8-2023

Repair As Research: How Copyright Impedes Learning About Devices

Anthony D. Rosborough

Aaron Perzanowski

REPAIR AS RESEARCH
HOW COPYRIGHT IMPEDES LEARNING ABOUT DEVICES

Anthony D Rosborough[1] *& Aaron Perzanowski*[2]

ABSTRACT

Widespread computerization and ubiquitous smart devices have enabled software-based copyright governance to reach into new domains. Beyond their instrumental utility, these devices are also containers of vast amounts of information in the form of software and technical know-how. Through copyright and anti-circumvention rules, however, this information can be cordoned off and confined to exclusive distribution channels. This can have a significant impact on research. While copyright law traditionally conceives research as the use of expressive works within institutional settings, this paper proposes a broader conceptualization that includes device research, including informal inquiries and DIY activities. Whether for the purposes of modification, repair, user innovation, or testing, device research involves the analytical engagement with physical devices. With a particular focus on repair-related activities as a modality of device research, this paper refers to product teardowns, reverse engineering, security research, and testing analyses. It then looks to case studies that exemplify the ways in which copyright can impede this type of research. In highlighting the conceptual overlap between the Right to Repair and Right to Research movements, the authors propose that a broader concept of research in copyright that includes device research could normatively reinforce and bolster support for a Right to Research in international copyright law.

[1] Doctoral Researcher, European University Institute. anthony.rosborough@eui.eu.

[2] Thomas W. Lacchia Professor of Law, University of Michigan. aperzano@umich.edu.

For their thoughtful comments on our presentation of the ideas in this paper, we owe thanks to Carys J Craig and Thomas Margoni. We are also thankful for Willie Cade's timely assistance and responses to some of our more technical questions. Overall, we are very thankful for being included in the Program on Information Justice and Intellectual Property's Right to Research in International Copyright Law project at the American University's Washington College of Law.

INTRODUCTION

Balancing the interests of rightsholders and the public is both a principal aim and recurring struggle for copyright law.[3] As the WIPO Copyright Treaty (WCT) recognizes, the rights of authors must be weighed against the broader public interest, particularly with respect to "education, research and access to information."[4] This recognition draws upon general principles articulated in the Berne Convention and parallels more specific provisions in national copyright laws.[5] Despite the longstanding inclusion of "research" as a pillar of the public interest, the concept often lacks precise definition throughout various international agreements and domestic laws. Broadly, copyright law conceives of "research" as the use of copyright materials for the purpose of gaining knowledge or understanding.[6] Over time, that concept has expanded

[3] It has been argued that "balance" in this respect serves as a statement of purpose, providing the basic structure for interpreting statutory provisions to define their meaning and purpose. See, e.g., Abraham Drassinhower, "From Distribution to Dialogue: Remarks on the Concept of Balance in Copyright Law" (2009) 34:4 J Corp L 991-1008 at 993.

[4] World Intellectual Property Organization Copyright Treaty, 20 December 1996, 2186 UNTS 38542 (entered into force 6 March 2002), Preamble [WCT], Preamble.

[5] The copyright "balance" referred to in the WCT is derived from the principles contained in Articles 2*bis*(2), 9(2), 10, and 10*bis* of the **Berne Convention** for the Protection of Literary and Artistic Works (adopted 14 July 1967, entered into force 29 January 1970) 828 **UNTS** 221. *See also* 17 U.S.C. § 107 (noting teaching, scholarship, and research as archetypal fair uses); R.S., 1985, c. C-42, s. 29 (describing research, private study, and education as examples of fair dealing).

[6] In the US Copyright Act, "research" shows up in section 107's preamble, 108's discussion of libraries, 111's discussion of television market research, and then in 1201's discussion of the criteria for exemptions, the 1201(d) library exception, and 1201(g)'s

from access to and reproduction of traditional scholarly works to embrace new research techniques, such as text and data mining (TDM).[7] In almost all cases, however, "research" as a copyright concept centres around access, collection, and reuse of text-based research inputs. As a result, copyright's characterization of "research" is often unnecessarily limited to activities carried out within a narrow range of institutional settings such as libraries, universities, museums, and archives.

