Electronic Frontiers Australia Inc.
W www.efa.org.au
E email@efa.org.au
@efa_oz

Right to Repair inquiry

Productivity Commission
Locked Bag 2
Collins Street East
Melbourne Vic 8003

1 February 2021

Submitted online

Dear Commission,

RE: Right to repair

EFA welcomes the opportunity to provide comment on the right to repair inquiry.

EFA's submission is contained in the following pages.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Justin Warren
Board Member
Electronic Frontiers Australia

Introduction

EFA strongly supports a right to repair and encourages the Commission to propose legislative changes that would ensure Australians have the right to repair faulty goods, including any software they may contain.

Competitive Markets

EFA submits that a competitive secondary market enhances competition in primary markets, even in concentrated markets where consumers may have limited choice. A robust secondary market means that vendors must essentially compete with themselves; if vendors' produce new products that are not of sufficient quality and priced competitively, then consumers can choose products from the secondary market, or to repair their existing product.

A right to repair would enable consumers to make use of an inbuilt market mechanism to counter attempts at abuse of market power. This counterbalance to market power would act as a kind of *automatic stabiliser* without the need to involve market regulators to intervene if a market failure occurred.

EFA believes this is particularly important for technology products as the majority of such products are not manufactured in Australia.

Digital Rights Management

EFA is strongly opposed to the artificial constraints imposed by so-called digital rights management (DRM) technologies. Such technologies create artificial barriers unique to software products that do not exist for other, purely physical products.

While tamper-resistant product designs exist, it is rarely *illegal* to physically open such products. This is frequently not the case for DRM-locked products where the very act of bypassing the DRM technology is a crime. Consumers' right to repair for software products is already *more* constrained than it is for physical products in many cases, and vendors are increasingly abusing the greater power embedded software provides them to exert control over what consumers are permitted to do with the products they have purchased.

It seems perverse that the rights available to Australians in the physical world should not be available in the online world.

DRM Obligations

Adding DRM technologies to products is a choice vendors make because they seek certain benefits from doing so. EFA submits that this choice should also subject vendors to certain obligations.

Where DRM technologies would prevent consumers from being able to independently repair or update products purchased from vendors, such as to patch them to address recently uncovered software flaws, vendors should be required to provide free updates to the software.

If vendors do not wish to provide these update services, then DRM technologies should either not be used on their products, or the DRM should be disabled, free of charge, once the vendor is no longer prepared to provide such free updates. Consumers would then be free to repair and update their devices as they see fit.

Product Quality And Software Flaws

Computers and software are increasingly embedded into consumer products, particularly with the explosion in Internet-of-Things (IoT) devices. Software is now present in major household appliances, including televisions, fridges, ovens, barbecues, doorbells, thermostats, and lightbulbs.

Software is complex, and almost all software contains bugs or flaws that are discovered over time. The software requires regular updates to remain secure, lest malicious actors (e.g. cybercriminals) misuse these products for their own ends.[1]

Many vendors of such products cease to provide regular updates to these products, often well before these products are no longer fit for use. Consumers are therefore left unprotected, and due to the restrictions imposed by vendors on embedded software, consumers are prevented from repairing their products.

This imposes additional costs as consumers must completely replace otherwise functional goods simply because new software flaws are discovered that make their devices vulnerable to attack.

Major Failure

EFA submits that if consumers knew that a 'smart' product would no longer receive software updates for its full, useful life they would consider it to be a failure under the *Competition and Consumer Act 2010*. In some cases, this would constitute a major failure, particularly for products that are costly and durable such as televisions or fridges, and consumers would expect at least a partial refund as compensation. Such knowledge is often not available to consumers at the time of purchase. In some cases this is because vendors change their mind about the availability of software updates, in others it is because vendors

It is in vendors' own interests that consumers have access to secondary market software repairs where vendors do not wish to commit to long-term software support. Consumers may not have the necessary skills and experience to repair the software themselves, but they should be able to seek out such help from professionals, much as they do for hardware repairs on appliances or home repairs.

---

[1] Lucian Constantin, *Critical Flaws Impact Millions of Commercial and Consumer IoT Devices across Industries* ARN, https://www.arnnet.com.au/article/680599/critical-flaws-impact-millions-commercial-consumer-iot-devices-across-industries/.

Public Safety Implications

There are public safety implications to insecure software running on consumer devices connected to public networks, similar to the public health implications of infectious disease. Malware and viruses that infect one consumer's unpatched devices can and does spread to other vulnerable devices. This effect is actively exploited by cyber-criminals to create botnets that are then reused for other, often criminal, purposes.

Vendors should, therefore, be required to warrant that the software included within physical goods will be kept in good working order at least as long as the physical product can be maintained and is expected to be present and active. This presents several issues.

Vendors are not currently required to service and repair goods for their full useful life, only a 'reasonable' amount of time.[2] This amount of time is not defined in law, and major software flaws can arise at any time in a product's active life. In some cases vendors can opt out of providing repair facilities by 'advising' customers that repair facilities and spare parts will not be available after a specified time. This shifts the burden of software flaws onto the public who must bear the cost of any adverse impacts of those flaws both individually and collectively.

In many cases, the vendor for an IoT product simply goes out of business and consumers are left with a device they cannot acquire updates for, and are unable to repair.[3] Because the product still functions, consumers continue to use the product despite its vulnerability. The risk to public safety of the ever-increasing number of vulnerable IoT devices connected to public networks should not be underestimated.

A right to repair would ensure that vulnerable devices purchased by consumers can be made safe by repairing the software running on those devices, thereby reducing the threat to themselves and to others. This would not require the participation of the vendor, which may well no longer exist.

Without a right to repair, it could be argued that vendors should be held liable for the public danger posed by the software in their products due to the way it degrades over time. However, this approach provides no protection in the case where the original vendor ceases to exist, thus a right to repair is required regardless of whether or not a vendor commits to a lengthy maintenance and repair period for its products.

In fact, without a guaranteed right to repair, any vendor providing such a lengthy maintenance period for its products in good faith can be undercut by bad-faith actors who claim they will provide a lengthy repair period but who then go out of business. While it could be argued that such vendors will not garner much business in the long run, even a relatively small number of vendors producing low-cost (but low-quality) products would accumulate over time.

Malware can present an asymmetric threat such that even a relatively small number of initial infected devices can quickly grow into a substantial infection, as we have seen with the NotPetya

---

[2] *Competition and Consumer Act 2010*.
[3] "October 2018: Abandoned Tech: When IoT Devices and Solutions Get Left Behind", https://connectedworld.com/when-iot-devices-and-solutions-get-left-behind/.

and Conficker malware. Only a right to repair would ensure that devices can be patched regardless of the status of the original product vendor when a significant software flaw is discovered.

National Security Implications

The scale of computer networks and the number of deployed devices is immense, and growing. The threat posed to national infrastructure has been recognised by the Australian government[4] and we have already seen the effects of widespread malware infections such as the NotPetya[5] malware.

A right to repair would provide a mechanism for addressing the potential national security threat in a scalable, distributed fashion. It is simply not possible for any centralised agency of government to be able to actively manage the software upgrade challenge. The active participation of consumers is required.

Consumers cannot actively participate if they are prevented from doing so by vendors who make repairing their devices impossible. A right to repair therefore becomes important for preserving national security.

[4] *Protecting Critical Infrastructure and Systems of National Significance*, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems viewed 10 November 2020.
[5] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" Wired, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.