Right to Repair Submission:

As a consumer, enthusiast and developer of various technologies, I am pleased to see that the Productivity Commission has taken serious consideration of the many growing difficulties and other issues relating to peoples' increasingly limited access to repair. The report has successfully identified many key economic and environmental issues, such as the incentive towards planned obsolescence, higher cost of repair due to lack of competition, and the production of e-waste. However, there are places where the Report fails to fully address the scope of the issue. I thus present a statement on my personal perspective on these shortcomings, in the hope that any legislation this inquiry spawns will reflect not only the interests of businesses, but also consumers.

Who Owns Your Device?

While limited access to repair harms independent businesses, market competition and the environment, as laid out in the report, they also have much greater implications on the future of consumer rights and a person's control over their own purchased property. The current barriers to Repair implicate the basic concept of device ownership, as the various mechanisms identified in the report serve to limit user control over their own devices. If the manufacturer retains control over a device after it has been sold, the customer's control is implicitly limited. This is especially egregious when dealing with mechanisms designed to limit access to the inner workings of a device.[1] These access control mechanisms cause a *de facto* transfer of authority over the device to the manufacturer, rather than the owner.

As such, the single most important change which Right to Repair legislation must make is to cement the rights of the customer over a purchased device. The device does not belong to the manufacturer, it belongs to the customer. The locks do not belong to the manufacturer, they belong to the customer. The keys do not rightly belong to the manufacturer, they rightly belong to the customer. Simply allowing them to be purchased is insufficient so long as the manufacturer retains a monopoly on the distribution of these keys, as such would allow them to charge an arbitrarily high price, the law must recognise that it is the customer's device, and as such any keys (or other tools used for access control), whether they are physical or digital in nature, are part of the product and must be turned over to the customer on sale.

1. Examples include: proprietary screw heads for which only the manufacturer may produce drivers; serialised electronic components which require secret calibration tools to pair to a device; and software locks which prevent a customer from replacing or modifying the software preinstalled on a device.

Fostering Technology through a Culture of Engineers

Another underappreciated aspect related to Right to Repair, is the associated Right to Tinker. Modern technology is built on the backs of curious minds, people who as teenagers would disassemble the hardware they used in everyday life, so they could learn how it worked, find alternative uses for the technology, and ultimately go on to develop their own technology. This sentiment has been echoed both by supporters of Right to Repair[1], and even its staunch opponents. Many modern technology behemoths were built on the backs of this access, revolutionising the modern world and tearing down the technology monopolists of their own time, yet now find themselves doing everything in their power to limit this access and secure lifelong control over every device they sell.

1. Steve Wozniak, founding engineer of Apple, has recently spoken out in support of Right to Repair, even going so far as to say "we wouldn't have had an Apple if I had not grown up in a very open technology world."[*https://youtu.be/CN1djPMooVY*]

The Walled Garden Business Model

A key issue with the modern lack of user control over devices is not simply lack of access to alternative repair, but lack of access to alternatives in general. A Walled Garden Business Model, utilised by companies such as Apple, Epson, or Nintendo, is one in which the manufacturer retains effectively complete control over devices beyond their sale by restricting users from installing alternative software, such as digital stores, alternative operating systems, or independently sourced applications developed for the device. If the manufacturer wishes to offer a specialised store with certified software that they have filtered through to remove any non-functional or malicious software, and warn users when they choose to install uncertified software, this is not an issue. However, the user must retain the ability to take on such risks for themselves, lest the device lose all functionality once developer support for the device has ended. The garden may have a wall, but it must also have a gate. A manufacturer may certify, but only the user may authorise.

Security in an Open Technology World

A key complaint offered by opponents to Right to Repair is that it puts users at risk if anybody can access the internals of these devices. However, there is a simple solution to this, which is to decentralise authorisation and access control. Security measures such as component serialisation can be done in a decentralised manner, by forcing the device to display warnings about modified components until the user inputs a security key to confirm that any modifications were properly authorised by the owner.

The Myriad Harms of Digital Rights Management

While the report recognised some of the barriers that DRM (Digital Rights Management) poses to consumer and independent access to repair, it failed to recognise the broader harms that DRM causes in the technology sector, including both software[1] and hardware[2] incompatibility, market distortion due to industry collaboration[3], unfair limitations on legitimate use of copyrighted works[4], and even security risks[5]. Laws against bypassing these measures, even absent any actual infringement on intellectual property, effectively prohibit any and all tinkering with technology used to read, transmit, store or display media without some particular grant of legal protection. And even if an exemption is issues for one type of circumvention, this rarely suffices to allow consumers to exercise these rights due to the prohibition on production or distribution of tools for this purpose.

[1] *Many programs or media, such as specialised apps, video games, music or movies, can be run on third party devices by use of emulators or similar software, allowing customers to use a purchased piece of software or media beyond the lifespan of the original hardware, adapting it for modern use. Similarly, many devices can also be modified to run specialised software, giving them a use beyond that of the original software.*

[2] *HDCP (High-Bandwidth Digital Content Protection) is a hardware DRM technology used in audiovisual technologies. In order for HDCP protected content to play, the entire signal chain, including source, speaker and display, must all be certified for the correct version of the protocol. As playback devices must all be updated every time the protocol is changed, even if they are physically capable of carrying the signal otherwise. For example, early "4K" high-resolution televisions used the HDCP 2.1 standard, but by the time "4K" content started to be produced, the HDCP 2.2 standard had been adopted, which would refuse to play on displays using the older standard, or even if the signal was simply routed through a signal-switcher or AV Receiver, causing these devices worth many thousands of dollars to become unusable for their primary purpose.*

[3] *Most DRM standards, such as Intel's HDCP or Google's Widevine, are secret, proprietary technologies yet are required for compatibility with much of the media or software standards out there today. By managing these standards, potential competitors are forced to pay to license the technology under restrictive terms, and ordinary users are compelled to use only products approved by these organisations or face massive incompatibility.*

[4] *Use of copyrighted works is permissible for certain purposes, such as critique or parody, yet DRM prevents such people from producing their own excerpts of the work, forcing them to rely on the very people they are critiquing for access to the necessary materials. It also interferes with creating software backups, transferring files to a different format, and can even outlast the copyright term itself, indefinitely blocking material from the public domain.*

[5] *As these technologies are all secret, legally protected and generally demand a secrecy even from the end user, it is impossible for independent researchers or security-minded individuals to verify the safety of these technologies, creating the potential for harm, as with "StarForce" copy-protection on certain video games circa 2005, which was revealed to have malware like characteristics that could damage a user's computer.*

By Sean O'Farrell