RE: Right to Repair

Right to Repair represents a defining challenge of the modern digital world. Whereas one can service a car at home, take it to a local mechanic, or to the genuine dealer; the same cannot be said for most digital products. In part, the complexity and miniaturisation of modern digital electronics represents a significant impediment to most consumers being able to repair such devices, and thus is subsequently exploited by manufacturers as evidence of why a consumer "should not" repair such devices. Most often, this comes across as "planned obsolescence" in the eyes of a consumer like me (and may in fact be the case, such as when a vendor releases a new product). Arguments are often thrown around by the vendor, stating "Intellectual Property", "Security" or "Safety Concerns"; whereas in most cases, this is simply not true had the consumer been able to access documentation, parts, and tools to service such devices themselves. **The net result of this is an erosion of ownership of a product a consumer has rightfully purchased, since we are beholden to the vendors' interests as to whether such a device can be repaired or supported officially, thus in effect, making all consumers a "subscriber" of even a physical product in their possession.** As an ICT Security Professional, "maker", consumer, husband, and father; Right to Repair falls close to my heart for several reasons that I will outline in the following paragraphs.

As an ICT Security Professional of more than 12 years, I have seen the evolution of computers from restrictive "proprietary" devices, such as early IBM hardware, the popularity of "brand name" workstations and laptops provided by the likes of Apple, Dell, and HP, to modern computing platforms in everything from cars to watches and cloud computing. The security implications of such a connected world are real, and very alarming to people like me who are tasked with protecting people in ways they may never know. But what strikes me and angers me at the same time, is the likes of Apple or Tesla suggesting that allowing consumers or independent repairers the ability to fix a product they rightfully own, as somehow being a "security risk" in some way. Consider a padlock - a physical security mechanism, but as a physical object it is bound to the laws of physics. A vendor may try as they can to "protect" a consumer from copying or reverse engineering the internals, but it simply cannot be done. It is possible to identify the workings and determine how the security works or even fix/modify it with the right skills (i.e., "lock-sports"). Software is no different, but simply exists in a different domain. To function, the software must at some point be accessible to the consumer, so despite mechanisms such as encryption and obfuscation; with the right skills it is possible to reverse engineer (i.e., "analyst" or "malware researcher") the software and observe the inner workings. With electronic hardware, there exists further protections that due to the microscopic size and complexity of such technology, that there is no easy way to reverse engineer in some cases. This latter approach is where Apple, Samsung and Tesla are working towards through "pairing" of components in devices, ensuring "authentication" and passing this off as "security". The consequence of this, however, is that any change to a faulty device breaks the overall product functionality, as it is either not possible to obtain a genuine replacement part (e.g., a pre-programmed EEPROM, such as the Apple Mac SMC), or not possible to "pair" the components without access to the correct password, encryption keys or tools (e.g., consider the John Deer repair case, or the Apple Mac SMC chip). It can be argued these mechanisms indeed represent solid security that can help protect consumer data, but as physical hardware that can be "shipped", with approaches such as encryption keys and online connectivity; it is readily possible for hardware to be replaced with appropriate guidance and pre-programmed hardware supplied directly by the vendor. The security argument is often raised by vendors against the Right to Repair movement, but from an

ICT professional perspective; the argument lacks solid ground in which to stand, as established methods to handle such scenarios are widely used and readily accepted in the ICT industry today.

I personally own several computers that I have built myself. I own pre-built equipment (e.g., printers, routers, switches, NAS devices and laptops). I also own numerous “Internet-of-Things” devices such as Arduino and Raspberry Pi. I use this equipment for my own purposes, including learning about the world around me, such as monitoring air quality, temperatures, particle counts and such through both code and hardware solutions. I also write complex multi-tier software in virtualised environments. This is what I do as a “maker”. There are also very few obstructions to me purchasing a CPU, mainboard, RAM, case, power supply, water cooling parts and graphics cards and putting them together how I please for significantly less cost than a pre-built system. I can also upgrade parts as I see fit, and through standardisation – the resulting system is both high performance and secure. The Arduino foundation achieved something similar at commercial scale with ARM Cortex and Atmel processors in creating their wide range of devices, opening the world to the ability to innovate and configure a multitude of devices however they say fit. In many ways, the maker community represents a “sharing” community of Open-Source proponents, hoping to further civilisation through widespread innovation whilst giving access to those who do not have the means to pay for proprietary equipment and software. It is a fantastic educational experience for children, students, and adults alike. This is the opposite from the proprietary approach chosen by vendors such as Apple and Tesla, who choose to lock down and even punish those who try to change/repair things (e.g., Tesla supercharging capability being disabled after a non-Tesla repair). Proprietary approaches may be necessary in some elements of a device such as a car for safety reasons, but the reality is; whether a car is digitally controlled through an electric motor or analogue controlled by a throttle on the air intake – the resulting behaviour of the device is identical and thus calls to question; if the device could be repaired to original specifications, or allow modification to within known tolerances; why should it not be allowed? This is no different from modifying a car to increase performance to use in racing or rallies. Human ingenuity will always find a workaround for any restriction, and this remains true in trying to “lock down” something against modification or repair, calling into question the need for restrictions in the first place.

