

**Securing the Internet of Things:**

**A Multistakeholder Approach for Canada**

**December 2017**



**Introduction**

This paper is meant to contextualize Canada’s multistakeholder process for the development of a broad-reaching policy to govern the security of the Internet of Things (IoT). It includes:

1. Policy Development Processes around the World
2. The Roles and Responsibilities of Each Stakeholder
3. Levels of the IoT Security Puzzle
4. Lessons Learned: Governance of Other Technologies
5. Challenges to Crafting Consumer Device Standards in an IoT Environment

**I. Policy Development Processes around the World**

Countries were selected based on their relative involvement in IoT, whether in its development or manufacturing.

China

China assigns a high level of importance to IoT, and seeks to maintain control and a top-down approach to policy development. The government leads standards development and seeks international acceptance for Chinese-developed standards.[[1]](#endnote-1)

The three most important government agencies in China with respect to ICT policy are the National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Science and Technology (MOST).[[2]](#endnote-2) MIIT is responsible for the policy and operational action in the ICT industry. China’s goals, ideas, and areas of focus for IoT development are outlined in the State Council’s Guidance on Advancing Orderly and Healthy IoT Development.[[3]](#endnote-3)

Although the government is not inclusive in developing IoT policy, there is an emerging trend within the government to consult non-state-owned companies.[[4]](#endnote-4) Input and buy-in from players like Alibaba and Tencent help the government develop ICT policies with legs. China’s 150,000 state-owned companies also have some lobbying power to influence policy development.[[5]](#endnote-5)

China has expressed interest in working with international partners. In January 2016, the EU-China IoT Advisory Group published a white paper that has a cooperation proposal, including items like “…improve the EU-China cooperation policy and mechanism in scientific research and innovation from a strategic and operational perspective, for elaborating policy recommendations.” [[6]](#endnote-6) As China’s economy becomes more reliant on international partners, the government with likely seek more policy alignment with countries on IoT.

Estonia

Estonia’s e-government approach both reflects and drives its multistakeholder approach to technology policy issues.

The Ministry of Economic Affairs and Communications’ Digital Agenda 2020 seeks to strengthen the multistakeholder nature of its policy development. In fact, the Digital Agenda 2020 itself was a product of a multistakeholder process from 2012-2013. The agenda specifies a series of targets, among them that “Services are developed and policies are formulated in co-operation between the public sector and the citizens.”[[7]](#endnote-7) Estonia seeks to increase participation of civil society and NGOs by increasing accessibility of public sector websites, enhancing feedback from public consultations, and developing platforms for participation.

Estonia seeks to share its ICT experience internationally and learn from other countries through the Open Government Partnership, especially in areas of e-governance.[[8]](#endnote-8) In terms of policy cooperation, Estonia has shown willingness to work with others, particularly within the EU policy space. For example, its active role in cyber security policy led to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence in Estonia. [[9]](#endnote-9)

Germany

The German model to IoT policy development operates in the contexts of Germany’s Digital Agenda, a strategic policy program adopted in August 2014 also referred to as Industrie 4.0. The Federal Ministry of the Interior and the Federal Ministry for Economic Affairs are both in charge of implementing the agenda.[[10]](#endnote-10) Germany’s [principles](https://www.digitale-agenda.de/Webs/DA/DE/Grundsaetze/Grundsaetze_Digitalpolitik/grundsaetze-digitalpolitik_node.html;jsessionid=A1F42A606E7666443415578B666DF467.s4t2) for its digital policy states that the Digital Agenda will help pool the forces of all stakeholders. There does not seem to be clear mechanisms to include stakeholders; however, the government has a reputation of being responsive to public debates. However, the mechanism to include all stakeholders is unclear.[[11]](#endnote-11)

Stakeholder engagement around IoT policy seems to be a patchwork of initiatives related to Industrie 4.0, which addresses intelligent manufacturing, and, by extension, IoT. The goal is to use IoT to connect CMEs more efficiently to global production and innovation networks.[[12]](#endnote-12)

In the past, Germany did not have a patchwork method to IoT policy development. From May 2010 until April 2013, the Enquete Commission on Internet and Digital Society (EIDG), a special parliamentary inquiry body of the German Bundestag, brought together 17 democratically elected members (members of parliament) and 17 experts and practitioners representing industry, trade unions, civil society and academia to address the digitization policy challenges.[[13]](#endnote-13) Furthermore, the public was invited to participate in the EIDG’s consultations “to a special degree,” which included efforts at transparency and an online engagement platform. The EIDG took the form of discussion forums and working groups, which produced several hundred recommendations in its final report, at which point the EIDG disbanded.[[14]](#endnote-14)

Germany seeks to develop policies in conjunction with international partners, especially at the European level. Its G20 presidency has pushed for norms and standards for four central topics: Industry 4.0, IT security, smart cities and smart mobility.[[15]](#endnote-15)

India

In 2015, India’s Department of Electronics and Information Technology (DeitY) rolled out its first policy framework on IoT. The framework has since been slightly revised, and continues to invite further comment.[[16]](#endnote-16) The framework supports the participation and collaboration of stakeholders “at an appropriate stage”.

