Submission in Response to the Parliamentary Joint Committee on Intelligence and Security regarding the inquiry into the Cyber Security Legislative Package 2024, October 2024

Prepared by Rebecca Trapani on Monday, 14 October 2024

Thank you for the opportunity to submit comments to the Parliamentary Joint Committee on Intelligence and Security regarding the inquiry into the Cyber Security Legislative Package 2024. In particular, I would like to address **Part 2—Security standards for smart devices**.

As an information security professional of eight years, privacy advocate, and Australian resident, I've seen a significant number of consumer-grade electronics exposed to the internet, often without the users' knowledge. Devices ranging from baby monitors to home security systems are left unsecured and accessible to anyone with an internet connection, simply because they are poorly configured or use default settings that allow easy access.

In many cases there sophisticated hacking isn't required to access these systems. These devices are openly available to anyone on the internet who knows their IP address. In my time as a security researcher, I've encountered a wide variety of results, from sleeping babies visible on unsecured baby monitors to a prized pot plant, and even a live feed of a suburban driveway. While these examples may seem trivial or even humorous, they point to a much larger, terrifying reality—one that most people are unaware of. Devices that are not properly secured by the manufacturer are constantly exposed to the internet, often without the user's knowledge or consent.

Case Study: Ecovacs Deebot X2 Hacking Incident

This exposure is not just theoretical—it is a real, present threat, as demonstrated by a recent hacking incident reported by Cyber Daily[1] on 14 October 2024. According to the article citing an ABC report, a hacker remotely took control of several Ecovacs Deebot X2 robot vacuums, using their live camera feed and remote control features to wreak havoc in the homes of unsuspecting device owners.

One user who spoke to the ABC said that despite restarting the device and resetting his password, the vacuum continued to cause issues. "I got the impression it was a kid, maybe a teenager," said the owner, "Maybe they were just jumping from device to device, messing with families." His primary concern was the device's ability to be used for surveillance and spying. He worried that the robot could watch him or his family undressed, and the issue was only resolved when he turned the device off and stored it in his garage.

The ABC also reported another user’s Deebot X2 being hacked, resulting in the vacuum chasing their dog around the house while shouting racial slurs. This chaotic and invasive behavior, along with the ability to take control of devices meant for personal use, underscores the severity of the threat posed by insecure smart devices.

The ABC had previously demonstrated this vulnerability in an investigation on 4 October 2024, proving that the Deebot X2 had a security flaw by hacking into the device and taking control of the video feed. Despite activating the camera, the vacuum failed to play the alarm that should have notified the owner, making it a silent and dangerous surveillance tool.

It remains unclear how many devices were affected by this hacking incident, but it is a stark reminder of the vulnerabilities that exist in smart devices today and the real-world consequences for consumers.

This report is an alarming indicator of how pronounced problems like this are. So the mandatory cyber security standards for smart devices introduced by the **Cyber Security Bill 2024** is a welcome step in addressing cyber security flaws in smart devices.

Supporting Consumer Law

From my reading of the bill, it specifies that manufacturers and suppliers of smart devices must comply with security standards. However, the bill doesn't clearly indicate that these standards will be directly enforced through Australian Consumer Law (ACL). Instead, it suggests that there will be rules set out in the bill itself and that enforcement mechanisms, such as compliance notices, stop notices, and recall notices, will be used by the government to ensure adherence.

This to me suggests there is potential for overlap with Consumer Law, especially since devices that don’t meet these security standards could be deemed as unsafe or unfit for purpose, which are key criteria under the ACL. It's possible that Consumer Law could complement the bill by providing additional avenues for enforcement, particularly if insecure products cause harm to consumers. However, this hasn’t been explicitly outlined yet.

I would like to see future regulatory developments or further legislative reforms will clarify how these cyber security standards interact with Consumer Law. Given the broad scope of consumer electronics impacted, many stakeholders are calling for stronger integration with Consumer Law to ensure comprehensive protection.