But research takes place in many other domains and modalities, embodying distinct subjects, purposes, and methodologies.[8] Interacting with text, images, and sound is crucial to many forms of research. Likewise, research sometimes entails engagement with physical devices and digital code to understand their design and functionality. These inquiries may involve product teardowns, reverse engineering, or other device testing analyses. This sort of research can yield, among other insights, new mechanical processes and technical solutions that remedy faults or improve performance. As will be shown, although they have other applications, these practices are part and parcel of many repair processes. These activities draw upon existing research fields in the engineering or materials science disciplines, but in this paper we join them together under the common banner of "device research." In practice, device research can range significantly in formality; from institutionalized research and development (R&D) to the home tinkering and DIY repair.

Historically, copyright law had little need to account for device research or related repair activities. The operation of mechanical and electronic devices was the exclusive province of patent law, which has its own set of doctrines to address research and repair. But with copyright law's uneasy embrace of software, the once clear delineation separating functional devices from expressive works has grown increasingly blurry and permeable. Many modern devices are fundamentally dependent on software code for their basic operation. Just as copyright can restrict access to and dissemination of text-based research, it can also now hamper device research. Accessing diagnostic information, analyzing embedded software code, and bypassing technological protection measures (TPMs) all implicate copyright law, which

---

encryption research provision.

[7] Chrstophe Geiger et al., "Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?" (2018) 49 *IIC - International Review of Intellectual Property and Competition Law* 814-844 at 817.

[8] For example, the National Science Foundation (NSF) classifies research into three categories: basic research, applied research, and developmental research. Basic research is systematic studies directed toward greater knowledge or understanding of the fundamental aspects of phenomena. Applied research is systematic studies to gain knowledge or understanding necessary to determine how a recognized and specific need may be met. Finally, developmental research is systematic uses of knowledge or understanding gained from research directed toward the production of useful materials, devices, systems, or methods, including the design and development of prototypes and processes. https://www.nsf.gov/statistics/randdef/rd-definitions.pdf

in turn plays a significant and sometimes determinative role in the legality and feasibility of device research.

With the foregoing in mind, this paper examines the right to research in copyright law as it applies to device research. There are many different motivations for device research. They include improving, modifying and testing existing products, developing new ones, as well as repair and maintenance. Of these motivations, this paper focuses primarily on repair-related device research, but also includes adjacent activities like diagnosis, testing, and modification. Our primary contention is that, insofar as copyright law implicates device functionality, its concept of "research" must expand accordingly. Such an expansion could reveal and solidify the significant overlap between the right to research and the right to repair movements. Both movements call for a more flexible and balanced approach to intellectual property law that can enable innovation, experimentation, and discovery. And both challenge efforts to use copyright law to limit access to information. They differ only in the type of information being sought. Whereas the traditional notion of copyright research interprets information embedded in expressive works, device research interprets information embedded in functional products. The aim of this paper, therefore, is to outline how copyright law limits device research, with a particular emphasis on repair, and why copyright's notion of research ought to embrace device research practices.

Part I looks at the concept of research within copyright law. We contend that the traditional institutionalized notion of research is in need of reinterpretation in order to capture the broader range of research activities that contemporary copyright law regulates. In Part II we develop more fully the concept of device research and show its connection to experimental repair practices. Drawing upon information and media studies literature, we break down these practices into three phases (diagnosis, implementation, and reporting). In the process, we reveal the many ways in which common repair practices involve inductive and deductive inquiry, often leading to new solutions or improvements. In Part III we then briefly explore how copyright can impede device research during each of these three phases, paying particular attention to technological protection measures (TPM). Finally, in Part IV we explore several case studies that illustrate the intertwined relationship between research and repair.

I. COPYRIGHT'S CONCEPTION OF "RESEARCH"

Within copyright law, "research" is often construed broadly but ambiguously. The public interest in facilitating research is reflected in articles 10(2) and 9(2) of the Berne Convention, but largely left undefined.[9] Given

[9] Jorg Reinbothe & Silke von Lewinski, The WIPO Treaties 1996: The WIPO Copyright Treaty and The WIPO Performances and Phonograms Treaty Commentary and Legal Analysis (Tottel Publishing, 2002), 54-55.