To integrate stakeholders into the policymaking process, the policy framework proposes creating several bodies. One would be a national expert committee for developing and adopting IoT standards in the country comprised of industry experts and organizations. Another would be a High Level Advisory Committee composed of from government, industry, academia, technology organizations, network organizations, and domain ministry members to provide ongoing guidance on IoT. It is unclear if and when these bodies will be created.

India seeks to learn from other countries and participate in global forums like IEEE. [[17]](#endnote-17) In addition, India seeks global and national participation from stakeholders to promote standards related to IoT interoperability, privacy, and security, among other topics.

Japan

Japan values a multistakeholder approach to policy development.

ICT bills are either proposed by a member of the Diet or by the Ministry of Internal Affairs and Communications. Stakeholders can influence policy from the bottom up, as junior and senior policy officers are most heavily involved in the drafting of a bill; political appointees become involved at a later stage. [[18]](#endnote-18)

Ministries, the business community, and business associations exert the most power on the policymaking process. The private sector benefits from the belief that collaboration and consultation results in more easily implementable and accepted regulations in the longer term.[[19]](#endnote-19)

That being said, there is a place for civil society in ICT policy development. Japan’s opening statement at WSIS 2017 made clear that Japan values transparent policy and regulatory frameworks through open multistakeholder processes.[[20]](#endnote-20) In fact, Japan expresses its desire to “strengthen collaboration among all stakeholders, at national, regional and international levels”.[[21]](#endnote-21) When Japan makes decisions regarding issues like IoT, it establishes a multistakeholder dialogue platform that includes the private sector, academia, civil society, and government. For example, Japan is currently developing AI guidelines – unbinding soft law - with this approach.[[22]](#endnote-22)

Japan seeks to align its domestic rules with international norms in order to facilitate trade and market access. Japan seeks to increase cooperation with its international partners, particularly with the EU and U.S.

Singapore

Overall, Singapore’s approach to IoT policy development appears to take a multistakeholder approach, with the Infocomm Media Development Authority (IMDA) acting as the deciding authority. The IMDA works with multiple stakeholders in what appears to be a multilateral fashion. IMDA continually engages and consults industry and consumers when formulating new policies or reviewing existing ones.[[23]](#endnote-23)

Within the IMDA, [The Telecommunications Standards Advisory Committee](https://www.imda.gov.sg/regulations-licensing-and-consultations/ict-standards-and-quality-of-service/industry-committees-and-working-groups/the-telecommunications-standards-advisory-committee) (TASC) provides recommendations for the setting of telecommunications standards. The TSAC initiates new work items and forms Working Groups ("TSAC WGs"). Draft standards must be endorsed by TSAC in order to be send to the IMDA for approval.[[24]](#endnote-24)

South Korea

In South Korea, the government views ICT policymaking as something to be approached with a light touch, except in cases market failure or societal need.[[25]](#endnote-25)

One of the government’s guiding aims is to work with local governments, private-sector agencies, experts, businesses, and academia. Civil society is notably absent. In addition, the aspiration to work with these different stakeholders has only been expressed in relation to the development of “the intelligent information society”.

Although the push to engage other stakeholders seems confined within this initiative, the establishment of the Strategic Committee for ICT, a policy review committee that consists of 12 ex-officio members and 13 non-official members, shows promise. [[26]](#endnote-26) South Korea intends to expand the non-official committee to include members of local governments, civil society activists, and representatives of businesses and transform the organization into the “Intelligent Information Society Strategy Committee”. The political structure in South Korea is generally amenable to government cooperation with civil society, especially bodies like Federation of Korean Industries (FKI), so this development makes sense.

South Korea has not had notable high-profile international policy cooperation, but the prospect is likely in the future. The country’s ICT sector is critical for the economy; harmonizing IoT policy would remove market entry barriers.

United States

In the United States, the Department of Commerce, alongside the Department of Homeland Security, have taken leading roles in developing IoT security policy. Overall, the U.S. government supports a multistakeholder approach in which industry takes the lead to establish best practices. The U.S. governments sees its role as creating an enabling environment.

