## Introduction

This inquiry response is focused on embedded software, and draws upon my experience as Computer Science graduate, Electronics Technician (radio), Computer Programmer, and free software hobbyists.

Repairing embedded software is different than maintaining physical goods, software doesn't wear, it will keep doing what its designed to do until the physical failure of the device that houses it. This demands a different approach to repairs than for physical products.

Software needs to change to remain fit-for-purpose, because;

- No software is perfect when shipped, bugs need to be repaired post-sale.
- Third party services that internet enabled devices depend on may not remain fit-for-purpose.
- Legal requirements may require changes to software.

There can be an urgency to repairs of internet enabled consumer devices post-sale, bugs can become significant threats to privacy and security of the device owner, and others internet users.

As a computer programmer I was an important contributor to the Busybox project, which is commonly used as a base for embedded software stacks, and licensed under terms that encourage repairs (the GNU Public License).

Despite my technical background and experience, its rare for me discover new consumer devices that have repairable embedded software, multiple times I have sought to use legal action to gain access to the embedded software of devices that I own, and which contains software I have licensed to the manufacturer (am both Licensee and Licensor), with only moderate success.

There is a significant power imbalance between manufacturers/suppliers and the developers of the non-commercial free software their product commonly depends on. My understanding is that there is a limited ability to claim damages in Australia from wrong doing where financial loss cannot be proven.

There is an enormous amount of time, and both financial and legal risk involved in repairing embedded software, and very limited reward.

An example of a embedded software ecosystem that I believe should be encouraged is the OpenWRT Community, which has for over a decade been providing independent firmware and facilitating repair of embedded software for many brands of modems and other devices.

The success of OpenWRT has resulted in many manufacturers basing their official firmware on OpenWRT’s work, however even products with such derived official firmware seek to discourage independent repairs.

## INFORMATION REQUEST 1

### What would a ‘right to repair’ entail in an Australian context? How should it be defined?

The ‘right to repair’ in Australian context should consider the significant role importers play in the supply chain, issues include;

- Ensuring manufacturers and suppliers respectfully honour their obligations under Australian law.
- The practical ability of consumers to pursue their rights, even over cheap consumer products.

The aim of the ‘right to repair’ should be to provide the ability of consumers to

- Ensure products remain ‘fit for purpose’ for their physical lifetime.
- Access a competitive market for repairs.
- Assess the repair-ability of a product prior to purchase.

To achieve these aims, repairers need to be able to;

- Disassemble then reassemble a product in working order
- Study and share information about the product.
- Have access to components on reasonable and non-discriminatory terms.
- Have access to information necessary to, and the right to construct compatible components.
- Have a legal right to modify the product.

**INFORMATION REQUEST 2**
**a) What types of products and repair markets should the Commission focus on?**

The commission should focus on products that have the potential to be serviced, repaired or improved post sale, and where existing markets for such repairs are not adequate.

Consumer devices with embedded software are such a product, essential repairs are made by way of irregular ‘upgrades’. Manufacturers and suppliers tightly control updates and limit repairs to essential changes in all but a few niche cases.

If embedded software could be customised new markets could emerge to extend the life of existing products

**b) Are there common characteristics that these products share (such as embedded technology and software or a high/low degree of product durability), and which characteristics would allow policy issues to be considered more broadly?**

Characteristics of software controlled consumer devices include;

- Embedded software, distributed strictly in a one-size-fits-all manner.
- Embedded software, not maintained outside warranty period.
- Embedded software, no ability for consumers to independently repair.
- Embedded software, no transparency over operation of firmware.
- Low cost, encourages repair-by-replacement.
- Low cost, discourages legal enforcement of rights by individual consumers.

A critical policy issue for Internet enabled consumer devices is the ability to repair security flaws in software over the life of the physical product, not just the warranty period.

The Internet is a dynamic environment, internet enabled devices require the ability to be modified to remain ‘fit for purpose’ within their physical lifetime.

An example of the seriousness that insecure consumer devices pose to the internet is the Mirai botnet that infected up to 600,000 consumer devices (in 2016) due to a security flaw, and was used to conduct cyberattacks.

Internet enabled consumer devices with critical vulnerabilities remain a threat to their owners and the broader internet until they become e-waste, the warranty period of the device, isn't given consideration by attackers.

