Labelling for Smart Devices Discussion Paper

Charu Bhardwaj

8/27/21

Labelling for Smart Devices

Executive Summary

IoT devices are rapidly expanding their capability to connect a number of electronic devices simultaneously for the purpose of collecting and sharing data over the internet. This is happening at a rate which is way faster than the rate at which they are being secured. We are seeing continuous improvement in the functionality and efficiency of their connectivity as more and more IoT devices enter the consumer market. Commonly, most IoT devices have poor security and are vulnerable to attacks by the hackers or cyber-criminal groups who could take control of the device and run their malicious code on them with ease. An effective way forward is to improve our national approach to cyber hygiene by labelling the IoT devices to provide transparency for the consumers.

It is important to note that consumers care about a lot of things when it comes to their privacy but sometimes it is contradictory as they also want the latest shiny things and will buy any fad gadgets that hit the market without an understanding of how the devices could impact them if the devices were to be compromised. Also, customers right now might not even want to pay extra for cyber security as the expectation is they are inbuilt which poses a challenge for the IoT manufacturers.

Introduction

This discussion paper looks at how countries such as Singapore and Canada are looking at managing their IoT device labelling. We will also look at how a successful labelling scheme can be introduced in Australia which is a challenge since there are no current direct financial benefits attached with purchasing devices with a better cyber security rating.

With a number of cyber security threats lurking around due to IoTs exponential growth, a number of countries are already moving towards IoT labelling scheme to protect vulnerable consumers from malicious attacks that could impact them financially, emotionally and psychologically. The evolution of labelling is not going to be a straightforward path but one of collaboration between different countries to establish standardisation in how IoT products manufactured within the country as well as imported from other countries can be labelled to avoid confusion and to achieve compliance [1].

Smart Nation Vision

Singapore is looking at introducing a level rating scheme which will allow customers to determine the level of security that is offered by the manufacturer of the IoT device and encourage consumers to be more security conscious when buying such devices. Labelling is a sure shot way of helping IoT manufacturers differentiate their products and by including secure-by-design in their product design lifecycle phase, the cost of compliance across nations could be reduced through mutual recognition. The four levels of labelling scheme that Singapore is looking at introducing include meeting basic security requrements, adherence to the principles of security-by-deisgn, absence of known common software vulnerabilities and resistence against common cyber attacks [2].

Standardisation is a critical part of enabling product comparisons to avoid consumers from getting frustrated and confused. However, the practical perspective can be quite challenging as the manufacturers have to balance both detailed as well as technical information with consumer needs. The labels can be used to provide direct information to the customers on how the device is to be used and pointers can be included for customers (using QR code) to obtain detailed and reliable information on how the product was tested, what protections are included, how was the product configured when tested, if all components were considered etc. Issues around how patches and updates are going to be addressed will also need to be considered [3].

Enhancing IoT Security through IoT Device Labelling

Another thing to consider is that labelling should not only be on the devices but also online as most purchase decisions in this dynamic world are made online. In Europe, the organisations are considering visualisation of labels i.e. basic level, high level and substantial levels whilst ensuring that any certification schemes are flexible and agile as the whole certification process can be quite time consuming which is at odds with how fast-past the technology is developing. It is also important that the developers start thinking about the emergent threats that may arise over a period of time and start including them during their security-by-design phase.

‘

The labels are meant to make sure they do what the consumers expect them to do and help set the frame for other devices that might be hooked into them. It is also important that these labels also provide info on how they can be disposed off in an environmentally sensible way once they reach the end of their lifecycle [3].

Role of the Government

The role of the government with labelling is to ensure policy coherence across different policies that are established. The government can perform a co-regulatory function and it is suggested that investments be made to educate its citizens on the why and what of cyber security. The government will also have to ensure there are consequences for the companies that are not complying with the regulatory requirements as otherwise there are chances of companies ignoring security requirements. Violations can be reported to a central authority and ongoing auditing will help ensure cyber security is embedded in all future IoT devices [4].

Conclusion

By raising the cyber seurity hygiene and incentivising developers to produce more secure products, Australian Government can help build a secure cyberspace for their citizens. The most important thing to consider is how to build and maintain trust amongst consumers if they put their faith in the labelling process. IoT labelling compliance is an opportunity for the organisations to wake up and understand the importance of a secure development cycle. There has to be some form of motivation for the manufacturers as they will be wary of labelling their product because that could have some legal implications in case their product was hacked.

Australian government can work in collaboration with other nations in ensuring standardisation is at the crux of IoT development in the future to avoid confusion and frustration amongst consumers and to also protect them from cyber attacks.

May be blockchain could provide an answer to solving a lot of problems in the future for the IoT devices but for now, there is still a lot of opportunity that needs to be explored.

Bibliography

1. Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong 2020, The impact of IoT security labelling on consumer product choice and willingness to pay, available at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800.
2. Youtube.com. 2021. *Cybersecurity Labelling Scheme*. [online] Available at: <https://www.youtube.com/watch?v=JJubrOX0FWY> [Accessed 27 August 2021].
3. Youtube.com. 2021. *Cybersecurity Labelling Scheme*. [online] Available at: <https://www.youtube.com/watch?v=JJubrOX0FWY> [Accessed 27 August 2021].
4. *Report on Labelling Webinar*, 2018. Canadian Multistakeholder Process: Enhancing IoT Security. [online] Available at: <https://iotsecurity2018.ca/wp-content/uploads/2018/10/Labelling-Webinar-Report-August-1-2018.pdf> [Accessed 27 August 2021].