The National Telecommunications and Information Association (NTIA) is a body within the Department of Commerce that has convened multistakeholder processes on IoT security policy. NTIA’s current multistakeholder process is focused on IoT security upgradability and patching.[[27]](#endnote-27)

U.S. Department organizations like the NTIA work with executive branch agencies to develop administration positions; however, Congress can also play a role through legislation. For example, the “Securing IoT Act of 2017” was introduced in the House of Representatives this year.[[28]](#endnote-28) In addition, various departments shape IoT policy within their sectors or interest; for example, the Department of Transportation is interested in transport infrastructure IoT security.[[29]](#endnote-29)

Another governmental body, the Federal Communications Commission (FCC), can craft IoT policy through its mandate to regulate interstate and international communications by radio, television, wire, satellite and cable. Most FCC regulations are adopted by a process known as "notice and comment" rulemaking, a process that allows all stakeholders – to have a voice in the rulemaking process by submitting comment.[[30]](#endnote-30) However, the process is more of a one-way communication channel; ultimately, the FCC develops the final rules. The Federal Trade Commission (FTC) also occasionally shapes IoT security policy due to its mandate to promote competition and protect consumers.

NTIA represents the executive branch in international telecommunications and information policy activities.[[31]](#endnote-31) Overall, the U.S. prefers that IoT policy be developed on a national basis with a multistakeholder approach.

**II. The Roles and Responsibilities of Each Stakeholder**

All stakeholders have a role to play in securing IoT and a responsibility to work together towards a more comprehensive and resilient security environment. The following is adapted from [*Securing the Internet of Things: A Collaborative and Shared Responsibility*](https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf)*,[[32]](#footnote-1)* a publication from the Online Trust Alliance, an initiative within the Internet Society (ISOC). It details the roles and responsibilities of each stakeholder in the security of IoT.

1. **Retailers, Resellers & E-commerce Sites** – Retailers have a responsibility not to knowingly sell IoT products with known critical safety and security defects. They also are responsible to convey, to the best of their knowledge, the security of the products they sell as clearly as possible to their customers. Responsible retailers can be key drivers of change by establishing minimum security and privacy standards for the products they sell, not unlike retailers pledging to not source products made by child labor or those from unsustainable forests. Retailers, particularly those with significant market power, have an opportunity and the responsibility to drive better security practices within the IoT market.

2. **Developers, Manufacturers & Service Providers** – IoT developers, manufacturers, and service providers are responsible for incorporating IoT security from the start of the design process through to end of life for a product. In practice, this means IoT developers, manufacturers and service providers must build secure and privacy respecting products; support them with timely, verifiable, and effective patches and updates to address known vulnerabilities; and continue to do so until a clearly stated end date for supporting the product. Security support commitments, including security and privacy policies, alongside product and service lifecycles (e.g. how long will support and updates be available, and what happens after they cease[[33]](#footnote-2)), must be disclosed to users prior to purchase. Security and privacy notices should be easily discoverable and included on product packaging and point of sale materials to easily inform the consumer prior to purchase. IoT Developers, manufacturers and service providers are responsible for articulating their security and privacy commitments in easy to understand terms, enabling the consumer make more informed purchase decisions.

3. **Brokers, Builders, Car Dealers & Realtors** – A smart home or connected vehicle are attractive selling points for every buyer or renter. Brokers, builders, car dealers & realtors are responsible for disclosing, to the best of their knowledge, all IoT products included in the sale of the connected vehicle or smart home. They must disable access to previous renters or owners, and enable new owners to re-set the IoT products. At “closing,” a car rental or sale the dealer, or former user, should ensure that physical and digital keys are turned in, and all personal data is erased.

4. **Network operators** – Recent, high-profile attacks performed by botnets made up of thousands of vulnerable IoT devices have highlighted the impact that IoT security can have on other stakeholders and Internet infrastructure.[[34]](#endnote-32) Networks operators play a critical role in mitigating the impact that insecure IoT devices and services have on the wider Internet ecosystem. Network operators are responsible for strengthening routing security by preventing the propagation of incorrect routing information, preventing traffic with spoofed IP addresses, and facilitating cooperation and communication among network operators.[[35]](#endnote-33) By preventing incorrect routing information and preventing traffic with spoofed IP addresses, network operators can limit the use of vulnerable IoT devices in reflective distributed denial service (DDoS) attacks. Similarly, strengthening communication between network operators will better allow for coordinated responses to IoT-based attacks. Network operators can also flag strange traffic flowing from a user’s home, alerting the user to a vulnerable IoT device that may need to be addressed.