Addressing Existing Challenges With Product Recalls and Consumer Rights

In a similar vein, for non-compliance, the bill includes provisions for issuing compliance notices, stop notices, and recall notices. These mechanisms allow authorities to prevent the sale of non-compliant products in Australia, enforce recalls, or impose penalties.

However, there is already a significant issue with product recalls in Australia. The Australian Competition and Consumer Commission (ACCC) noted in 2019,[2] that while around 650 products are recalled each year, only about half of these are ever returned.

As it currently stands I believe that even if the Bill were to be successful there is a significant risk that if a recall were announced for an insecure product that poses a security or privacy risk, the percentage of devices returned would not be significantly higher than the current figures. This raises concerns about the effectiveness of the recall process when applied to cyber security risks in consumer electronics.

If only half of recalled products are being returned, that leaves a large number of potentially vulnerable devices still in circulation, continuing to pose risks to consumers' privacy and security. This gap in enforcement needs to be addressed for the bill to truly protect consumers.

The Federal Government should consider strengthening the existing recall system to ensure that when a product is identified as insecure, there are more effective mechanisms to ensure that the majority of affected devices are either returned, repaired, or rendered inoperable. This could involve tighter regulations for online marketplaces or stricter penalties for non-compliance to ensure that insecure products are swiftly removed from the market.

I think this is also an indicator that the Federal Government must consider the overlap with Consumer Law sooner rather than later, and work to strengthen Consumer Law by considering the ACCC's recommended safety duty for businesses, a proposal the ACCC suggests would require businesses to take reasonable steps to ensure that the products they sell are safe and secure from the start. Without this, insecure products are likely to continue to circulate even after compliance notices, stop notices, and recall notices exposing consumers to preventable risks.

Compliance Issues and Potential Drawbacks

The bill rightly places responsibility on manufacturers to ensure that their products meet Australian security standards if they are aware (or could reasonably be expected to be aware) that their products will be sold here.

However, as a consumer, I have concerns that some manufacturers may opt to exit the Australian market rather than bear the costs and challenges of complying with these new standards. For smaller manufacturers, particularly those producing low-cost or niche smart devices, the burden of compliance may outweigh the benefits of maintaining a presence in the Australian market. This could lead to reduced availability of certain products domestically, potentially limiting choices for Australian consumers.

In response, many consumers may turn to on-shipping services to purchase products directly from overseas, bypassing Australian retailers and, unfortunately, Australian regulations. These services, which allow consumers to buy products from international markets and have them shipped to Australia via third-party intermediaries, are becoming increasingly popular. However, when consumers use these services, they unknowingly circumvent the protections provided by the bill, as manufacturers can argue they were unaware that their products were being purchased by Australian consumers. This creates a loophole where manufacturers can avoid accountability for the security of their products, undermining the effectiveness of the bill.

Furthermore, the lack of accountability means that consumers may unknowingly purchase devices that don’t meet Australian security standards, leaving them exposed to potential security vulnerabilities. This is especially concerning given that many consumers might not be fully aware of the risks associated with insecure devices or might be attracted to cheaper options available on international markets without understanding the potential privacy and security trade-offs.

To address this issue, the Federal Government must ensure that the bill accounts for the rise in on-shipping services and that mechanisms are in place to protect consumers who purchase products through these channels. One potential solution could involve greater cooperation with international regulatory bodies or creating systems that hold manufacturers accountable, regardless of how their products enter the Australian market.

Without these measures, we run the risk of creating a two-tiered system, where products purchased through Australian retailers are secure, but those bought directly from overseas may expose consumers to significant risks. The bill’s effectiveness depends not only on domestic compliance but also on addressing the increasingly global nature of e-commerce.

Ambiguities In Manufacturer Compliance

While the bill mandates security standards, it leaves room for ambiguity in how manufacturers will demonstrate compliance and how these standards will be enforced in practice. This is a critical issue, as the effectiveness of any regulation depends on clear, measurable criteria and consistent enforcement mechanisms. Without these, we risk the standards being undermined by manufacturers who may appear to comply on the surface but do not implement the meaningful security measures required to truly protect consumers.

