Australian Productivity Commission's Right to Repair Inquiry ACS submission

ACS thanks the Productivity Commission for the opportunity to provide a submission to the Right to Repair inquiry and would like to advance the following comments on the Issues Paper dated 7 December 2020.

In this submission, ACS sets out the case for the following recommendations:

- Embedded software should be covered in any Australian Right to Repair
- Products included under a Right to Repair should not be limited to consumer items
- The Productivity Commission considers how intellectual property rights can be balanced against a Right of Repair

Executive Summary

Household and industrial items with embedded software is now commonplace and often essential to the functioning of products. For example, a typical modern motor vehicle contains over 150 million lines of code[1], fifteen times what would have been found in a 2010 car.

Over the same period, the number of internet connected devices, the 'Internet of Things' or IoT, is soaring. with 43 billion IOT devices estimated to be in use by 2023. In Australia, consulting firm Telsyte reported that nearly 61% of households in 2019 have at least one smarthome product[2].

Telsyte's report illustrated the broad range of applications for these devices with the fastest growing categories in 2019 being video doorbells & locks, smart outlets, smart garden devices, and smart cameras. Additionally, smart speakers, security lighting, and Energy & HVAC sensors had strong sales growth in 2020.

These connected devices do have downsides however, as described in the Issue Paper's example of John Deere tractors, proprietary software is often used to stymie competition and 'lock' consumers into a vendor's ecosystem. Also, should a manufacturer withdraw support for a device, consumers can find product functionality is impaired[3].

In this submission, we examine some of the Right to Repair issues. We would be delighted provide the Commission any support in developing its recommendations.

[1] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture

[2] https://www.telsyte.com.au/announcements/2020/10/20/iohome-gathers-pace-with-home-bound-australians

[3] https://www.theverge.com/2020/1/21/21075043/sonos-software-updates-ending-play-5-connect-zone-players

About ACS

The professional association for Australia's technology sector ACS has over 48,000 members working in business, education, government. ACS exists to create the environment and provide the opportunities for members and partners to succeed.

ACS strives for technology professionals to be recognised as drivers of innovation in our society, relevant across all sectors, and to promote the formulation of effective policies on technology and related matters. Building Australia's technological capacity is one of the three pillars of ACS' 2017-2022 Strategy[4] so the maintenance of software dependent infrastructure is a fundamental concern to the society.[5]

Software embedded consumer and industrial devices are now commonplace and are taking an increasingly important role in industry and in the lives of consumers, therefore the right to maintain and repair the code associated with these products raises issues for both business and domestic users.

Scope of Right to Repair issues

For the ICT profession, the 'Right to Repair' is an important consideration, particularly as household and industrial devices now feature extensive computing functions enhanced by the Internet of Things that sees products increasingly connected to each other and remote services.

Taking this further, the rise of Smartcity technologies and embedded industrial systems exposes industry and government alike to financial and operational risks[6] through practices like restrictive licensing, 'vendor lock-in', and planned obsolesce.

An example of the industrial 'vendor lock-in' are the software protections in John Deere agricultural equipment cited in the issues paper (pp. 15). While farmers have been vocal in their opposition to the use of embedded software and cloud services to restrict their abilities to maintain and repair essential machinery, this issue is being felt across the commercial and domestic sectors[7].

Another industry grappling with the consequences of embedded systems is the automotive industry. While the Issues Paper focused on the sector's policies around third-party spare parts and repairs, the use of 'black box' computer technologies by most automakers has restricted competition in maintenance and repair services[8].

[4] https://ia.acs.org.au/article/2020/acs--approach-to-positively-influencing-the-national-agenda.html#:~:text=The%20ACS%20Strategy%202017%2D2022,a%20conduit%20for%20sparking%20innovation).

[5] https://www.theverge.com/2020/1/13/21063596/spectrum-home-security-discontinued-service-charter-cable-cost-refund

[6] https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z

[7] https://www.computerworld.com/article/3458773/hp-inks-compensation-agreement-over-printer-cartridge-lock-in.html

[8] https://www.reuters.com/article/us-autos-selfdriving-safety-insight-idUSKBN1X919G

For broader society, today's Smartcity purchasing decisions by governments could have effects felt by consumers, businesses, and communities for decades to come as systems are deployed across towns and cities[9]. Often, the need to maintain devices and services in civic applications such as CCTV, parking systems, and infrastructure monitoring over decades may outlast the vendors that supplied the products.

ACS would therefore ask the Productivity Commission to consider the broader impact of vendors restricting access to embedded software and cloud-based services, with attention paid to competition aspects, maintenance needs and security issues.

Obsolesce and security issues

As identified in the Issues Paper, there is a distinction to be made between planned product obsolescence and the natural evolution of products due to technological change and consumer demand (pp. 19).

However, regardless of whether a product was designed to become obsolete or has been superseded by technological changes or advances, the need to update software is essential on smart devices to address security weaknesses and changing operational needs. The inability to update, or patch, software due to vendor restrictions can pose threats to household and industrial users due of the risks posed by potential security weaknesses[10].

An example of security weaknesses in embedded software is illustrated by 2014's 'Heartbleed' flaw[11] where a mistake in a commonly used encryption protocol exposed millions of websites and devices to potential hackers. Resolving this software bug required updating the affected devices, many of which were no longer supported by their suppliers[12].

Restricting the ability of home or commercial users to fix such issues in equipment could have ramifications for networks beyond individual devices simply not working such as the 2020 ransomware attack on Toll Holdings which saw the logistics giant's IT systems crippled for several weeks[13] and demonstrated the critical role technology plays in Australia's supply chains. Similar attacks since have affected most of the world's major shipping lines[14], underscoring the importance of computer code to industry.

[9] https://home.kpmg/au/en/home/insights/2019/12/smart-cities-snapshot-australia-2019.html
[10] https://home.kpmg/content/dam/kpmg/co/pdf/KPMG_Co_BTMY_TMT_Risk_or_reward.PDF
[11] https://www.vox.com/2014/6/19/18076318/heartbleed
[12] https://www.technologyreview.com/2014/04/09/74706/many-devices-will-never-be-patched-to-fix-heartbleed-bug/
[13] https://ia.acs.org.au/article/2020/mytoll-still-down-after-ransomware-attack.html
[14] https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

While the 2019 attacks on logistics companies may not have been directly related to embedded devices, they illustrate the ability to repair and patch software is essential to running modern systems and the flow on effect to business and the broader economy.

ACS would therefore ask the Productivity Commission to consider the rights of consumers and industrial users in maintaining and repairing equipment that has been deemed obsolete or superseded by suppliers.

Policy responses

The policy responses to the topic raised in the Issues Paper are broad and have implications across many areas of law, not limited to Intellectual Property fields such as the Patents Act, the Copyright Act and Designs Act, along with broader government policies and trade agreements.

ACS would be prepared to explore these topics in more detail should the Commission wish to do so during the public hearings period.

Conclusion

ACS would like to thank the Productivity Commission for raising this important issue. As products with embedded software becomes more common, the issue of repairing and maintaining computer code will become more essential to consumers, industry, and the national interest.

As the inquiry goes forward, we would welcome the opportunity to address these and other issues around the Right to Repair in more detail.