5. **Vulnerability Researchers** - Security professionals must work collaboratively to test product security and disclose any vulnerabilities in a responsible manner.[[36]](#endnote-34) Security researchers play an important role in testing the security of devices, and alerting manufacturers and service providers to discovered vulnerabilities.

5. **Consumer Groups** – Consumer groups have a role to play in the development, implementation, and evaluation of IoT security. Through product reviews, consumer groups can aid consumers in factoring security into their buying habits.

6. **Platforms** - IoT platforms, cohesive systems that can be controlled from a single app, (e.g. Homekit, Weave, etc.) hold significant market power. The choices of platform vendors greatly impact the level of security and privacy within the IoT market.[[37]](#endnote-35) By further strengthening their certification programs and including the overall security of certified devices in their assessment, platform vendors can pressure IoT developers, manufacturers, and service providers to use better security in order to be compatible with a platform.

7. **Insurance Industry** – The insurance industry can also influence security practices. Improving risk assessments by prioritizing better privacy and security requirements in their underwriting practices, alongside requiring systems or devices to have security certifications in order for their owners to be insurable, would exert positive market influence.[[38]](#endnote-36)

8. **Consumers** – Consumers must buy and use IoT devices responsibly. When buying a connected device, consumers should review the company’s support commitment and privacy policy. If this information is not readily available or if their privacy practices are unacceptable, look for another product. Once they own or are using a device, they need to regularly update and, when a device is beyond its expected life, replace it. Consumers should not have to risk having their personal information collected, sold and shared in perpetuity without explicit consent, but should be expected to recognize when clearly opting into such data collection and realize the added benefits may be a fair value-exchange.

**9. Governments -** Governments are responsible for strengtheningthe IoT security ecosystem by improving incentives for better security, strengthening accountability, improving security signaling and fostering tech neutral solutions. Governments can use their extensive buying power, alongside policy tools, to strengthen IoT security practices.

**III. Levels of the IoT Security Puzzle**

IoT security policies need to take a holistic view in order to make an impact. Sound security principles[[39]](#footnote-3) must be applied at all levels of the device ecosystem, including the device level, application level, and network level. In addition, IoT security extends to the level of the developers, since many products coming to market rely on third party or open source components and software.[[40]](#endnote-37)

The reason it is important to take a holistic view is that the system is only as strong as its weakest link. Devices may be tested in isolation and deemed to have sufficient security, but if the mobile application or back-end services are vulnerable, attackers could still compromise the security or privacy of those devices. Likewise, attackers could use weak device security to infiltrate an entire system and leverage their attack to impact many users of that service.

The other aspect of IoT security and privacy that is commonly overlooked is “sustainability,” or the lifecycle aspects of the products and services. For instance, how does someone hand over a smart home that may have a dozen or more connected devices, each with their own applications and back-end services? The same goes for devices such as fitness bands. IoT manufacturers need to offer safe, transparent and convenient ways to allow users to delete data or transition device use to someone else.

Policies that address all levels of the IoT ecosystem will be more effective. However, the security of an IoT device cannot be characterized as “secure” or “insecure”. Rather, it is useful to conceptualize IoT security as a spectrum of device vulnerability.[[41]](#endnote-38)

The complexity of the IoT system is compounded by its ties with Big Data and AI, each with its own set of security challenges and stakeholders.[[42]](#endnote-39) For instance, using AI seemingly innocuous data flows can be correlated to identify individuals and their habits, even predicting their behavior. If not correctly protected, this data could be used for anything from simple targeted marketing to spying, social engineering schemes, identity fraud, blackmail or even physical attacks.

**IV. Lessons Learned: Governance of Other Technologies**

When considering how to approach the governance of IoT, it may be helpful to consider what we can learn from the governance of other technologies.

The Internet

At one time, the Internet itself was a new technology. In late 90s, the U.S. government was considering its role in governing and regulating the Internet. The Telecommunications Act of 1996 determined that the government should avoid burdening the Internet with regulation. The following year, the FCC published “Digital Tornado: The Internet and Telecommunications Policy,” which emphasized that government policy approaches toward the Internet should start from two premises: avoiding unnecessary regulation and questioning the applicability of traditional rules.[[43]](#endnote-40) These premises were echoed in the Clinton administration’s 1997 *Framework for Global Electronic Commerce*.[[44]](#endnote-41)

This approach was key to the economic benefits the Internet has brought the U.S. and global community. Had the U.S. government taken an ex ante approach - developing regulations prior to the emergence of actualized harms in anticipation of potential worst-case scenarios – the Internet would not have the same global reach or enable such permissionless innovation.