In my experience, it can be extremely difficult to distinguish between genuine security and what is often referred to as “security theatre.” Security theatre involves practices that give the appearance of strong security but are, in reality, superficial or ineffective. For example, a device might implement a password requirement, but if it uses a weak encryption standard or defaults to simple, easily guessable passwords, it’s offering little real protection. The outward appearance of compliance can give consumers a false sense of security, making them believe their personal data is safe when, in fact, the underlying vulnerabilities remain.

The government must provide clear, detailed guidelines for how manufacturers are expected to meet these security standards. For example in 2020, California passed a law that bans default passwords in connected devices and mandates that any new device must prompt the user to create a new means of authentication before granting access to the device for the first time.

This approach forces users to change the default, often easily guessed passwords, right from the start. While a law like California’s may not be entirely appropriate for Australia, it is essential that we aim for a similar standard in our own security laws and regulations .

Without well-defined and enforceable criteria, there is a real risk that manufacturers may cut corners, focusing more on minimizing costs than on prioritizing security. This could result in products that meet the letter of the law but fail to provide adequate protection for consumers.

Moreover, I'd like to see the bill better outline how enforcement will work in practice:

- Will there be regular audits or inspections to verify compliance?
- Will manufacturers be required to have each device certified?
- If changes are made to a device’s software, at what point would a reassessment be required?

To help manage these obligations will manufacturers be able to self-certify that their products meet the standards? Relying too heavily on self-certification can be risky, as it opens the door for manufacturers to claim compliance without fully addressing the necessary security requirements. To combat this, the government could establish a certification program that requires independent, third-party verification of security measures before a product can be sold in Australia. This would provide an extra layer of accountability and ensure that manufacturers are meeting the required standards.

Another area that needs clarity is the penalties for non-compliance. While the bill mentions the use of compliance notices, stop notices, and recall notices, the specific conditions under which these penalties will be applied remain unclear. It's crucial for the bill to define what constitutes a violation and how significant security breaches will be handled, particularly in cases where manufacturers are found to have repeatedly failed to comply with the standards. Strong penalties must be in place to deter manufacturers from attempting to circumvent the rules, but these penalties need to be fair, transparent, and consistently applied.

Without clearer guidelines, there is also a risk that some manufacturers might resort to implementing bare minimum security features that technically comply with the letter of the law but fail to offer real protection. This could include measures like simply adding a password field without robust encryption or using outdated security protocols that are easy to bypass. In such cases, consumers would be left vulnerable despite the presence of so-called "compliant" devices. The government must ensure that the standards are future-proof and can adapt to the evolving threat landscape, ensuring that manufacturers continually update and strengthen their security measures as new threats emerge.

Finally, the government should consider providing support and resources for manufacturers, particularly smaller companies, to help them understand and implement the required security standards. This could include guidance materials, workshops, or technical assistance to ensure that all manufacturers—regardless of their size—are equipped to comply with the new regulations. The goal should be to foster a culture of genuine security within the industry, rather than one focused on simply meeting the minimum legal requirements.

Supporting Security Research

In my experience as a cyber security professional, I've come across unsecured devices that highlight security flaws in consumer products. However, one of the most significant challenges we face is that good faith security research—even when conducted with the goal of responsible disclosure—can lead to legal threats[3] from manufacturers. Existing anti-hacking laws are often outdated and overly broad, which raises the possibility that Good Faith Security Researchers engaging in ethical vulnerability disclosure could face legal liability.

Many manufacturers threaten litigation when faced with responsible disclosure. This stifles research that could help manufacturers improve the security of their products, and more importantly, help consumers stay safe. As a result, many security researchers are left with the difficult choice of remaining silent about vulnerabilities or facing potential legal battles.

This is where the concept of “safe harbor” becomes crucial. Safe harbor provisions offer protection from liability in certain situations, usually when certain conditions are met. In the context of security research, it means that hackers engaged in good faith security research and ethical disclosure are authorized to conduct such activities and will not be subject to legal action from the organization whose product has the vulnerability. This not only encourages transparency and collaboration between researchers and manufacturers but ultimately leads to more secure products.