Due to the proliferation of IoT devices, where anything the can be connected will be connected, this security threat will only increase.

Transparency is an issue related to security, there have been contested allegations towards one prominent device manufacturer that their devices have the potential to be made insecure. If embedded software on such devices where capable of being independently analysed it would enhance trust in its operation.

**c) If there are particular products that the Commission should focus on, what are the unique issues in those product repair markets that support such a focus?**

Product repair for software on consumer devices has many barriers.

### Non-modifiable firmware:

The ability to modify firmware is not always supported, with some devices designed to be repair-by-replacement, which reduces its potential lifespan, and limits the ability to innovate.

### Missing documentation:

Manufacturers may limit access to essential information about the device or tools needed to repair the device, such as the technical details of how firmware is loaded onto a device.

### Locked software:

Products can be locked with software to only allow ‘authorised’ repairs, method of locking include requiring passwords, or secret software tools needed to update the device.

### Legal risks:

Suppliers of products may present legal claims that may be valid in the origin country, but are not be valid in Australia, such as stickers that claim ‘warranty void if removed’. Most consumers do not have the knowledge or means to assert their legal rights.

### Intellectual Property:

Software may have licensing that forbids software components being re-distributed, or reverse engineered. If software use is tied to the sale of a hardware, and not sold separately, any Intellectual Property rights should remain with the owner of the hardware.

**INFORMATION REQUEST 3**

**a) Do the consumer guarantees under the ACL provide adequate access to repair remedies for defective goods? If not, what changes could be made to improve access to repair remedies? Are there barriers to repairing products purchased using new forms of payment technologies, such as 'buy now pay later'?**

ACL provides consumer guarantees that a product be 'fit for purpose' when sold. However due to the dynamic nature of internet and internet distributed services, a product may cease to be 'fit for purpose' post sale due to the behaviour of third parties.
e.g. A security flaw is found in a 3rd party service utilised by a consumer device, or the 3rd party service introduces undesirable licensing conditions post sale (eg monetising personal information), alternative 3rd party services may be available, but the consumer has no ability to switch to it.

Similarly ACL provides protection against 'unsafe goods', however if embedded software is not able to examined, there is no ability for consumers (or repairers) to verify if a product is safe.

ACL provides consumer guarantees around availability of 'spare parts' however it is uncertain (to me) how that applies when reproducing a firmware composed of embedded software components.

- Is software considered a 'spare part' ?
- Does the guarantee apply to new version of software ?
- How does licensing of Intellectual Property interact with this law ?
- Should the spare part be delivered as an individual software component, or as part of the original collection of software components that compose a complete firmware ?
- How would the software component be verified as a genuine 'spare part' if the manufacturer provides no way examine the firmware ?

Repair remedies would be improved by giving consumers the right to repair software embedded in consumer devices (as per my information request 1)

**b) Is the guarantee of available repair facilities and spare parts effective in providing access to repair services and parts? Or is the opt-out clause being widely used, making the guarantee ineffective?**

The guarantee of available repair facilities and spare parts is not effective in providing access to repair services and parts within the domain of embedded software.

Consumers generally have no expectation that devices (other than Phones or Computers) can have embedded software repaired (or improved), and manufacturers tightly control repairs.

Attempting to modify or improve embedded software is typically declared to void the warranty of the whole device, this and other methods to limit repair-ability are used in place of an 'opt-out' clause

There is a systemic failure of markets that undermines the repair guarantee that might apply to embedded software.

**c) Should consumer guarantees seek to balance the broader societal costs of remedy choices (such as the environmental impacts of replacements) with consumer rights, and if so how? For example, should repairs be favoured as a remedy?**

Consumer guarantees should enforce a minimum set of expectations, and encourage best practices for both the individual and broader society. Where that choice is not clear, consumers (rather than the manufacturer) should decide.

**d) Are consumers sufficiently aware of the remedies that are available to them, including the option to repair faulty products, under the ACL's consumer guarantees?**

**If not, would more information and education be a cost-effective measure to assist consumers understand and enforce guarantees? What would be the best way to deliver this information? What other measures would be more effective?**

It is difficult for consumers to comprehend remedies available to them. Products typically include legal agreements that require experts to interpret and weigh against consumer guarantees.

More information and education could be helpful, however it has to be presented in a manner that isn't open to interpretation, and applies to everywhere, with no loopholes.

