Canadian Multistakeholder Process: Enhancing IoT Security

Report on Consumer Protection through Digital Standards Webinar

Location: Online
Date: July 14, 2018
Remote Attendance: ~15
Video Link: https://bit.ly/2M0FYlH

Overview:

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

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

On 14 June, the Planning Committee organized a webinar to further the discussion on Consumer Protection. Tatevik Sargsyan, Senior Research Fellow with Ranking Digital Rights (RDR) presented and discussed RDR's partnership with Consumer Reports to develop the Digital Standard and assess IoT based on privacy and security criteria in the Digital Standard.

The Digital Standard is an open source initiative, which consists of privacy and security standards reflecting best practices in the areas of encryption, security oversight, privacy by default, data collection and control, transparency, and others. Its long-term goals are to help guide the future design of IoT products, enabling consumer organizations to test and report on whether new products protect consumer security and privacy, and to empower consumers to make informed choices.

Key Points:

Ranking Digital Rights is a research initiative that sets global standards for how companies in the information and communication technology sector should respect user human rights. The project produces an annual corporate accountability index that ranks 22 internet, mobile, and telecommunication companies on their commitments to freedom of expression and privacy.

The Digital Standard is an open-source project that includes privacy and security standards, collectively developed by Consumer Reports, Ranking Digital Rights, the Cyber-independent Testing Lab, and other contributors. Some of their evaluation frameworks are either directly borrowed or adapted from the corporate accountability framework. The primary goal of the standard is to provide an effective assessment tool to consumer organizations or researchers to evaluate and test internet-connected products and services. This establishes a privacy and security baseline, allowing users to make more informed choices.

There is overlap between both initiatives in that they both aim provide a roadmap for manufacturers to use in the design of consumer products, as well as provide a tangible backing for consumer protection policy considerations. The Digital Standard covers security, privacy, ownership, as well as governance and compliance. The basic principles of the standard are:

1. Products should be secure;
2. Consumer information should be kept private;
3. Consumers should have and maintain ownership rights;
4. Products should be designed in a way that help protect privacy and other human rights, such as freedom of expression.

Frameworks such as The Digital Standard aim for consumer empowerment by creating an environment which challenges manufacturers and service providers to adopt improved privacy and security behaviors. By helping consumers shop with these factors in mind, it will encourage companies to respond and improve in those areas. This incentivizes companies to publish device information in very simple language that is easily understandable. This extends not only to general data protection information, but also how products should and should not be used to ensure the highest degree of privacy and security (for instance: IP cameras that can help protect the home but can also intrude the neighbors' privacy). Especially for small manufacturers, the Digital Standard can be a good roadmap to outline what basic requirements a product should meet before it goes to the market. When this roadmap is adopted, a positive review from Digital Standard users help improve the reputation of organizations with strong privacy and security practices, which often translates into an increased market share and revenue.

There are various challenges with the Digital Standard and other similar standards which are persistent. Arguably the most difficult challenge is with respect to the limited ability to of Ranking Digital Rights collaborators to test the security and privacy of products beyond what is disclosed by companies. This leads to situations where a company might have a great privacy and security practices which are not captured by information released to the public. Conversely, a company may have adequate transparency and disclosure practices, but they may not highlight flaws in their security practices. Any one of these factors could be overlooked due to the capacity of those providing evaluation on behalf of the Digital Standard. There are also challenges with maintaining the standard itself by having to continually collaborate with stakeholders using consensus-based approaches to adapt to emerging issues. Constant improvement in all these areas is necessary to maintain the reputation of the standard itself.

As a group, we also recognized that because the IoT supply chain is so complex there may be a need to create guidelines for actors in the chain should review and choose their own vendors, because it's becoming more and more essential. This "chain responsibility" is also one of the elements in GDPR. There is a need for some very good key recommendations in this area that product manufacturers and service providers ought to adopt.

Finally, we discussed the importance of understanding the business model(s) of companies in the IoT value chain and how these impact digital rights and privacy. Various questions ought to be considered, including: What do they make money on? Sharing data? If so – is that clear, and is there a fair price for using that data (e.g. discounts)? More importantly: what is it the consumer cares about, what do they expect, how can this best be communicated (through a label?)? Ideally, any communication plan ought to include a description of a product's functionality throughout its life cycle – which includes an outline of what occurs after the product is disposed of. Is this included?

In conclusion: open standards can help consumers make smarter choices. Consumers that make smarter choices buy products from suppliers that are more secure and transparent. This has knock-on *effects within the marketplace, stimulating changes to products and organizational practices which are increasingly consumer-centric. This suggests that an important aspect of the Canadian Multistakeholder Process ought to be to help consumers understand what the stakes are in each of these products and product categories. In this sense, there may be overlaps between the Consumer Education and Labelling Working Groups.*