the enormous range and diversity of fields in which research takes place, leaving a wide margin for interpretation of the concept is warranted.[10] Nevertheless, in analyzing a selection of prominent legal instruments addressing copyright, the meaning of "research" appears to vary along two dimensions. The first is the degree to which research is referred to as a general activity, or instead limited to areas of specialization and disciplinary focus. The second is the degree to which research is characterized as a formal, expertise-driven process that occurs within particular institutional settings, or whether it includes informal research undertaken by individuals outside of those institutions. Much of the academic literature focusing on intersections between intellectual property and "research" adheres to a quite narrow and institutional conception[11], but the literature focusing on the copyright implications of software and reverse engineering is generally more inclusive of informal or research processes.[12]

Along the general/specific axis, the WCT and the Marrakesh Treaty both include very broad and open notions of research, with no further specificity or guiding criteria. In both agreements, research appears alongside "education", and "access to information" as one of three manifestations of the public interest. Notably, in *Marrakesh*'s preamble, the general "opportunity to conduct research" is characterized as a blanket positive right. Likewise, the U.S. Copyright Act identifies research as a paradigmatic example of fair use without defining the term or otherwise narrowing its scope.[13]

But not all copyright provisions addressing research are so open-ended. A prominent subset of research referred to in EU copyright law is "scientific research".[14] Both the EU's Database Directive and Digital Single Market

[10] In fact, the Berne Convention Working Group in charge of exceptions and limitations made the conscious decision *not* to specify an exception for works 'having a scientific character' on account of 'the expansion of the field of science'. See, e.g., Sam Ricketson & Jane Ginsburg, *International Copyright and Neighbouring Rights: The Berne Convention and Beyond*, 3rd ed (OUP, 2022) at 783.

[11] See e.g., Christophe Geiger & Bernd Justin Jutte, "Conceptualizing a 'Right to Research' and Its Implications for Copyright Law: An International and European Perspective" (7-2022) Joint PIJIP/TLS Research Paper Series (no 77) at 54 where the authors describe the benefits of a mandatory research exception under EU copyright law given that Europe is "boasting an active research industry, with some of the largest pharmaceutical manufacturers in the world, and some of the most important producers of technologies that will be indispensable for a European and global move towards a more sustainable future."

[12] Pamela Samuelson & Suzanne Scotchmer, "The Law and Economics of Reverse Engineering" (2002) 111:7 *The Yale Law Journal* 1575-1663 at 1649-1653.

[13] *See* 17. U.S.C. § 107. In practice, the leading fair use cases dealing with research focus on the use of text-based expressive works. See, e.g., Williams & Wilkins Co. v. United States, 487 F.2d 1345 (Ct. Cl. 1973); Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1995). But see Sega Ents. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992).

[14] See, e.g., Christophe Geiger & Bernd Justin Jutte, "Conceptualizing a 'Right to Research' and Its Implications for Copyright Law: An International and European Perspective" (7-2022) Joint PIJIP/TLS Research Paper Series at 54, where the authors reason that "scientific research" may not include industrial research or applied research.

(DSM) Directive clarify that scientific research "should be understood to cover both the natural sciences and the human sciences".[15] This implies that exceptions and limitations for these purposes should extend to the study of physical phenomena. In the EU's Information Society Directive, use of copyright works "for the sole purpose of illustration for teaching or scientific research" is also a non-mandatory exception to the rights of reproduction and communication to the public. Another less familiar example is the "commercial advertising market research" exception under United States law that permits the alteration of commercial advertisements in secondary television transmissions for research purposes.[16]

With the introduction of anticircumvention regimes, we've seen explicit recognition of some domain-specific forms of research. For example, "encryption research" is a common basis for exceptions or limitations found in legislation around the world.[17] The United States Copyright Act defines encryption research as "activities necessary to identify and analyze faults and vulnerabilities of encryption technologies applied to copyright works, if these activities are conducted to advance the state of knowledge in the field of encryption technology…".[18] This definition bears a strong resemblance to the European Union's (EU) "research into cryptography" referenced by the Information Society Directive as an activity that should be safeguarded from TPM overreach.[19]

Taken together, these examples reveal a largely fluid and malleable concept of research within copyright law, but one that has been supplemented by more domain-specific definitions in response to legislative expansion of copyright's practical scope.

Copyright law's concept of research also ranges in its orientation toward either formal or informal settings. On the institutionalized end of this spectrum are frameworks that regard research as principally taking place within libraries, archives, or museums.[20] In other instances, research is construed as "scholarly" or "by researchers at institutions of higher education." This view is featured strongly in the EU's DSM Directive, where TDM research is envisioned as being carried out within "universities and

---

[15] Database Directive, recital 36; Digital Single Market Directive, recital 12.