In its 2017 *Fostering the Advancement of the Internet of Things* paper, NTIA credits the 1997 framework for promoting technology and innovation, and voices its support for its approach to governance,

*“Dating back at least to the 1997 Framework for Global Electronic Commerce, the U.S. Government has been operating under the principle that the private sector should lead in digital technology advancement. Even where collective action is necessary, the U.S. Government has encouraged multistakeholder approaches and private sector coordination and leadership where possible. When governmental involvement is needed, it should support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.”*

These principles have served the Internet well. Given that the IoT is an extension of the Internet itself, they are worth considering. However, others would argue that presuming that former regulatory provisions apply to new technologies is insufficient.[[45]](#endnote-42) Instead, a case-by-case approach that examines the strengths and weakness of previous regulations may be more effective.

Unmanned Vehicles

The regulation of commercial unmanned aerial vehicles is an ongoing case, one that has caused much frustration in the U.S. To date, the Federal Aviation Administration (FAA) has taken an *ex ante* approach, one that develops regulations in anticipation of potential harmful scenarios. However, this approach has slowed change in delivery services and transportation.

Some complain that the FAA has “dragged its feet” crafting final rules for the safe integration of commercial UAVs into U.S. airspace.[[46]](#endnote-43) However, it has taken an interesting approach in the interim – experimental regulation. In December 2013, the FAA approved six different research and test sites for UAVs. The idea of experimental regulation is to regulate within a restricted scope to test legal approaches or gather more information about them.[[47]](#endnote-44) However, the 2013 experiment did not result in more answers addressing how to regulate commercial UAVs. In fact, the Trump administration launched the new Unmanned Aircraft System Integration Pilot Program to gather input on how to craft rules for drones.[[48]](#endnote-45) The takeaway: experimental regulation can be an innovation-friendly approach, but one that needs to be accompanied by regulatory learning.

The debate over regulation of self-driving motor vehicles has echoed this takeaway. At a hearing titled “Self-Driving Vehicle Legislation” in June 2017, The U.S. Chamber of Commerce’s Technology Engagement Center (C\_TEC) outlined recommendations to craft policy regarding emerging technologies, a couple of which stand out.[[49]](#endnote-46) First, regulations should be technology-neutral to avoid indirectly picking technology winners and losers, which could hamper competition. Second, exemptions should be granted by regulators to ensure that entrepreneurs can test new technology. This recommendation points again to the value of experimental regulation.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**IV. Challenges to Crafting Consumer Device Standards in an IoT Environment**

There are four key challenges to making consumer device standards work in an IoT environment:

1. **Enforcing standards without stifling innovation.** If standards are too general, they become meaningless; if standards are too detailed, the burden of compliance will stifle innovation.[[50]](#endnote-47) This is even more true in such rapidly evolving area as the IoT. The costs of implementation should be kept to a reasonable level when possible, although this may be challenging. Any consumer device standards must try to strike an appropriate balance.
2. **Taking into account the entire IoT ecosystem.** IoT security is bigger than devices; consumer device standards must address the systems and services around them, which brings supply chain dynamics into play. Effective consumer device standards will address far more than the devices themselves, to include associated software/firmware development and updates, and related services.
3. **Looking ahead.** To craft effective standards, policymakers and standards development organizations (SDOs) need to look ahead and take into account (where applicable) other factors such as Big Data and AI.[[51]](#endnote-48) If consumer device standards are established, they must leave room for change and flexibility to accommodate emerging challenges.
4. **Security is not a state.** The security of an IoT device is not static. If consumer device standards are reduced to a one-off compliance check, they will be less effective. A more effective approach should include assessing the general security posture of the vendor, its ISM (Information Security Management) processes, including supply chain security management and software quality assurance.

Policymakers looking to craft effective consumer device standards that address these challenges might look to initiatives like the [OTA IoT Trust Framework®](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework2.1.pdf)[[52]](#endnote-49) Consumer Reports’ [“The Digital Standard”](https://www.thedigitalstandard.org/the-standard)[[53]](#endnote-50), [Underwriters Labs Cybersecurity Assurance Program](https://industries.ul.com/cybersecurity), or [ENISA’s Baseline Security Recommendations for IoT](https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot).