Government should monitor and enforce consumer guarantees, a high probability of financial penalties would be an effective motivator for commercial distributors.

**INFORMATION REQUEST 4**

**a) The Commission is seeking information on the nature of repair markets in Australia, including detailed data on the repair markets for specific products, covering:**

**market size — by employment, revenue, number of businesses, profit margins**

**market composition — such as market share between authorised, independent and DIY repairers.**

There is presently an insignificant market for repair (or customisation) of software components on consumer devices in Australia due to lack of awareness that it is possible, and the inability to realise such repairs.

There is a potential for a market to develop for customisations of embedded software in consumer products with updated or alternative software with new features and styles.

Customised software also adds a layer of trust for the consumer as it is independent of any one service provider or manufacturer, and capable of being more transparent.

**b) Is there any evidence of a difference in quality, safety or data security between authorised repair networks and independent repairers? Are there ways to address concerns around quality, safety or data security while promoting a vibrant independent repair market?**

Firmware is commonly built from hundreds of independently developed freely distributable software components. The manufacturer will typically combine these freely distributed components with one or two proprietary components, their own branding, interface design, and configuration files.

Authorised repairers have an advantage over proprietary software components, and where specialised tools are needed to produce a usable firmware and install it. However, they have no advantage over the non-proprietary components of the firmware.

The independent repairer can have an advantage over authorised repairers in cases where there are inter-operable software components, authorised repairs will be required to conform to the official standard, independent repairers can customise the firmware to the specific needs of consumer.

OpenWRT is an example of a vibrant community of independent repairers. It provide the ability for many modems to be customised freely. The quality of their work is such that some manufacturers base their official firmware on it, but may also add proprietary components which locks out those independent repairers.

**c) Are there available examples of the contracts between OEMs and authorised repairers? Do these contracts limit effective competition in repair markets (such as by limiting the number and reach of authorised repairers or requiring authorised repairers to not be authorised by a competing brand)?**

Unknown

**What is the process to become authorised? Is it open and competitive?**

Unknown

**d) Are there specific examples or other evidence of practices by OEMs or their**

**authorised repairers that create barriers to competition in repair markets?**

Many devices do not have authorised repairers and instead repair by replacement.

**Do other factors also create barriers to competition in repair markets, such as short-sighted consumer behaviours, switching costs, poor information availability or consumer lock-in?**

Consumers are generally not aware of the potential ability to repair or customised the embedded software on a device. Even simple changes such as a customising a user interface design (different colors or styles) are not possible on most consumer devices.

The market for repairs has not evolved to beyond the minimum requirement, there is no leadership from manufacturers to foster the evolution of the embedded software their products depend on, even when its in the commercial interests to do so.

Embedded software on consumer devices should be closer to where PC software is, where anyone can write an install an application on devices they own without requiring special permission from manufacturers, suppliers or other third parties.

**e) What is the relationship between the intensity of competition in the primary product market and the risk of consumer harm from a lack of competition in repair markets?**

There is effective competition for consumer devices, however this competition has not been strong enough to promote innovation in embedded software on those devices.
There has been consumer harm in the consumer device market through a lack of innovation in embedded software, however its not possible to speculate on what benefits we have missed out on to this point because they have not evolved.

**Can competitive primary markets compensate for non-competitive repair markets?**

Competitive primary markets for consumer devices can only compensate for non-competitive repair markets in hardware.
There are non-competitive repair markets for embedded software where there are competitive primary markets, so in a practical sense it is false, competitive primary markets do not compensate for non-competitive repair markets for consumer products with embedded software.
In theory primary markets could drive competition in the embedded software of consumer devices, but I speculate that has not happened, for one, due to different industry operating models between hardware, which is best run like a manufacturing industry (design and build each product standalone); and software, which is best run like a services industry (continually evolving a product over several products).

**Is an absence of effective competition in the primary market a necessary condition for consumer harm from non-competitive repair markets?**

No, consumer harm from non-competitive repair markets for embedded software on consumer devices exist due to the high levels of control manufacturers have over their primary market, if they didnt have such control they would not be unable to artificially restrict repairs.

They choose not to compete in embedded software or their repair markets, despite possible benefits.

**To what extent would measures that enhance competition in the primary market address concerns about a lack of competition in repair markets?**

There is no repair market for most embedded software, so competition within it does not exist.

