Before the
United States Copyright Office
Library of Congress

In the matter of

Section 1201 Study:
Request for Additional Comment

Docket 2015-0012

Comments of
The Repair Association and iFixit

Submitted on behalf of
The Repair Association and iFixit by

Luis Villa
Law Office of Luis Villa
luis@lu.is
(415) 938-4552
October 27, 2016

Table of Contents

Introduction

About The Repair Association

The Repair Association, formerly known as the Digital Right to Repair Coalition, is a 501(c)6 trade association founded in July of 2013 to support individuals and businesses engaged in repair, reuse, and recycling of digital electronic parts and products. Our members range in size from individual hobbyists to multinational repair and services providers, and include consumer rights organizations, sustainability advocates, agricultural organizations, flexible labor networks, equipment trading networks, and logistical services networks.

The Repair Association has advised state governments on right to repair laws based on the 2012 Massachusetts Automotive Right to Repair law.[1] This bill provided a clear path for state legislative action, and also served as the foundation of major national voluntary agreements adopted by automotive[2] and commercial vehicle[3] manufacturers. The success of this approach strongly suggests that commercial interests and consumer repair are complementary values that can both be served when policy and legislative approaches are well-drafted.

About iFixit

iFixit.com is an international, open-source, online repair manual for everything. Our mission is to provide people with the knowledge they need to make their things work for as long as possible.

iFixit represents a global community of makers, tinkerers, fixers, and repair professionals. In 2015, the iFixit community taught repair to over 80 million people from almost every country in the world. The strongly collaborative group has published over 20,000 repair guides. This massive, free resource has helped people fix everything from

1 "An Act protecting motor vehicle owners and small businesses in repairing motor vehicles", Massachusetts Session Law of 2012, Chapter 368, *available at* https://malegislature.gov/Laws/SessionLaws/Acts/2012/Chapter368.

2 Memorandum of Understanding, January 14, 2014, *available at* http://www.nastf.org/files/public/OtherReference/MOU_SIGNED_1_15_14.pdf.

3 Memorandum of Understanding, *available at* http://www.nastf.org/files/public/OtherReference/HD-MOU_2015.pdf.

cellphones to game consoles, toys to musical instruments. iFixit also stands firm in its support of the tinkerers and independent repair professionals in our community. We believe that owners should have the right to repair, modify, and tinker with the things that they own.

Role of 1201 and software in modern repair

The Repair Association and iFixit thank the Copyright Office for this opportunity to comment on the impact of Section 1201 on the ability of American consumers and businesses to repair the things they own.

We write in part to remind the Copyright Office that "software is eating the world".[4] Since the DMCA was passed, we've gone from a world where software is rarely seen outside of a general-purpose computer, to a world where billions of microprocessors are embedded every year in virtually every type of device. Essentially all categories of manufactured products now contain software that is central to the functionality of the product, from lightbulbs to toothbrushes. As a result, software has also become central to the repair of devices.

Manufacturers are, unfortunately, taking this opportunity to prevent users from repairing or modifying the devices they have bought, from tractors[5] to printers[6] to coffee cups.[7] They are also invoking the DMCA to justify and protect these anti-consumer behaviors.

This sea change in the reach of software, coupled with the abuse of the DMCA by manufacturers, has unintentionally made the Copyright Office a central regulator of American consumers' and businesses' right to repair the things that they own. States,

4 "Why Software Is Eating The World", Marc Andreesen, *Wall Street Journal*, Aug. 20, 2011, *available at* http://www.wsj.com/articles/SB10001424053111903480904576512250915629460; discussed more recently in *"Software is Still Eating the World"*, Techcrunch, June 7, 2016, *available at* https://techcrunch.com/2016/06/07/software-is-eating-the-world-5-years-later/.

5 "We Can't Let John Deere Destroy the Very Idea of Ownership", Kyle Wiens, *Wired*, Apr. 21, 2015, *available at* https://www.wired.com/2015/04/dmca-ownership-john-deere/.

6 "HP Inc Backtracks On Its Controversial Printer Lockdown", David Meyer, *Fortune*, Sep. 29, 2016, *available at* http://fortune.com/2016/09/29/hp-printer-ink/.

