against international cybersecurity and privacy frameworks and standards, such as the OTA IoT Trust Framework (see also Recommendation 2.1 in Section 3.2). The results can be used to advocate for legislative and policy changes.
- Develop guidelines or codes of practice for IoT security and privacy based on internationally accepted standards and best practices.
- Engage in discussions with the IoT industry to explore the development of a certification scheme and trustmark for IoT security and privacy. Approach and collaborate with other countries and economies developing a certification scheme and trustmark for IoT to reduce the amount of fragmentation in the market for certification initiatives and labels (see Recommendation 1.2 in Section 3.1).
- Organise a multistakeholder process to develop strategies for formulating and implementing IoT security and privacy policies and regulations (see Section 3.6).
- Incorporate a set of security and privacy standards for IoT devices and systems in public procurement policies.
- Offer financial or other incentives to companies whose IoT products or services meet a set of specified security and privacy standards.
- Raise awareness among government officials and industry on the impact of IoT security and privacy threats on key development sectors.
- Join the IoT Security Policy Platform, a collaborative body of government agencies and global organisations working together to harmonise national- and global-level IoT security frameworks and promote best practices to address key challenges to the IoT ecosystem.

4.3 Advanced Stage Development

Characteristics:

Economies have cybersecurity and data protection policies and regulations in place that specifically address IoT challenges and have strong enforcement bodies. They participate in global forums and platforms in setting IoT security and privacy frameworks and standards. The IoT industry and IoT users have some awareness about IoT security and privacy, and some capacity to respond to and mitigate IoT-based threats.

Priority Actions:

- Engage a mulitstakeholder group to periodically review cybersecurity and data protection regulations, policies and guidelines to ensure that they include safeguards against new vulnerabilities and risks, and are aligned with international cybersecurity and data protection frameworks and best practices.
- Review the liability framework to ensure it defines clear responsibilities and consequences for companies across the IoT system and throughout the lifecycle (see Recommendation 3.1 in Section 3.3).
- Strengthen legal protections for security and privacy researchers.

- Investigate and prosecute manufacturers, developers or service providers who make misleading or deceptive representations about the security and privacy of their IoT products or services.
- Assess the capacity needs of IoT stakeholders and formulate a capacity development plan to enhance their knowledge and skills to respond to and mitigate IoT security and privacy threats.
- Incorporate awareness on IoT security and privacy in digital literacy programmes and/or cybersecurity awareness campaigns.
- Support emerging economies in improving IoT security and privacy and encourage international alignment on IoT security and privacy.

Annex 1: A sample of internationally-recognised frameworks, standards, recommendations and guidelines for IoT security and privacy

Organisation	Framework/Standard/Recommendation/Guideline
Internet Society's OTA	IoT Security & Privacy Trust Framework version 2.5 (October 2017)
Cloud Security Alliance	IoT Security Controls Framework (May 2019)
Consumer International	Consumer IoT: Trust By Design – Guidelines and Checklists (2019)
Consumer International and others	Securing Consumer Trust in the Internet of Things: Principles and Recommendations (2017)
ETSI Technical Specification	ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements (June 2020)
GSMA	GSMA IoT Security Guidelines and Assessment (March 2019)
IEEE	P1912 - Standard for Privacy and Security Framework for Consumer Wireless Devices (under development) IEEE 2413-2019: Standard for an Architectural Framework for IoT (May 2019) IoT Security Best Practices (February 2017)
Industrial Internet Consortium	The Industrial Internet of Things: Managing and Assessing Trustworthiness for IIoT in Practice (July 2019) Industrial IoT – Volume G4: Security Framework (September 2016) and other resources
Internet Engineering Task Force (IETF)	Manufacturer Usage Descriptions (MUD - RFC 8520 – March 2019) standard provides a means for end devices to signal to the network what sort of access and network functionality they require to properly function, thus, reducing the threat surface. See also IoT Security: State of the Art and Challenges (RFC 8576 - April 2019)
International Standards Organisation (ISO)	ISO/PC 317: Consumer protection – Privacy by design for consumer goods and services (forthcoming)
IoT Security Foundation	IoT Security Compliance Framework (May 2020) and other resources
IoT Security Initiative	Cybersecurity Principles of IoT version 1.1 and other resources