If competition in embedded software repair markets could have emerged via competition in the primary market, I expect it would have by now.

**f) Are the restrictive trade practices provisions of the CCA (such as the provisions on misuse of market power, exclusive dealing or anti-competitive contracts) sufficient to deal with any anti-competitive behaviours in repair markets?**

Laws can only change behaviour if they are enforced, the loopholes and significant barriers to bring legal action over breaches of CCA make the provisions irrelevant to any embedded software repair markets.

**g) What policy changes could be introduced if there is a need to increase competition in repair markets and improve consumer access to, and affordability of, repairs?**

Due to the differing nature between the repair of software and hardware, I feel a new area of policies need to be considered to cover the *repair of automated services* that software provides.

I do not feel I have the expertise to add any further insight.

**What are the costs and benefits of any such proposal to the community as a whole? How does it balance the rights of manufacturers and suppliers, with those of consumers and repairers?**

There is a danger that if the burden of making devices repairable was so burdensome, then some products could be withdrawn from sale.

The repair-ability of products should be mutually beneficial to consumers and the brand value of manufacturers.

**INFORMATION REQUEST 5**
**a) To what extent do current IP laws already facilitate repairs by consumers or independent third parties (e.g. the spare parts defence under the Design Act)?**

Current IP laws hinder repairs of embedded software by consumer or independent third parties.

Most firmware are built of a layer of software licensed to deliberately facilitate repairs by consumers or independent third parties. (Copyleft and Permissive licences).

Manufacturers and suppliers go out of their way to prevent consumers or independent third parties from conducting repairs, one of the ways they do so is by adding their own proprietary layer (protected by IP laws) between the repairable software and the consumer.

There is little risk that manufacturers and suppliers will be inconvenienced if caught violating IP rights of non-commercial developers.
copyright licences as it is commonplace,due to a power imbalance, and a negative risk/reward even if legal action is successful.

**b) Are there any aspects of IP laws where consumers' rights with respect to repairs are uncertain?**

There is uncertainty as to the obligation of manufacturers and suppliers to provide accurate and relevant information specific to Australian IP laws for all (sub-)components of a device.

**c) Do current IP protections (e.g. intellectual property rights, technological protection measures, end-user licensing agreements) pose a significant barrier to repair in Australia? If yes, please comment on any or all of the following:**

- **the specific IP protections that prevent consumers from sourcing competitive repairs and/or inhibit competition in repair markets**
- **the types of products or repair markets these barriers mainly affect**
- **the prevalence of these barriers**
- **the impacts of these barriers on third party repairers and consumers (e.g. financial cost, poorer quality repairs)**
- **options for reducing these barriers and their associated benefits, costs and risks (including potential impact on market offerings).**

Current IP protections do pose a significant barrier to repair in Australia.

Copyright and patent are legal tools used to prevent firmware from being repaired by non-authorised repairers.

Any consumer device containing a graphical computer interface or a network connection likely has a firmware that could be repairable, this includes (but is not limited to), Cars, Phones, TVs, Set-to-boxes, Modems and other network devices.

It is rare to find a consumer device that has repairable firmware due to IP barriers.

IP barriers impact repairs as licensing conditions can restrict re-use or reverse engineering of critical components of a firmware (eg device drivers), and the tools required to repair a firmware (eg installation tools).

Options to reduce barriers to repair could include an obligation to disclose information necessary to facilitate reverse engineering of software to install and repair firmware.

**d) In what ways might government facilitate legal access to embedded software in consumer and other goods for the purpose of repairs? What are the pros and cons of these approaches?**

The potential economic and social damage from non-repairable software in consumer and other goods should be taken seriously, and considered in the same manner as threats from the failure of physical equipment.

The government could facilitate legal access to embedded software by introducing a reliability obligation for embedded software in consumer and other goods.

Such a reliability obligation could require that a device’s software is capable of being operated in accordance with Australian laws over the useful life of the hardware.

It could further ensure transparency around its operation so third parties can verify its operations.

Such an approach would require software be up-datable to reflect changes in Australian law with regard to security, privacy and other consumer protections. It would facilitate bug fixes that effect usability, and changes to the devices operating environment, such as updating protocols, and codecs.

Transparency provision would require third parties be able to disassemble and reassemble the firmware to study and test its operation.