**The OTA IoT Trust Framework** includes 40 principles aimed at manufacturers and service providers, addressing privacy, security, and sustainability of IoT systems. Because the framework centers around strategic principles, it is relevant to the entire IoT ecosystem. Since the framework was developed through a consensus driven multi-stakeholder process, stakeholders had the opportunity to voice their concerns if the cost of implementation was stifling. The framework is a mix of core requirements and recommendations. The framework is managed via OTA’s IoT working group, and updated as necessary approximately twice a year. Typically, updates occur to reflect activity and output from other multi-stakeholder IoT efforts where OTA has been involved.

**The Digital Standard** defines and reflects consumer values that should be addressed in IoT products. The standard was developed by Consumer Reports, an independent, nonprofit organization based in the U.S. The Digital Standard is organized by general “tests” which are broken down into more detail with criteria, indicators, and procedure overview. The tests can be applied to almost all levels of the device ecosystem. Room for change and flexibility is built in by categorizing each test in one of three categories: (1) well understood with a developed testing approach in place, (2) under development with some outstanding questions, and (3) under development, usually due to the sensitivity and complexity of the issue.[[54]](#endnote-51) By inviting broad participation to collaborate in the development of the standards, smaller stakeholders are able to provide their input.

**The Underwriters Labs Cybersecurity Assurance Program (UL CAP)** offers testing security criteria based on UL 2900 cybersecurity standards or custom requirements. The testing criteria evaluate software vulnerabilities and weaknesses. The White House Cybersecurity National Action Plan (CNAP) cited the program as a way to test and certify network-connectable devices within the IoT supply chain.[[55]](#endnote-52) The UL CAP 2900 set of standards was developed with input from major stakeholders representing the U.S. government, academia and industry.[[56]](#endnote-53)

**European Union Agency for Network and Information Security (ENISA)’s Baseline Security Recommendations for IoT** includes detailed security measures / good practices in Annex A. The recommendations are unique because they are geared toward the context of Critical Information Infrastructures. The annex breaks down issues like “privacy by design” into actionable good practices, with references for those seeking more detail. The recommendations were developed by interviewing experts in industry, policy, academia, as well as research organizations from 9 EU member states and from the United States of America.[[57]](#endnote-54)

Endnotes

1. Atkinson, Robert, “ICT Innovation Policy in

   China: A Review,” *Information Technology and Innovation Foundation*, <http://www2.itif.org/2014-china-ict.pdf> [↑](#endnote-ref-1)
2. Atkinson, Robert, “ICT Innovation Policy in

   China: A Review,” *Information Technology and Innovation Foundation*, <http://www2.itif.org/2014-china-ict.pdf> [↑](#endnote-ref-2)
3. “EU-China Joint Paper on the Internet of Things,” *China Academy of Information and Communication Technology (CAICT)*, *European Commission – DG CONNECT,* <https://euchina-iot5g.eu/wp-content/uploads/EU-China_Joint_White_Paper_on_the_Internet-of-Things.pdf> [↑](#endnote-ref-3)
4. Flanagan, Eleanor. “When ICT Policy Goes Global,” *Ericsson Business Review*, <https://www.ericsson.com/en/publications/ericsson-business-review/eastern-time-when-ict-policy-goes-global> [↑](#endnote-ref-4)
5. Flanagan, Eleanor. “When ICT Policy Goes Global,” *Ericsson Business Review*, <https://www.ericsson.com/en/publications/ericsson-business-review/eastern-time-when-ict-policy-goes-global> [↑](#endnote-ref-5)
6. “EU-China Joint Paper on the Internet of Things,” *China Academy of Information and Communication Technology (CAICT)*, *European Commission – DG CONNECT,* <https://euchina-iot5g.eu/wp-content/uploads/EU-China_Joint_White_Paper_on_the_Internet-of-Things.pdf> [↑](#endnote-ref-6)
7. “Digital Agenda 2020 for Estonia,” *Ministry of Economic Affairs and Communications*, <https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf> [↑](#endnote-ref-7)
8. “Estonia,” *Open Government Partnership*, <https://www.opengovpartnership.org/countries/estonia> [↑](#endnote-ref-8)
9. “Cyber Security Strategy 2014-2017,” *Ministry of Economic Affairs and Communication*, <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> [↑](#endnote-ref-9)
10. Pohle, Julia, “Analysing internet policy as a field of struggle,” *Internet Policy Review*,