IoT Security Policy Platform	Members' Joint Statement (November 2019)
IoXt Alliance	IoXt Security Pledge
Mozilla and others	Minimum Security Standards for Tackling IoT Security (November 2018)
World Wide Web Consortium	Web of Things (WoT) Security and Privacy Guidelines W3C Editor's Draft (April 2020)

Annex 2: A summary of selected national legislations, frameworks, plans, guidelines, certification schemes and trustmarks for IoT security and privacy

Economy/Region	Legislation/Framework/Plan/Guideline/Certification/Trustmark
Australia	**IoT security and privacy:** IoT Alliance Australia (IoTAA) Strategic Plan to Strengthen IoT Security in Australia version 4 (September 2017), IoT Security Guideline version 1.265 (November 2017), Department of Home Affairs' Draft Code of Practice: Securing IoT for Consumers (June 2020)[66] **Certification:** IoTAA Security Trust Mark (forthcoming) **Privacy and data protection:** Australian Privacy Principles, Notifiable Data Breaches Scheme 2018 and Consumer Data Right[67] that the IoT industry must comply with.
Canada	**IoT security**: Canadian Centre for Cyber Security's Internet of Things Security for Small and Medium Organizations (ITSAP.00.012); Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report (May 2019) **Certification:** One of the proposals put forward by the report above is creating security certification label for devices. **Data protection:** IoT industry must comply with the Personal Information Protection and Electronic Documents Act (PIPEDA)
European Union	**IoT security:** European Union Agency for Network and Information Security (ENISA) Baseline Security Recommendations for IoT (November 2017); Online Tool for IoT and

[65] The IOTAA IoT Security Guidelines is comprehensive in that it takes into account system-wide security (that includes the security of devices, applications, cloud services and networks) and user privacy aspects, as well as lifecycle support. The guide has incorporated the OTA IoT Trust Framework. It covers not only consumer IoT, but also IoT for business use and critical infrastructure use.

[66] This draft code aligns with and builds upon the guidance provided by the UK Code of Practice for Consumer IoT.

[67] Consumer Data Right gives Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorised. The Right will be implemented initially in the banking, energy, and telecommunications sectors, and then rolled out economy-wide on a sector-by-sector basis. For more information see: http://treasury.gov.au/consumer-data-right

	Smart Infrastructures Security (January 2019); and Good Practices for Security of IoT - Secure Software Development Lifecycle **Certification:** EU Cybersecurity Act 2018 establishes an EU Framework for Cybersecurity Certification for online services and consumer devices. Certification is voluntary. **Data protection:** IoT industry must comply with the General Data Protection Regulation (GDPR)
Hong Kong	**IoT security**: Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) IoT Security Best Practice Guidelines (January 2020)
Japan	**IoT security:** National Center of Incident Readiness and Strategy for Cybersecurity (NISC) General Framework for Secure IoT Systems (August 2016). In 2018, the framework was incorporated in the nation's Cybersecurity Strategy Ministry of Economy, Trade and Industry (METI) Cyber/Physical Security Framework (April 2019), Guidelines for Cyber-Physical Security Measures for Building Systems (June 2019), and Draft IoT Security Safety Framework (March 2020) Japan Computer Emergency Response Team Coordination Center (JPCERTCC) IoT Security Checklist (June 2019) **Incentive for IoT security:** The IoT Tax System (abolished March 2020) reduced corporate tax if companies can prove their investments in IoT devices increase productivity and cybersecurity **Data protection:** IoT industry must comply with the amended Act on Protection of Personal Information 2020
Republic of Korea	**IoT security:** Korea Internet and Security Agency (KISA) IoT Common Security Principles and IoT Security Certification Service; Guidelines on Automatic Processing, IoT and Privacy by Design (February 2020) **Data protection:** IoT industry must comply with the Personal Information Protection Act 2011 (amended February 2020)
Malaysia	**IoT security:** Malaysian Technical Standards Forum Berhad (MTSFB) Technical Code on IoT Security Management (October 2018) **Data protection:** IoT industry must comply with the Personal Data Protection Act 2010
Singapore	**IoT security:** Infocom Media Development Authority (IMDA) IoT Cyber Security Guide (March 2020) **Data protection:** IoT industry must comply with the Personal Data Protection Act 2012, which is currently being reviewed in light of emerging technologies, including IoT. Voluntary Data Protection Trustmark certification scheme (although not specifically addressing IoT)