**INFORMATION REQUEST 6**

**a) What evidence is there of planned obsolescence in Australian product markets? Do concerns about planned obsolescence principally relate to premature failure of devices or in them being discarded still working when more attractive products enter the market?**

Planned obsolescence is evident in Australia in areas such as RSP supplied NBN modems.
A modem is provided when signing up to many service providers, effectively obsoleting a previous modem irrespective of its suitability.

**b) How can the Commission distinguish between planned product obsolescence and the natural evolution of products due to technological change and consumer demand?**

Obsolescence of a device should not happen for purely software reasons, however physical limits of the hardware may restrict the ability of software to naturally evolve.
Example1. Physical memory limitations may restrict a newer, larger firmware from being installed.
Example2. Adding support for a new video codec in software, with adequate processing capability in hardware.

Obsolescence due to natural evolution of product would be the switch from ADSL modems to VDSL. Or a streaming service requiring a new set-top box to allow the use of more efficient codecs with hardware support.

Planned obsolescence may occur when a service provider locks a customer out of their modem, preventing it being reconfigured to operate on a competitors service.
forcing new unrequested features on customers that are beyond the capabilities of e

**c) How does planned obsolescence affect repairers, consumers and the broader community in Australia?**

It increases the costs of services for consumers where newly supplied products are subsidised by services fees.
It creates e-waste.
It prevents repair markets from establishing, and evolving superior products.
As replacement products are not typically manufactured in Australia, it sends money offshore rather than local repairers.

**d) What measures do governments currently use to prevent planned obsolescence or mitigate its effects (in Australia and overseas)? How effective are these measures?**

**e) What are the benefits, costs and risks of Australia adopting measures similar to those currently used overseas, such as product design standards and rep-arability ratings?**

**f) Do consumers have access to good information about durability and rep-arability when** making purchases? If not, how could access to information be improved?

**INFORMATION REQUEST 7**

**a) What data are available on the amount of e-waste generated in Australia?**

**What data is there on the composition of e-waste in terms of particular materials (such as hazardous materials) by product type?**

**How does hazardous e-waste compare to hazardous general waste in its prevalence and risks? Is there merit in distinguishing between hazardous e-waste and non-hazardous e-waste? And if so, how could this be done in practice?**

I have no specific knowledge about e-waste

**b) What estimates are available on the costs of e-waste disposal on the environment, human health and social amenity, in Australia and internationally?**

**How do the impacts differ by disposal type, or by the type of product or hazardous material?**

No comment

**c) How much of Australia's e-waste is shipped overseas for recycling? Is there evidence of circumstances where this creates problems for recipient countries?**

**Are there barriers to the expansion of domestic recycling facilities or the adoption of new recycling technologies in Australia (such as plasma arc incinerators)?**

No comment

**d) What are Australia's current policy settings for managing the potential environmental and health effects of e-waste (such as landfill bans, the National Television and Computer Recycling Scheme or Mobile Muster)? Are these policy settings broadly right — that is, are they proportional to the impacts of e-waste on the community?**

No comment

**e) How can a right to repair policy further reduce the net costs of e-waste in Australia, and would such an approach be an effective and efficient means of addressing the costs of e-waste to the community?**

A right to repair policy can facilitate a longer useful life for consumer product by minimising , reducing the need for replacement products, and therefore reducing the amount of e-waste generated.

**INFORMATION REQUEST 8**

**a) What policy reforms or suite of policies (if any) are necessary to facilitate a 'right to repair' in Australia?**

The repair of embedded software should treated independently to the repair of the physical device that houses it.

Declare embedded software to be an 'automated service', and develop policy around the persistance or repair of these services.

Consider security flaws that emerge in embedded software to be a safety defect for the purposes of ACL, requiring a repair, recall or refund.

No time limits to liability for software defects.

**b) Are there any other barriers to repair and/or policy responses that the Commission should consider?**

The ability to assert ones rights is a significant barrier due to legal costs, and the limited resources of organisations such as the ACCC.

**c) What are the costs and the benefits of the various policy responses that have been proposed to facilitate repair (such as those outlined in table 1)?**

No comment

**d) Are there other international policy measures or proposals that the Commission should consider as part of this inquiry?**

Intellectual property rights are being used to assert control over physical property and peoples lives through data collection and dissemination, there is a huge scope creep.