7 "How the Internet of Things Limits Consumer Choice", Bruce Schneier, *The Atlantic*, Dec. 24, 2015, *available at* http://www.theatlantic.com/technology/archive/2015/12/internet-of-things-philips-hue-lightbulbs/421884/.

courts, and other regulatory bodies can support a right to repair, but since firmware protected by technological measures is intimately involved in the operation of most new devices, the DMCA (and Copyright Office policy) can preempt the work of policy makers and markets.

The Office recently acknowledged these problems with repair of land-based motor vehicles, but did not extend the same perspective to other equipment. (Existing exemptions, for example, would allow consumers to repair internet-connected refrigerators—but not extend the same consideration to commercial refrigerators.) We respond to this notice of inquiry with hopes that the Copyright Office will refocus on copyright, and restore the questions of repair policy to the policymakers, businesses, and consumers best positioned to answer them.

The Unlocking Technology Act of 2015

Most of the concerns raised below could be remedied by amending Section 1201 to make clear that neither circumvention of a technological measure, nor the development and distribution of circumvention devices, is unlawful unless those acts are done for the purpose of infringing copyright. The current approach to addressing this—an ever-growing series of exceptions—fails to account for either new technological changes or age-old concepts like fair use and property ownership.

The Unlocking Technology Act of 2015 (H.R. 1587) is, potentially, a straightforward and consistent way to update the law and meet many of these goals. Passing this act would make clear that reuse and repair of Americans' devices are not a violation of copyright law, while leaving in place other statutory and judicial regimes that appropriately limit such behaviors. As such, we believe it could be an excellent first step towards addressing most of the issues raised below. However, in the spirit of constructive engagement, we also offer more targeted alternatives below.

1. New Permanent Exemptions

1.a. Assistive Technologies

We believe that all electronics should be open to use and modification by the owner or by third parties at the request of the owner. Consistent with this position, we support the right of book purchasers to make legal use of the copyrighted material they have

purchased. As a result, we strongly support permanent exemptions for all assistive technologies.

When evaluating the question of accessibility more broadly, we note that as currently drafted this exemption concerns access to the "core" subject of copyright—creative materials like books and videos. This contrasts with most manufactured goods, where technological protection of embedded software is used primarily to control and enable hardware functionality. For example, one of The Repair Association's supporters in Massachusetts is confined to a motorized wheelchair whose software was not appropriate to his level of disability. By modifying the software, he was able to improve his directional control, and join us at the State House in Boston to deliver testimony in favor of the Massachusetts Digital Right to Repair bill. This modification did not implicate or threaten the creative concerns that are at the core of copyright, but nevertheless could have been blocked by Section 1201.

When revising this exemption, the Copyright Office must keep the distinction between functional and creative works in mind, and ensure that a new exemption protecting the right to access books and movies does not accidentally block functionally-focused software modifications that improve accessibility for Americans with other forms of disability.

1.b. Device Unlocking

In keeping with the observation that "software is eating everything", the number of devices that rely on data networks for core functionality continues to grow every day. (For example, during the internet outage of October 21st, 2016, some people reported being unable to set their internet-connected thermostats!) As a result of this trend, repairing network connectivity is becoming an important part of repairing older devices. We therefore strongly support permanent exemptions for unlocking of mobile and other networked devices.

Unfortunately, the language of the existing exemption is too specific. Instead, we recommend that *all* network-attached equipment be exempted permanently, without qualification, allowing owners of devices to switch their devices to other networks or future communications technologies and protocols.

If the Office does not create a general exemption for all device unlocking, we foresee problems both for The Repair Association and iFixit's members, and for the Office itself.

For our members, and American consumers more generally, the problems of being unable to change and repair network connections will be vast and will continue to grow. Without the flexibility to unlock or adjust settings to permit movement between networks, millions of products (not just the mobile phones currently covered by the exception) will simply stop working as networks and network services change. These devices will eventually become waste, unless their owners are allowed to move them to new networks when the owner has new needs.

More subtly, in an age of remote diagnostics, directing diagnostic data output from one network to another is critical to competition for repair services. As a result, the ability to change networks and connectivity is key to ensuring that independent repair organizations can continue to fix devices on behalf of their owners. Because of this, the Massachusetts Right to Repair law ensures that remote diagnostics must be available to independents. If this exemption is not made more broad, efforts like this one at the state level will be easily thwarted by technological measures and Section 1201.