[16] s 111(c)(3).

[17] See, e.g., Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the Information Society [*InfoSoc Directive*], Art 6(4), Australia Copyright Act, s 116A(2)-(7), Canadian Copyright Act, s 30.62. In addition, the DMCA's security testing exception is addressed to the act of "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability." 17 U.S.C. § 1201(j).

[18] s 1201(g)(1)(A). Despite the generality of this exception, subsection 1201(g)(3) lists weighing factors for determining whether it may apply to in certain cases, including "whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology…"

[19] InfoSoc Directive, Recital 42.

[20] See, e.g., Canada *Copyright Act*, s 29, 30.2(1)-(2), 30.21(3.1)(b).

other research organisations".[21] The exception created by the DSM Directive permits TDM research for "universities and other research organisations", among other entities. It defines "research organisations" as including universities, libraries, and hospitals; with their common denominator being that they act "on a not-for-profit basis or in the context of a public-interest mission recognised by the State".[22] These examples reveal a strongly institutionalized notion of research that takes place primarily within the confines of public institutions.[23]

Under U.S. copyright law, the fair use doctrine appears indifferent to institutional setting, at least on its face.[24] In practice, however, the leading fair use cases concerning research are situated in formal settings. In *Williams & Wilkins*, the court determined that the National Institutes of Health, the federal government's "principal medical research organization," was engaged in fair use when it photocopied scientific articles "to assist [researchers] in their on-going projects [or] … simply for background reading."[25] Decades later, the Second Circuit reached the opposite conclusion when it considered Texaco's practice of photocopying of scientific journal articles.[26] Notably, the court pointed out that it's analysis did "not deal with the question of copying by an individual, for personal use in research," holding open the possibility that such uses "might well not constitute an infringement." And finally, the Ninth Circuit held Accolade was engaged in fair use when it copied Sega's video games in order to reverse engineer their functional requirements and "create[] a development manual" to produce compatible games.[27]

Rather than reflecting any preference for formal research settings, the prevalence of formalized research in the fair use cases likely reflects some selection biases in the sorts of disputes that courts are asked to resolve. As Pam Samuelson has suggested, "One possible explanation for the paucity of such cases may be that copying for learning-related purposes is often done in private, noncommercial settings. This makes detection of infringement difficult. The costs of enforcement or of attempting to license many of these uses would be far greater than the economic returns likely to result."[28]

But in other instances "research" explicitly includes activities outside of

---

[21] Digital Single Market Directive, recital 8.

[22] Digital Single Market Directive, recital 12.

[23] The U.S. DMCA's does not require that encryption research takes place in a formalized setting but does consider whether a defendant is "engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology." 17 U.S.C. 1201(g).

[24] The statutory factors do favor nonprofit educational actors over commercial ones. 17 U.S.C. § 107(1). But the statute does not explicitly favor informal settings over formal ones.

[25] Williams & Wilkins Co. v. United States, 487 F.2d 1345, 1347 (Ct. Cl. 1973), aff'd, 420 U.S. 376, 95 S. Ct. 1344, 43 L. Ed. 2d 264 (1975)

[26] Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 916 (2d Cir. 1994)

[27] Sega Ents. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992).

[28] Pamela Samuelson, *Unbundling Fair Uses*, 77 Fordham L. Rev. 2537, 2582-83 (2009).

institutionalized settings. This may be partially attributed to the fact that "research" is often listed as a separate and distinct activity from the more institutional uses like "teaching" and "scholarship".[29] This autonomous characterization is consistent with both the WCT and Marrakesh, which clearly separate research from education and access to information.