While the Cyber Security Bill 2024 may not be the appropriate place to fully address the issue of vulnerability disclosure, it’s critical that the Federal Government considers how it can support security researchers as part of its long-term strategy. For this bill to succeed, the government must think about the ecosystem of security researchers who discover vulnerabilities in consumer products and report them responsibly to manufacturers—or to the government itself if manufacturers are uncooperative.

The government should also consider ways to protect Australian security researchers engaged in good faith security research from being threatened with litigation by manufacturers, especially those supplying products to the Australian market. This would help foster a safer, more transparent internet, where security researchers can collaborate with industry to reduce the number of unsecured devices, rather than being punished for trying to improve the situation.

Establishing an Ombudsman

This brings me to one of my final points. As of now, the bill does not mention the creation of a specific ombudsman to oversee the enforcement of the mandated cyber security standards. Enforcement appears to be managed through existing regulatory bodies, likely under Home Affairs or other government agencies tasked with cyber security responsibilities. The Cyber Incident Review Board, established by the bill, will play a role in reviewing incidents and providing recommendations, but it does not have the same powers or responsibilities as an ombudsman.

While establishing an ombudsman may not be a key aspect of this bill, it should be seen as a mandatory step in ensuring the effectiveness of these laws. Given the critical role that security researchers and consumers can play in identifying and reporting non-compliant devices or concerns about security vulnerabilities, there needs to be a dedicated body for overseeing these reports. Without an ombudsman, we risk having a fragmented approach to enforcement, with responsibility scattered across agencies that may not be fully equipped to handle consumer issues or respond to reports in a timely and transparent manner.

An ombudsman would provide a central and easily accessible point of contact for reporting issues, ensuring that there is clear accountability for manufacturers failing to meet security standards. This role would also serve as a crucial link between the public, the government, and the marketplace by offering transparency in how cyber security standards are being met and enforced.

Having an ombudsman in place would be essential for the purposes of reporting on the performance of manufacturers and their products. Consumers need to be able to make informed choices about the products they purchase, especially when it comes to security and privacy. An independent body that tracks and publicly reports on the compliance of manufacturers would give consumers the information they need to determine which products are secure and which pose potential risks. This transparency fosters trust in the marketplace, empowering consumers to make decisions based on clear, reliable data.

The last thing consumers need when it comes to understanding their security and privacy is ambiguous or vague information provided by a government body that doesn't typically work directly with consumer concerns. By establishing an ombudsman—or designating an existing body to take on this role—information provided to consumers could be clear, actionable, and trustworthy. This would also create a direct line of communication between consumers and regulators, ensuring that reports of non-compliance are handled effectively and that manufacturers are held accountable.

In conclusion, I believe that **Part 2—Security standards for smart devices** is a much-needed step forward in addressing the growing security risks posed by smart devices. However, as outlined in this submission, there are several areas where the bill could be strengthened to ensure its effectiveness in both protecting consumers and holding manufacturers accountable. Integrating the cyber security standards more clearly with Consumer Law, improving the recall system, and addressing the loopholes created by on-shipping services are crucial steps to making this legislation as impactful as possible.

Furthermore, ensuring that compliance is enforceable through clear guidelines and robust mechanisms is essential for preventing manufacturers from cutting corners. Supporting security researchers through safe harbour provisions and protecting them from legal threats is also critical to fostering a safer internet. Lastly, establishing or designating an ombudsman to oversee the enforcement of these security standards would provide the transparency, accountability, and consumer protection that is needed in an increasingly interconnected world.

Thank you again for the opportunity to submit my comments. I look forward to seeing how this bill evolves and how it will contribute to a safer and more secure digital landscape for all Australians.

---

1. Robot vacuum cleaners yell racial slurs, chase pets after cyber attack ↩
2. ACCC Media Release on Recalled Products ↩
3. Research Threats: Legal Threats Against Security Researchers ↩