Quokka

3031 Tisch Way, Ste 505
San Jose, CA 95128, USA
www.quokka.io

25 October 2024

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
pjcis@aph.gov.au

Submission relating to the "Cyber Security Bill 2024"

Dear Committee

Thank you for the opportunity to provide input on this important work.

About Quokka

Quokka is a global organisation, headquartered in Silicon Valley, with roots in a US DARPA project, focusing on making mobile applications and smartphone safe to use in the US defence force. Among current customers we find the US Cybersecurity & Infrastructure Agency and the US Department of Homeland Security, and many others.

Scope of Submission

This submission from Quokka relates to "Part 2 – Security Standards for Smart Devices" of the "Cyber Security Bill 2024".

Executive Summary

This submission argues that

- the **definition of the Product** is unclear, and further,
- for the Security Standard to be meaningful, the definition of product should be the **combination of the Smart Device and its Companion App**.

The definition of the Product

Since the Bill is referring to the smart device as a **Product,** (Part 2, Division 1 of the Bill, page 12-14), we find it fundamental to the Bill to be clear on what defines a Product.

In our opinion the Product the consumer buys and/or uses, is **the combination of the Device and its Companion App**. In most cases, without the companion app, you don't really have usable product.

But more importantly, the standard sets out that the user must be able to set their own password, and that in most cases requires the use of the companion app. That basically means that in order for the device to fulfill the requirements of the standard, you will need a companion app. They cannot be separated.

The product discussed in Part 2, Division 1, of the Bill must thus include the companion app to be meaningful. And conversely, without any mentioning of the App in the product definition, one could argue that the Bill leaves the product undefined.

Examples from legal discussion from a Consumer rights perspective

Below some examples where the inclusion of the App as part of the product is discussed.

"If an IoT device requires an app to function, the app is typically considered an essential component of the overall IoT product, even though it might not be physically part of the device. Legally, whether the app is considered part of the product depends on the terms of service, warranties, and other agreements associated with the device."

"From a consumer and regulatory perspective, the app could be seen as part of the product ecosystem. This means that both the device and the app work together to provide the intended functionality, and the app's performance can influence the overall user experience and satisfaction with the product. In some cases, legal obligations related to product quality, security, and data privacy might extend to both the physical device and the accompanying app."

"For example, if an IoT device manufacturer guarantees a certain level of service or features that rely on the app, any failure of the app could affect liability or warranties related to the product as a whole."

A legal case where the App was considered part of the inadequate security

In the Ring LLC class action lawsuits, 2019-2020, the fault was attributed to both the cameras and the companion app. The primary issue stemmed from inadequate security measures in the Ring ecosystem, which included vulnerabilities in the cameras and a lack of robust protection in the app.

1. Camera Vulnerabilities: The cameras themselves had weak security protocols, including hard-coded or easily guessable passwords. Hackers were able to exploit these flaws to gain unauthorized access, allowing them to view live feeds and control the devices.

2. App Security Flaws: The companion app was also criticized for not enforcing stronger security measures, such as multi-factor authentication. This made it easier for hackers to gain access to the camera systems through user accounts by exploiting poor password hygiene or using leaked passwords from other breaches.

Overall, the combination of insufficient security in both the hardware and software components led to these breaches, highlighting the importance of securing the entire IoT ecosystem.

Companion Apps for IoT Devices worse than other Apps

In fact companion apps for smart devices are often a much higher security risk than other apps on a consumer's smartphone. Please see the list below why IoT Companion Apps poses higher threats than General Purpose Apps.

- **Higher Collusion Threat:** There's a significant risk of collusion between smart devices and companion apps, allowing them to combine personal data and device-collected information, which can bypass existing security defenses.
- **Increased Access to Data:** Companion apps can access data from connected smart devices, bypassing the restrictions that mobile operating systems impose on general-purpose apps, leading to potential privacy concerns.
- **Lack of User Control:** Users have limited visibility and control over the data collected and shared by smart devices through companion apps, unlike with general-purpose apps where permissions are more transparent.
- **PII (Personal Identifiable Information) data threat:** While general-purpose apps often use ads and trackers for revenue, companion apps and even IoT devices themselves increasingly include these elements, leveraging their unique data access for additional income.