    <https://policyreview.info/articles/analysis/analysing-internet-policy-field-struggle#footnote17_m2j7fmp> [↑](#endnote-ref-10)
11. Pohle, Julia, “Analysing internet policy as a field of struggle,” *Internet Policy Review*, <https://policyreview.info/articles/analysis/analysing-internet-policy-field-struggle#footnote17_m2j7fmp> [↑](#endnote-ref-11)
12. Kranz, Maciej, “Government’s Role in the Internet of Things,” *Cisco Blogs*, <https://blogs.cisco.com/innovation/governments-role-in-the-internet-of-things> [↑](#endnote-ref-12)
13. Gollatz, Kirsten, “Enquete Commission on Internet and Digital Society,” *Global Network of Internet and Society Research Centers*, <https://publixphere.net/i/noc/page/IG_Case_Study_EnqueteKommission_Internet_und_digitale_Gesellschaft> [↑](#endnote-ref-13)
14. “Binsch, Jessica, “Network politicians call for Internet Ministers,” *Spiegel Online*,

    <http://www.spiegel.de/netzwelt/netzpolitik/internet-enquete-fordert-ausschuss-und-minister-a-895256.html> [↑](#endnote-ref-14)
15. “Industry 4.0: The Digital Revolution in Manufacturing,” *Federal Ministry of Economic Affairs and Energy*, <https://www.de.digital/DIGITAL/Redaktion/EN/Standardartikel/G20-Shaping-Digitalisation/global-innovative-fair-3-industry-4-0.html> [↑](#endnote-ref-15)
16. “Internet of Things,” *Ministry of Electronics and Information Technology*, <http://meity.gov.in/content/internet-things> [↑](#endnote-ref-16)
17. “IoT Policy Document,” *Ministry of Electronics and Information Technology,*  <http://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf> [↑](#endnote-ref-17)
18. Flanagan, Eleanor. “When ICT Policy Goes Global,” *Ericsson Business Review*, <https://www.ericsson.com/en/publications/ericsson-business-review/eastern-time-when-ict-policy-goes-global> [↑](#endnote-ref-18)
19. Flanagan, Eleanor. “When ICT Policy Goes Global,” *Ericsson Business Review*, <https://www.ericsson.com/en/publications/ericsson-business-review/eastern-time-when-ict-policy-goes-global> [↑](#endnote-ref-19)
20. “Statement from Japan at Opening Segment,” *Ministry of Internal Affairs and Communications*, <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Japan_opening_statemant_2017.pdf> [↑](#endnote-ref-20)
21. “Statement from Japan at Opening Segment,” *Ministry of Internal Affairs and Communications*, <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Japan_opening_statemant_2017.pdf> [↑](#endnote-ref-21)
22. “Statement from Japan at Opening Segment,” *Ministry of Internal Affairs and Communications*, <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Japan_opening_statemant_2017.pdf> [↑](#endnote-ref-22)
23. “Consultations,” *Infocomm Media Development Authority*, <https://www.imda.gov.sg/regulations-licensing-and-consultations/consultations> [↑](#endnote-ref-23)
24. “TSAC Standards-Setting Framework & Procedures,” *Infocomm Media Development Authority,* <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/industry-committee-and-working-gps/tsac/tsac_framework.pdf?la=en> [↑](#endnote-ref-24)
25. Flanagan, Eleanor. “When ICT Policy Goes Global,” *Ericsson Business Review*, <https://www.ericsson.com/en/publications/ericsson-business-review/eastern-time-when-ict-policy-goes-global> [↑](#endnote-ref-25)
26. “Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society,” *Government of the Republic of Korea Interdepartmental Exercise*, <file:///Users/carolin/Downloads/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf> [↑](#endnote-ref-26)
27. “Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching,” *National Telecommunications and Information Administration*, <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security> [↑](#endnote-ref-27)
28. “H.R.1324 - Securing IoT Act of 2017,” *Congress.gov*, <https://www.congress.gov/bill/115th-congress/house-bill/1324> [↑](#endnote-ref-28)
29. “DOT - How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century,” *Department of Transportation*, <https://www.transportation.gov/government-affairs/testimony/dot-how-internet-things-iot-can-bring-us-transportation-and> [↑](#endnote-ref-29)
30. “What We Do,” *Federal Communications Commission*, <https://www.fcc.gov/about-fcc/what-we-do> [↑](#endnote-ref-30)
31. “About NTIA,” *National Telecommunications and Information Administration,* <https://www.ntia.doc.gov/about> [↑](#endnote-ref-31)
32. © 2017 All Rights Reserved. Online Trust Alliance (OTA) / The Internet Society (ISOC) [↑](#footnote-ref-1)