As a consumer nothing is more frustrating than having to return a faulty device under warranty or get something repaired and being left with nothing for the entire duration of shipping overseas and back for a “genuine” fix. Even more frustrating, is when the “fix” costs more than a new device or results in total loss of data. Again, this is more often the case with Apple devices as official repairers rarely provide board-level repair services, and thus will instead quote entire new boards (which includes CPU, memory, SSD, and graphics) at often near-cost to a new device. Adding to the frustration is that such repairs will often result in a total loss of all data on the device. By contrast, Microsoft is an example of a business innovating, whilst increasingly committing to the Open-Source world. Microsoft has also committed to improving repairability of their Surface notebooks/tablets. On the other end of the spectrum, Apple devices are increasingly becoming less repairable by increasing the usage of proprietary hardware, restricting access to interfaces necessary to diagnose faults, and creating poor quality hardware (e.g., non-existent waterproofing of Mac Books), whilst charging a major premium for the “privilege”. This is by no means intended to be “Apple Bashing”, it is simply a statement of fact. One only needs to look at the thousands of videos produced by the likes of Louis Rossman of Rossman Repair Group in New York or Jessa Jones of iPad Rehab to see the proof of this, or the various news reports of Apple “Genius Bar” price gouging on simple faults that

an independent repairer could fix for just a few dollars that could have avoided total data loss. There is absolutely no justification for such behaviour, as it is against consumer rights everywhere and represents bad social license. On this exact point, it is near impossible to upgrade any part of a Mac Book and in modern devices, it is not even possible to recover the data if a major component such as the Apple SMC fails, since neither independent repairers OR genuine repairers can obtain the replacement component that “pairs” with the soldered-on solid-state-drive (SSD) encryption key, thus a consumer will lose all their data unnecessarily and permanently if they accidentally spill water on their Mac Book or the chip fails for some other reason. Some components, such as batteries or high-voltage electrics (e.g., in a Tesla) are indeed extremely dangerous, if mistreated, but I would argue are MORE dangerous to the consumer attempting a repair with a lack of documentation from the vendor. If as a consumer, I am clearly explained through detailed guidance how to do something safely, I will follow that advice clearly and probably learn a lot from the experience too. For this reason, the argument by vendors that “safety” is an issue that warrants them withholding repair documentation fails as an argument, since withholding such information in fact increases the risk to the consumer (I suggest this argument is more about liability to the vendor, since providing documentation puts liability for damage on the vendor, rather than the consumer). Knowledge is power, and accurate information helps make better decisions.

Finally, as a father and husband, I do not have endless resources to spend on new devices every time something breaks. Neither do I want every faulty device to simply become e-waste, because a vendor simply needs a marketing or shareholder reason to release a new product to the market. Most devices I tend to keep going until either they no longer can meet my requirements (e.g., capacity, performance, or compatibility), or they fail (e.g., battery lifespan, broken components). I have a young daughter who I want to have a world she can enjoy, where consumers are not simply treated as walking wallets to big business and genuine innovation needs to occur to make a sale. We are already seeing the consequences of consumerism across the world, resulting in major divides between the rich and poor, global warming and resource depletion. This generation owes it to the many future generations to come to stop wastage and greed resulting from discarded goods.

For humans to continue to thrive, the Right to Repair argument represents a basis to enablement. Commitment to the initiative requires long-term vision, real solutions that can adapt to changing situations, collaboration, and above all, respect. As it stands, vendors and shareholders carry little (if any) respect for the consumer other than as a source of profit. Consumers willingly accept gouging and forceful upgrades because they are conditioned to this behaviour by the vendors. This does not represent respect, it does not respect collaboration, resources or present a viable sustainable future for anyone. If we continue to allow things as they are, innovation will suffer, resources continue to be wasted, and our rights as consumers continue to erode. Whilst only a small part of the bigger picture, the Right to Repair initiative could not be more important to the future of Australia, and indeed, the world.