Network unlocking also allows tinkerers and innovators to explore new ways to offer improved products to the consumers and businesses who have purchased them. For example, we have spoken with is a company that provides farmers with advanced data services, and would like to be able to save farmers money and use data more efficiently by interfacing directly with the networks already embedded into tractors. A broad network unlocking exemption (still tied to an infringement nexus) would allow such experimentation, for the benefit of American business, without increasing copyright concerns.

Finally, past the pragmatic problems for consumers, the Copyright Office should also seek a broad exemption to avoid a literally never-ending stream of requests for new exemptions. The current approach, requiring regular applications for exemption of every new class of device, invites uncertainty for those trying to repair devices and permanently injects the Copyright Office into technology policy in a way that is not supported by the text of the statute.

1.c. Computer Programs

General approach

We admire the Copyright Office's openness to exploring the question of "facilitat[ing] users' ability to engage in permissible uses of software". However, we must stress that

the question is much broader than that: because software will be embedded in essentially everything, this question is really about facilitating users' ability to engage in permissible uses of *all of the devices* they buy, from tractors to light bulbs, and everything in between. Any analysis that treats this question as simply one of software avoids the broader context of the use of software in the modern world. Without consistent legal access to this embedded software, repairs, subsequent reuse, and secondary markets for legally-purchased manufactured products are impaired, and will be increasingly impaired as software continues to "eat everything".

"specific formulations"

The Office invited comment on "specific formulations" of "an exemption that would permit legitimate activities such as the repair of automobiles or the use of third-party device components" "for purposes of diagnosis, maintenance and repair".

We welcome the Office's reference to policies created by the judiciary (like *Aro*) and the states, such as the right-to-repair laws that we have supported. However, given the diversity of potential approaches to repair in the age of the Internet of Things, and the likelihood that the best approach will change rapidly in coming years, we believe that the Copyright Office should not look to specific pre-existing language when drafting an exemption. Instead, an exemption for "diagnosis, maintenance, and repair" should be drafted very broadly, giving more appropriate entities (like states, judges, the market, and the Federal Trade Commission) maximum latitude to regulate without having to also negotiate the vagaries of Section 1201.[8]

In brief, we suggest that the best approach is a general exemption for circumvention done without a nexus to infringement.[9] This is consistent with how courts have interpreted the statute,[10] and would have a strong positive effect on all legitimate activities, including those for repair and modification. Alternately, as previously

8 For discussion of why the Office should defer to other entities and focus on copyright to the exclusion of other policy areas, we refer to the extensive discussion in Sec. 2 of the Electronic Frontier Foundation's earlier comments ("Section 1201 Claims Should Not Be Used To Address Public Policy or Legal Concerns Outside of Copyright, and Non-Copyright Concerns Should Never Be Grounds for Denying or Narrowing an Exemption", p. 4-8), available at https://www.regulations.gov/document?D=COLC-2015-0012-0058.

9 For a detailed version of this proposal, *see* id. at 4.

10 *See Lexmark Int'l, Inc. v. Static Control Components, Inc.,* 387 F.3d 522, 547-48 (6th Cir. 2004).

suggested, we believe that the language of the Unlocking Technology Act would have a similarly positive effect.

"consumer activities"

The Office further asked if an exemption would "adequately address users' concerns regarding ... 1201's impact on consumer activities". As we have stressed in past comments on Section 1201, the problem here is not merely a *consumer* problem—just as software-enabled consumer automobiles presaged software-enabled commercial tractors, software-enabled home thermostats are also presaging software-enabled commercial thermostats, and so on and so forth. As a result, commercial organizations, from family farms to government agencies, are also impacted. Any regulatory action by the Copyright Office, or proposed legislation, must take these uses into account as well.

Considering the needs of businesses as well as consumers again suggests that a broad exception, covering all uses *except* those specifically impacting copyrighted works, is the correct approach. The broad proposals we support above would protect these business and government uses.

"lawful modification of a computer program"

The Office has asked for comment on whether an exemption "for purposes of engaging in any lawful modification of a computer program" should be considered. For the same reasons given in the previous section, we would strongly support such an exception. With computer software providing key parts of the functionality of many devices bought by American consumers and businesses, repair and improvement of those devices will depend on their ability to modify software, just as they currently have the ability to modify hardware they've purchased.

However, the limitation to "lawful" modification is problematic. As ably detailed by briefs in earlier comments on Section 1201,[11] when Congress has made a particular action unlawful, such as modifications to engine control software that would impact emissions, then the Copyright Office should defer to those statutory and regulatory schemes.