Thailand	The National Broadcasting and Telecommunications Commission (NBTC) has established a committee to draft a regulatory framework for IoT, including IoT security and privacy
United Kingdom	**Consumer IoT security and privacy:** Department of Digital, Culture Media and Sport (DCMS) Code of Practice for Consumer IoT (June 2019); proposed regulations on consumer IoT security (February 2020); and proposal for regulating consumer smart product cybersecurity (July 2020) **Data protection:** IoT industry must comply with the Data Protection Act 2018
United States of America	**IoT security legislation:** In September 2018, California enacted legislation, to come into effect in2020, that requires manufacturers to equip connected devices with reasonable security features, appropriate to the nature and function of the device The IoT Cybersecurity Improvement Act of 2019 introduced into the US Senate in March 2019, if passed, would require IoT-related devices procured by the US government to meet certain minimum security criteria--although this Act does not extend to consumer equipment **Privacy:** The California Consumer Privacy Act (June 2018)[68] **Certification:** The Cyber Shield Act of 2019 re-introduced into the US Senate in October 2019, proposes a voluntary certification process for IoT devices **Guidelines:** National Institute of Standards and Technology (NIST) Foundational Cybersecurity Activities for IoT Device Manufacturers (May 2020) and Considerations for Managing IoT Cybersecurity and Privacy Risks (June 2019)

Annex III: Canadian Multistakeholder Process Case Study

Case Study: Canadian Multistakeholder Process: Enhancing IoT Security[69]

Introduction

From 2018 to early 2019, Canada embarked on a multistakeholder process to develop recommendations to enhance the security of consumer IoT products and services in the country.

This initiative is a partnership between the Internet Society, the Ministry of Innovation Science and Economic Development (ISED), the Canadian Internet Registration Authority (CIRA), the Canadian Internet

[68] The California Consumer Privacy Act gives California residents the following rights: (1) the right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold; (2) the right to opt out of allowing a business to sell their personal information to third parties; (3) the right to have a business delete their personal information, with some exceptions; and (4) the right to receive equal service and pricing from a business.

[69] For more information see: Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/

Policy and Public Interest Clinic (CIPPIC) and Canada's National Research and Education Network (CANARIE).

Objectives

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

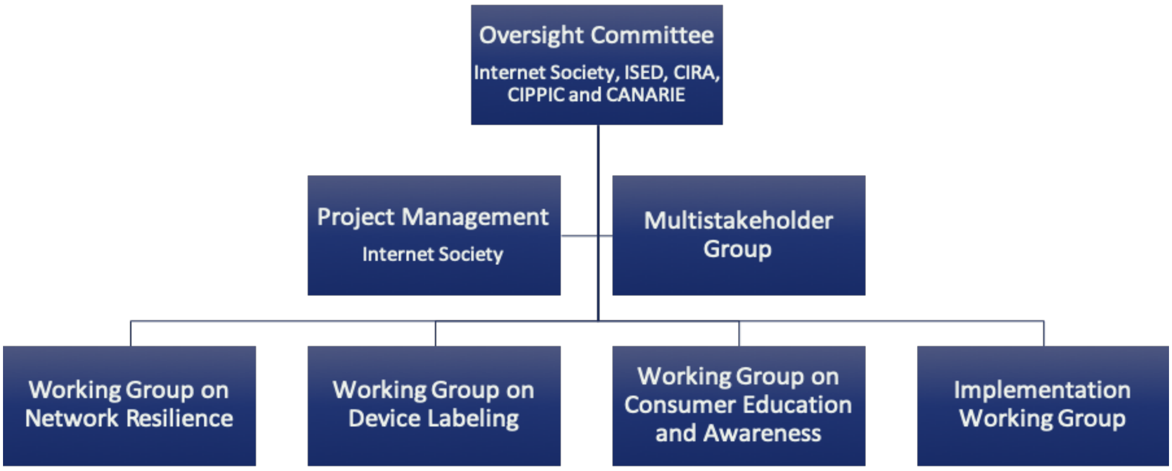
Governance

An Oversight Committee (OC) was created to set the overall goals of the process, review working group output, oversee report development, and approve external communications. It included representatives from the Internet Society, ISED, CIRA, CIPPIC and CANARIE. Decision-making within the OC was based on consensus and norms established at the beginning of the process.