33. It is not uncommon for devices to remain in service long after their officially supported lifespan. [↑](#footnote-ref-2)
34. <https://www.internetsociety.org/blog/2017/02/the-internet-of-things-as-an-attack-tool/> [↑](#endnote-ref-32)
35. “Mutually Agreed Norms for Routing Security (MANRS),” *Internet Society*, [↑](#endnote-ref-33)
36. “Paths to Our Digital Future,” *Internet Society*, <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf> [↑](#endnote-ref-34)
37. Robachevsky, Andrei, “Can IoT platforms from Apple, Google and Samsung make home automation systems more secure?,” *Internet Society* <https://www.internetsociety.org/blog/2017/09/can-iot-platforms-apple-google-samsung-make-home-automation-systems-secure/> [↑](#endnote-ref-35)
38. “Paths to Our Digital Future,” *Internet Society*, <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf> [↑](#endnote-ref-36)
39. Security Principles for IoT can be found in the OTA IoT Trust Framework® at <https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework2.1.pdf> [↑](#footnote-ref-3)
40. “IoT Security & Privacy Trust Framework v2.0,” *Online Trust Alliance*, <https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework2.1.pdf> [↑](#endnote-ref-37)
41. “The Internet of Things: An Overview,” *Internet Society*, <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf> [↑](#endnote-ref-38)
42. Robachevsky, Andrei, “There Is No Perimeter in IoT Security,” *Internet Society,* <https://www.internetsociety.org/blog/2017/06/there-is-no-perimeter-in-iot-security/> [↑](#endnote-ref-39)
43. “Digital Tornado: The Internet and Telecommunications Policy,” *Federal Communications Commission*, <https://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf> [↑](#endnote-ref-40)
44. “About a Framework for Global Electronic Commerce,” *The Clinton White House*, <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/about.html> [↑](#endnote-ref-41)
45. Stokes, Elen, and Diana M. Bowman. "Looking Back to the Future of Regulating New Technologies: The Cases of Nanotechnologies and Synthetic Biology."*European Journal of Risk Regulation: EJRR*, vol. 3, no. 2, 2012, pp. 235-241*, Research Library*, <https://search.proquest.com/docview/1026948521?accountid=142883> [↑](#endnote-ref-42)
46. Hagemann, Ryan, “A Regulatory Framework for Emerging Economies,” *1776*, <https://www.1776.vc/insights/regulation-emerging-technology-government-drones-hyperloop/> [↑](#endnote-ref-43)
47. Ranchordás, Sofia. "INNOVATION-FRIENDLY REGULATION: THE SUNSET OF REGULATION, THE SUNRISE OF INNOVATION."*Jurimetrics*, vol. 55, no. 2, 2015, pp. 201-224*, Research Library*, <https://search.proquest.com/docview/1727961449?accountid=142883>. [↑](#endnote-ref-44)
48. Stewart, Jack, “President Trump Moves to Fill America’s Skies with Drones,” *Wired*, <https://www.wired.com/story/faa-trump-drones-regulations/> [↑](#endnote-ref-45)
49. “Testimony of Tim Day,” *House Energy and Commerce Committee*, <http://docs.house.gov/meetings/IF/IF17/20170627/106182/HHRG-115-IF17-Wstate-DayT-20170627.pdf> [↑](#endnote-ref-46)
50. Robachevsky, Andrei, “There Is No Perimeter in IoT Security,” *Internet Society,* <https://www.internetsociety.org/blog/2017/06/there-is-no-perimeter-in-iot-security/> [↑](#endnote-ref-47)
51. Robachevsky, Andrei, “There Is No Perimeter in IoT Security,” *Internet Society,* <https://www.internetsociety.org/blog/2017/06/there-is-no-perimeter-in-iot-security/> [↑](#endnote-ref-48)
52. “Internet of Things,” *Online Trust Alliance*, https://otalliance.org/initiatives/internet-things [↑](#endnote-ref-49)
53. “The Digital Standard,” *Consumer Reports*, https://www.thedigitalstandard.org/ [↑](#endnote-ref-50)
54. “The Standard,” *Consumer Reports*, <https://www.thedigitalstandard.org/the-standard> [↑](#endnote-ref-51)
55. “Fact Sheet: Cybersecurity National Action Plan,” *The White House: President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> [↑](#endnote-ref-52)
56. “UL Global Cybersecurity Services & Standards,” *The Underwriters Labs*, <https://industries.ul.com/wp-content/uploads/sites/2/2017/04/UL_CAP_Overview.pdf> [↑](#endnote-ref-53)
57. “Baseline Security Recommendations for IoT,” *European Union Agency For Network And Information Security*, <file:///Users/carolin/Downloads/WP2017%20O-1-1-2%201%20Baseline%20Security%20Recommendations%20for%20IoT%20in%20the%20context%20of%20CII_FINAL.pdf> [↑](#endnote-ref-54)