We do not feel that this broader formulation would be likely to result in economically harmful unauthorized uses of copyrighted works. Very little embedded software is sold

11 *See*, e.g., Electronic Frontier Foundation comments, available at https://www.regulations.gov/document?D=COLC-2015-0012-0058.

independently of the hardware in which it is embedded, so allowing users to modify software would not impact the market for those goods.

The Office's suggested mitigation ("conditioning the exemption on ... not engaging in any unauthorized use of a copyrighted work") is unnecessary - if the use is not authorized, then the standard statutory and contractual penalties for infringement (and the standard defenses, such as fair use) should be the primary tools used to combat the unauthorized use.

1.d. Obsolete Technologies

We of course support the Office's interest in extending and broadening consumers' and businesses' ability to continue repairing and using older devices. It is important, however, to note that many such devices are not "faulty", so we have some concern about the framing of the question. Manufacturers of devices that contain embedded software often *deliberately* choose to abandon maintenance of such software, and the DMCA currently helps prohibit users from fixing the devices themselves. This has huge repercussions, not just for maintenance, but also security.

For example, many smartphone manufacturers use technical protection measures to lock the bootloaders of phones, so that users cannot upgrade the software to new versions, and then stop updating the software, leaving devices that are only 18 months old but a security hazard for their users.[12] Similarly, Chinese camera manufacturers who have not updated their software may have been partially responsible for the massive internet outage that occurred while these comments were being drafted.[13]

Because this "abandonware" is the most common class of older device today, any new permanent exemption that seeks to address this problem must cover both "faulty" software as well as software for which manufacturer no longer provides updates.

2. Existing Permanent Exemptions

As a general matter, we support making exemptions permanent. The current process requires vast efforts every three years, which is difficult for small organizations like

12 "Want a Secure Android Phone? Get an Unlocked Phone", *PC Magazine*, March 15, 2016, available at http://www.pcmag.com/commentary/342915/want-a-secure-android-phone-get-an-unlocked-phone.

13 "Chinese firm admits its hacked products were behind Friday's massive DDOS attack", *IT World*, Oct. 23, 2016, available at http://www.itworld.com/article/3134038/.

independent repair providers. If anything, all trends in the embedded software marketplace strongly indicate that such exemptions will become more necessary, not less necessary, so requiring that organizations show proof of that over and over again is a waste of the resources of all parties involved.

2.a. Security research exemption

The security research exemption should be made permanent. However, because security is now a factor for all internet-connected devices, the limitations on which devices qualify for the exemption must be removed.

For example, the distributed denial of service attack that took down large portions of the internet on Oct. 21, 2016 was likely powered by in part by hacked digital-video-recorder software embedded in closed-circuit TV cameras sold to businesses. These cameras posed a significant threat to the national infrastructure, but research on them would not have been protected by the 2015 exemption, because they do not appear to have been primarily "consumer" devices.[14] This serves as a strong reminder that *all* devices with embedded software, not just those covered by the narrow exemptions in the 2015 rulemaking, are now security threats.

In response, we would urge the Copyright Office and the Congress to make this exemption permanent, while expanding it to cover any goods which contain a computer program. If such steps are not taken, researchers will continue to be prevented from improving security for businesses, governments, and any other purchaser of software-enabled products, and repair organizations will be unable to help their customers by improving the security of older devices.

As with other points discussed in our comment, we also believe the exemption should not be limited to "lawful" or "good faith" research. Other statutes, like the Computer Fraud and Abuse Act, not the Copyright Act, should be used to assess and (where necessary) punish such activities. For more details on the reasoning behind this, please see earlier comments, including those from the Electronic Frontier Foundation.

14 *Id.*; *see also* "Over 500,000 IoT Devices Vulnerable to Mirai Botnet", Security Week, Oct. 7, 2016 (indicating that video surveillance products from Dahua Technology, a maker of closed-circuit security cameras for businesses, may have been the largest vector for the attack), available at http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet.

2.b. Authorization requirement

We believe that the owner of any property should have unfettered control over how their property is repaired or modified, including the option to hire any party to assist them. In addition, security of software is becoming of increasing importance, as the software more and more devices can be used to eavesdrop on the communications of individuals and businesses. As a result, we believe that security testing (like that contemplated in Section 1201(j)) should obviously be permitted when requested by consumers or businesses that own a device.