Courts have also interpreted "research" as including independent and informal activities. For example, in interpreting the meaning of research for fair dealing purposes, Canada's Supreme Court has taken the view that the concept:

"...can include many activities that do not demand the establishment of new facts or conclusions. It can be piecemeal, informal, exploratory, or confirmatory. It can in fact be undertaken for no purpose except personal interest. It is true that research can be for the purpose of reaching new conclusions, but this should be seen as only one, not the primary component of the definitional framework."[30]

This holistic view is shared by Geiger & Jutte in their working paper on Conceptualizing a Right to Research in copyright law:

"The right to research should not be limited to a particular institutional context [or] to a specific professional background. To put it simply, not only university professors conduct research, but also non-academic researchers, commercial enterprises and even private individuals, alone or collectively… [R]esearch-enabling copyright rules should not distinguish in their general application between public and private or commercial and non-commercial users."[31]

Informal research carried out by 'private individuals' or for 'personal interest' is reflected most strongly in copyright's exceptions and limitations involving computer-related research. These are security research and related exceptions for the most part. For example, broad language in the EU's Computer Programs Directive appears to permit informal research in its exceptions for "black box" analysis: "...a person having a right to use a computer program should not be prevented from performing acts necessary to observe, study or test the functioning of the program".[32] Though this language was primarily intended to encourage competition between

[29] See, e.g., United States Title 17 at s 107, where teaching, scholarship, and research are treated as distinct purposes. See also s 108(a)(2)(ii), allowing reproduction by libraries and archives where collections are available "not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field…"

[30] Society of Composers, Authors and Music Publishers of Canada v Bell Canada, 2012 SCC 36 at 22.

[31] Christophe Geiger & Bernd Justin Jutte, "Conceptualizing a 'Right to Research' and Its Implications for Copyright Law: An International and European Perspective" (7-2022) Joint PIJIP/TLS Research Paper Series (no 77) at 44.

[32] Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs [*Computer Programs Directive*].

commercial software developers, the wording implies that end-users in informal settings can also be beneficiaries of this exception.[33] And though the word "research" is not specifically used, 'observation, study, and testing' are practically indistinguishable.

In a similar vein, the United States' Librarian of Congress (LoC) has granted a series of exemptions permitting TPM circumvention for "good-faith testing, investigating, or correcting" of security flaws and "good-faith security research" dating back to 2006.[34] That initial exemption has been renewed or expanded on several occasions, most recently in 2021.[35] In 2015, the LoC noted that exemption proponents stressed the importance of "independent" security research. Based on concerns from manufacturers that security research could present dangers to individuals or the public, the LoC defined "good-faith security research" as being carried out "in a controlled environment designed to avoid any harm to individuals or the public…"[36] Despite the notion of a controlled environment, the LoC omitted any reference to formal research institutions or organizations. The result is a good-faith security research exemption that is largely inclusive of informal research activities.

What emerges is not a consistent, unified notion of research, but rather a broad—if somewhat amorphous—concept left largely undefined with the exception of some domain-specific instances governed by comparatively precise statutory terms. Whether open-ended or narrowly-tailored, these notions of "research" also range in their degree of formality and institutionalization. General and open-ended research exceptions and limitations mostly apply regardless of formality or institutionalization, whereas exceptions targeted at certain types of research are sometimes limited to particular institutional settings. Within this relatively malleable framework, we support a broad and purposive interpretation of "research", particularly as it applies to new areas of copyright governance as facilitated by technological advance. Our view is that a meaningful Right to Research should embrace not only the analysis of expressive works, but all forms of research across the natural and social sciences.[37] With this in mind, the following section investigates device research practices with an emphasis on those related to experimental repairs.

---

[33] Alan K Palmer & Thomas C Vinje, "The EC Directive on the Legal Protection of Computer Software: New Law Governing Software Development" (1992) 2:65 Duke Journal of Comparative & International Law 65-87 at 78-79.

[34] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006).

[35] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 86 Fed. Reg. 59,627 (Oct. 28, 2021).

[36] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Effective Date, 80 Fed. Reg. 65,944 (Oct. 28, 2015)..

[37] See, e.g., United Nations Educational, Scientific and Cultural Organization (UNESCO). 1997. *Recommendation Concerning the Status of Higher Education Teaching Personnel.*

II. REPAIR AS RESEARCH

Repair practices touch upon nearly every object and environment in our world. Public infrastructure, personal property, and even the human body are all scenes of repair.[38] The content of these practices can be greatly influenced by the various social, technical, and ethnographic settings in which they are carried out.[39] Despite this diversity, we can think of repair in two distinct ways when viewed at the general level: routine repair and experimental repair.