The Internet Society took the responsibility of managing the initiative, and reporting to the OC.

The OC convened a multistakeholder group, drawn from government, civil society, academia, technical and security community, industry, and other relevant sectors to participate and contribute to the process.

The multistakeholder group agreed to establish three working groups (WGs) on Network Resilience, Device Labeling (trustmark), and Consumer Education and Awareness, and identified members to undertake research on these thematic areas and develop specific recommendations.


Oversight Committee
Internet Society, ISED, CIRA, CIPPIC and CANARIE
Project Management
Internet Society
Multistakeholder Group
Working Group on Network Resilience
Working Group on Device Labeling
Working Group on Consumer Education and Awareness
Implementation Working Group

An Implementation Working Group was subsequently created to ensure that recommendations from the Outcomes Report contribute to the policymaking process. It also took charge of coordinating next steps, including Canada's participation in international IoT security initiatives. Made up of OC members, working group leads and individuals from the multistakeholder group, it now meets monthly to discuss progress made and opportunities for engagement.

The multistakeholder group also selected areas for research, reviewed documents, and provided guidance on the development of policy recommendations.

Methodology

The multistakeholder group organised six half-day and full-day in-person meetings. These were moderated, open, public and live streamed for remote participation. Meeting recordings, and outcome reports outlining next steps were made available online.

A series of virtual meetings and webinars was organised in between multistakeholder meetings. There were also in-person and virtual meetings for working groups, as well as focus group discussions.

All announcements, meeting reports and research materials were posted on a dedicated website https://iotsecurity2018.ca/.

The first multistakeholder meeting developed ground rules for participation, discussion and consensus-building. Participants also set year-long goals and agreed on a definition of IoT for the purpose of the initiative.

The second meeting established the three WGs, and settled on their scope, stakeholders and communication modality.

The following three meetings focused on WGs' findings and updates on their progress, along with discussions to identify policy recommendations, and steps for implementation along the three thematic areas.

The sixth and final meeting finalised the WGs' recommendations towards the development of an Outcomes Report.

Efforts were made to include individuals from different regions, languages and backgrounds in these conversations. Meetings were held in both English and French, and included specific target sectors, such as youth and indigenous groups.

Experts from other economies were invited to contribute. For example, the Device Labelling Working Group collaborated with the UK's Department for Digital, Culture, Media and Sport for inputs on possible labelling schemes.

A draft Outcomes Report was released for one month for public comment, with eight organisations representing five stakeholder groups responding.

Lessons Learned and Good Practices

Piggyback on relevant events and forums to engage a wider and more diverse group of stakeholders – The multistakeholder process in Canada took advantage of key events like the Canadian Internet Governance Forum (IGF) 2019 and the Indigenous Connectivity Summit to engage with a wider and more diverse group of stakeholders. Youth's perspectives were solicited through Youth IGF in Canada by means of an online survey.

Engage a facilitator who is knowledgeable in IoT, familiar with the national context and has experience in the multistakeholder process – This is a critical component that has contributed to the success of Canadian initiative.

Track stakeholder engagement – Set up a system to keep track of who is participating in what to identify which stakeholders need to be encouraged to participate, and pull in stakeholders from poorly-represented stakeholder groups.

Maintain momentum and continue engagement with stakeholders in between in-person meetings – There were a series of virtual meetings, webinars and smaller workshops with special interest groups organised to maintain interest and stimulate participation. This was supplemented by online discussions on communication platforms like Slack and listservs.

Bring in examples of practice from other economies and organisations – The Canadian experience found that many solutions to challenges have already been identified by other economies and organisations. Ways to bring in these external examples include developing and presenting case studies, interviewing external experts or inviting them to participate in multistakeholder meetings.

A multistakeholder process takes time – Dialogue and consensus-building can move slowly--it is important to plan for extra time and possible additional costs.

Please send comments and feedback to:

Internet Society - Asia-Pacific Bureau
3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190
Tel: +65 6549 7138
Fax: +65 6549 7001

E-mail – apac@isoc.org
Website – https://www.internetsociety.org/apac
Facebook – /isocasiapacific/
Twitter – @ISOCapac
LinkedIn – https://www.linkedin.com/company/internet-society-apac/

Subscribe to newsletter – http://bit.ly/ISOC-APAC-signup