However, given the broad scope of claims made by manufacturers of devices with embedded software about the ownership of underlying software, we feel that it is important that the statute be clarified to ensure that manufacturers cannot block users from doing their own testing. For example, a significant security flaw in Nissan software was discovered by someone testing their own car.[15] This is clearly in keeping with the policy goals of Section 1201, but given that General Motors has claimed to own the software in a car,[16] it is not implausible to imagine that manufacturers would claim a violation has occurred. This would be a disastrous policy outcome.

The courts have, to date, mostly rejected this approach. As the court in *Chamberlain* put it, "the DMCA emphatically *did not* 'fundamentally alter' the legal landscape governing the reasonable expectations of consumers or competitors" (emphasis in the original),[17] so that buyers of a product still have a clear property right in the things that they have legally purchased. However, it should not require extensive litigation to make clear that purchasing a product gives you basic property rights to do things like repair and modify the thing you've bought.

15 "Nissan disables its Leaf remote control app", *Engadget*, Feb. 24, 2016, *available at* https://www.engadget.com/2016/02/24/nissan-leafs-connected-climate-control-has-a-security-flaw/ (summary); for a more detailed account of the computer-security student who tested their own Nissan Leaf, see the original account by Troy Hunt, *available at* https://www.troyhunt.com/controlling-vehicle-features-of-nissan/.

16 *See* "Proponents Have Failed to Demonstrate That Vehicle Owners "Own" the Computer Programs in Vehicles", in *Comments of General Motors LLC*, March 27, 2015, *available at* http://copyright.gov/1201/2015/comments-032715/class%2021/General_Motors_Class21_1201_2014.pdf.

17 *Chamberlain Group v. Skylink Tech., Inc.*, 381 F. 3d 1178, 1194 (Fed. Cir. 2004).

Similarly, hardware leases for things like tractors typically grant lessees control of property under their contracts, leaving users in control of matters of repair and reuse. This same control should be extended to those who seek to perform security testing on devices which they have a long-term lease on.

With these two use-cases in mind, we suggest revising 1201(j)(1) to read:

> the term "security testing" means accessing a device containing software, computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner, lessee, or operator of such device, computer, computer system, or computer network.

2.c. The two-factor framework of subsection (j)

The factors in 17 USC 1201(j)(3) are not exclusive, and so their impact is somewhat muted. Nevertheless, it is important to note that (particularly for older devices, or for devices where the manufacturer obtained software from a foreign provider) the ability of security testers to contact manufacturers may be limited. As such, 17 USC 1201(j)(3)(A) could be construed against security testers in common repair situations, such as when working on older cars or phones.

We recommend either breaking up (A) into two clauses, with the second clause focused on *good faith* attempts to share information with the developer of the software; or removing (j)(3) altogether (as proposed by the Breaking Down Barriers to Innovation Act of 2015).

2.e. Interoperability

Many of the Repair Association and iFixit's members regularly engage in the business of making older systems work with one another outside of the original intentions of their manufacturers — the oldest and purest form of "interoperability" work. Our members also improve systems over time, by installing and modifying peripherals and aftermarket parts into existing systems. And of course, as providers of tools and services, they do this not only for themselves, but for others.

As such, the ambiguity of 1201(f) on the question of circumvention after the initial analysis is troubling. In particular, it implies a vision of interoperability where all interoperability is a one-off, custom act, and where no markets can be built for services or parts. For example, tractor Engine Control Units can be salvaged from one model of

tractor to another, but require reflashing with new software, which may required specialized tools and knowledge. Prohibiting tools that allow such reuse of salvaged parts would be antithetical to how the American repair industry has functioned for many decades, to settled expectations of American consumers and businesses, and to the goals of legislation like the state-level Right to Repair act passed by Massachusetts.

We endorse the language proposed in the Breaking Down Barriers to Innovation Act to improve subsection (f). These changes would clearly allow repair professionals to experiment, build new systems, and distribute them to the many Americans who would like to keep their older tools and systems working alongside new ones.

3. Anti-Trafficking Provisions

Background

In a world where software is embedded in everything, any policy that prohibits businesses from developing products and services that repair and modify software is a policy that prohibits the repair of most manufactured products. This is particularly true when manufacturers of many classes of goods have so little economic incentive to fix their old products that they often don't even give themselves the ability to deliver new software. As leading security expert Bruce Schneier put it, for many classes of devices, "the only way for you to update the firmware … is to throw it away and buy a new one".[18] As Schneier and other industry analysts have noted, "the sellers of those devices don't care" about security — not out of malign intent, but because their business model does not make it profitable to issue new software for older hardware.