Examples of IoT-related cyber legislation that indirectly or directly address companion apps

1. U.S. IoT Cybersecurity Improvement Act of 2020

This act focuses on setting minimum security standards for IoT devices used by the federal government. While it primarily addresses IoT devices, it encourages strong security practices, which can extend to companion apps that interact with these devices. For example, secure development practices and vulnerability management, both of which could apply to apps as well as devices.

2. California Senate Bill 327 (SB-327)

This was one of the first IoT-specific laws in the U.S. It requires manufacturers of IoT devices to equip devices with reasonable security features that protect the data and prevent unauthorized access. Although the law primarily focuses on device security, companion apps would need to comply with this law if they are necessary for the device's functionality and impact the security of the device.

3. European Union Cybersecurity Act (2019)

This act establishes a framework for the certification of IoT devices in terms of cybersecurity. While not directly targeting companion apps, it encourages the development of secure-by-design IoT ecosystems. Since companion apps are often integral to device functionality, they are expected to follow the security guidelines that ensure the safety of both devices and the networks they connect to.

4. UK Product Security and Telecommunications Infrastructure Bill (2022)

This UK legislation mandates specific cybersecurity requirements for smart devices sold in the country. It covers things like unique passwords, vulnerability disclosure processes, and keeping software up-to-date. While it doesn't explicitly mention companion apps, any app associated with a smart device must adhere to these rules, especially in areas like secure communication with the device, updates, and password management.

5. Singapore's Cybersecurity Labelling Scheme (CLS)

Singapore has introduced a cybersecurity labelling scheme for consumer IoT devices, where devices are rated based on their security features. Companion apps are a vital part of the IoT product's overall security. Hence, this scheme covers apps by assessing whether an IoT product as a whole (including the companion app) meets certain cybersecurity standards.

Key Areas Where Companion Apps are Affected

- Data Transmission Security: Ensuring that data sent between the app and the IoT device is encrypted and secure.
- Authentication and Authorization: Strong password policies, two-factor authentication, and user authentication are required for both IoT devices and companion apps.
- Regular Updates: Companion apps must be regularly updated to fix vulnerabilities, aligning with legislation requiring continuous security patches for IoT devices.
- Privacy Protections: Since companion apps often collect PII, privacy laws such as GDPR and CCPA apply, ensuring proper data handling and user consent.

Singapore's Cybersecurity Labelling Scheme

Singapore's Cybersecurity Labelling Scheme, CSL, clearly include the Companion App in the IoT Product to pass the Cybersecurity Standard.

Already in the definitions in the publication for the *Assessment Methodology* that applies even for the developer's self-declaration for Level 1, the **Authentication Interface** is recognised as being either on the device itself, or its companion application. Please see below.

DEFINITIONS

Term	Definition
Authentication Interface	Interfaces on the device (or its companion application/services) that requires user interaction for authentication. Examples: GUI login portal, Mobile application login page, etc.

As you apply for higher levels of certification, you have to have your device tested in a lab, and from these Singapore CSL Level 3 testing requirements we ca read:

"The test laboratory shall determine if the firmware and companion mobile application of the Device Under Test (DUT) is free from common software errors such as buffer overflown, known vulnerabilities in any of the third-party libraries being used, and known malware."

Please note the specific mentioning of both the **firmware and companion mobile application** of the Device Under Test (DUT).

Conclusion

What we have tried to illustrate in this submission is the importance of including the companion app in the definition of the product that has to fulfil the standard outlined in Part 2, of the Bill. And further, not mentioning the companion app leaves the product undefined.

If you allow a somewhat crude analogy, having a Cyber Security standard for an IoT product, omitting the required or for practical use needed Companion App, is like having a standard for a safe, only addressing the thickness of the steel walls, but omitting any requirements on the door and the lock of the safe, that is actually what in most cases will be used to access the safe, similarly to how the app is used to access and control the device. It will address only a small fraction of the real threat spectrum.

Thank you for the opportunity to maintain an ongoing dialog on his topic, and we look forward to anyway we could be of further assistance.

Best Regards,

[redacted]

Hakan Eriksson

APAC Executive, Quokka

[redacted]