If we are to avoid a world where throwing out old literally billions of old devices is the only way to address security problems, the anti-trafficking provisions must be interpreted so that individuals and businesses who have purchased older devices can discover, share, and sell the fixes to these problems, rather than doing reinventing the security wheel over and over again.

18 "We Need to Save the Internet from the Internet of Things", Bruce Schneier, *Motherboard*, Oct. 6, 2016, *available at* https://motherboard.vice.com/read/we-need-to-save-the-internet-from-the-internet-of-things.

Analysis of 1201(a)

We agree with the Electronic Frontier Foundation and others that Sec. 1201(a) should be interpreted so as not to bar the creation of tools for repair of devices that contain embedded software protected by technological measures. The gist of the analysis in the EFF's comments on the vehicle exception rulemaking[19] is correct, and applicable across most tools that allow repair of devices that contain embedded software.

For example, a security researcher has used their expertise to build software tools that allow older "smart" lightbulbs to be controlled by a newer smart home "hub". They then make the code for these tools available to the public, so that anyone can use these otherwise obsolete bulbs more useful. If this person could not distribute their tools, it seems unlikely that most owners of these bulbs would be able to replicate the work on their own.

Luckily, as in EFF's analysis of vehicle repair services, it seems quite likely that this person's tools fall outside of the scope of 1201(a)(2). The primary purpose of the tools is to control existing devices, not to circumvent technological measures, so (a)(2)(A) does not apply. Similarly, the tool has a "significant purpose or use" other than circumvention, so (a)(2)(B) does not apply. And this person's tools are not "marketed" for use in circumvention, except as such circumvention is necessary for the purposes of interoperability with other, newer devices, so (a)(2)(C) does not apply.

This interpretation of the DMCA is in keeping with the policy goals of copyright, which must seek to balance the rights of authors and technological progress. As the Supreme Court reminded us in *Sony*[20], "if a *significant* portion of the product's use is *noninfringing*" (emphasis in original), the product's manufacturer is not a contributory infringer. Similarly, 1201(a)(2) should be interpreted to strike a similar balance.

19 Electronic Frontier Foundation, Comments In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201, Class 21, at 25, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class21.pdf

20 *Sony Corp. of America v. Universal City Studios, Inc.*, 464 US 417, 491 (1984).

Unfortunately, the Register's position[21] that tools that "may" violate 1201(a)(2) cannot be permitted suggests that this issue is not as clear as it should be. To avoid future confusion, and to avoid a proliferation of abandoned lightbulbs (as well as tractors, cars, and virtually every other class of manufactured product), we recommend that the statute be amended.

The language of the Unlocking Technology Act could be one basis for such an amendment. Perhaps inspired by *Sony*, it makes clear that tools "primarily designed or produced to facilitate noninfringing uses"

3.a. Personal use

Section 1201(a)(2) does not prohibit creation of tools for one's own use, where an exemption applies. Even where the creation of a tool is not permitted by the analysis given in the previous section, the phrase "or otherwise traffic" in 1201(a)(2) clearly indicates that "manufacture" should be interpreted as large-scale production for the purposes of *trafficking* to the public, not mere creation of a tool for personal use.

Beyond the language of 1201(a)(2) itself, it would be incoherent for Section 1201 to include an extensive list of permitted behaviors (such as the interoperability exemption), but prohibit the creation of the tools necessary to actually perform such behaviors.

3.b. Services

As discussed above, most repair services should not be interpreted to violate Section 1201(a)(2) or (b)(1) — their primary purpose is to repair and improve the functionality of products that include software; circumvention is merely a mechanism by which this broader purpose must sometimes be achieved.

21 Section 1201 Rulemaking, Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights at 246-47 (Oct. 8, 2015), *available at* http://copyright.gov/1201/2015/registers--recommendation.pdf.

Conclusion

As software has come to be embedded in everything, Section 1201 has come to have a direct bearing on the right of every American, including both consumers and businesses, to repair and modify the devices they have purchased. The current exemptions and exemption process have served mostly to show that the process is extremely broken, and for Americans to regain the right to repair their devices, it must be broadly reformed.

Respectfully submitted-

Gay Gordon-Byrne

Executive Director, The Repair Association

Kyle Wiens,

CEO, iFixit