Routine repairs follow established procedures and processes toward a known result. These activities typically rely on conventional inputs like published documentation, assembly diagrams, and replacement part distribution chains. An example of routine repair is fixing a bicycle's flat tire. This involves initially testing the tube to see if it can hold air at the appropriate pressure and verifying that the valve stem is functioning properly. If the tube is the culprit, the repairer must then remove the wheel, separate the tire from the rim, and remove the tube. If the tube's hole is small enough it may be patched. Otherwise, the repairer then must replace the tube (ensuring that it is not kinked) and reassemble.[40] These repair practices follow a series of known conventions that have been refined and rehearsed millions of times by people around the world. Sometimes routine repairs are handled by specialists or experts. In other cases, individual consumers can take them on independently.[41]

But if one looks back far enough, it is likely that all routine repairs were at one point the subject of research and experimentation. This approach becomes necessary where known procedures or solutions are either inapplicable or inadequate, warranting some experimentation. The path to successfully completing the repair may not be obvious for a few reasons. For one, it could be that the cause for breakdown or malfunction is not immediately apparent or readily ascertainable.[42] This scenario is common in the case of complex or computerized devices. Second, repair through conventional processes and procedures may not align with time or financial

---

[38] Roselyne Min, "This tiny robot could 3D print inside your body to make repairs and fight cancer" (9 April 2023) *Euronews.net*, online: https://www.euronews.com/next/2023/04/09/this-tiny-robot-could-3d-print-inside-your-body-to-make-repairs-and-fight-cancer

[39] For example, ethnographic research into the repair of medical devices in hospitals shows the impacts of the institutional and organizational structures of hospitals on ways in which repair and maintenance is understood and carried out. See, e.g., Cornelius Schubert, "Repair Work as Inquiry and Improvisation: The Curious Case of Medical Practice" in I Strebel el al (eds) *Repair Work Ethnographies* (Palgrave MacMillan, 2019) 31-60.

[40] Ikaika Cox & Christopher M Osborne, "How to Replace a Bike Tube" (22 September 2019) *WikiHow*, online: https://www.wikihow.com/Replace-a-Bike-Tube

[41] Jérôme Denis & David Pontille, "Beyond breakdown: exploring regimes of maintenance" (2017) 6:1 *Continent* 13-17 at 15.

[42] Stephen Graham and Nigel Thrift, "Out of Order: Understanding Repair and Maintenance" (2007) 24:3 Theory, Culture & Society 1-25 at 4.

constraints, necessitating a workaround or an alternative approach. Finally, conventional repair may not be possible because of its reliance on inputs that are unavailable or inaccessible. These could be specialized knowledge or expertise, or compatible spare parts, specialized tools, or diagnostic or technical information that is unavailable, particularly where access is restricted by the manufacturer.[43]

In these latter scenarios repair often takes the shape of an experiment. It is a form of situated inquiry and discovery, albeit largely out of necessity. Theorists in the Information Studies field posit that the situated inquiry approach to repair is what enables it to move from an inconspicuous and out-of-sight activity governed by expertise to a form of conspicuous, active, and participatory engagement.[44] It involves the application of human ingenuity and analysis where the procedures, techniques, and outcomes are not known in advance. It is often guided by improvisation, fault-finding, and testing. Experimental repair is relatively common in the case of computerized device repair, where the path to complete repairs can more often be without standardization or precedent.[45] Experimental repair can involve a number of different techniques and approaches that depend on the object or device in need of repair, including repetition, changes in technique or tools, bypasses, workarounds, trial and error, as well as fabricating entirely new and custom tools, equipment, or replacement parts.[46]

Experimental repair involves deductive and inductive reasoning at three discernable stages.[47] The first is the *diagnosis* stage. This involves identifying the problem with the device or object and determining what needs to be fixed. The methodologies employed at this first stage might include diagnostic testing, troubleshooting, or reverse engineering with the end goal of assessment.[48] The second stage is the *implementation* stage. This involves actually fixing the problem through the application of technique and often entails trial and error. *Reporting* is the final stage of experimental repair. By

---

[43] See, e.g., Lara Houston, Steven J. Jackson, Daniela K. Rosner, Syed Ishtiaque Ahmed, Meg Young & Laewoo Kang, *Values in Repair*, Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems 1403 (2016) (describing the practice of "looping," in which Ugandan mobile-phone repairers use thin copper wires to connect device components to the motherboard in the absence of infra-red soldering stations).

[44] Thomas Lee & Rachael Wakefield-Rann, "Conspicuous and inconspicuous repair: A framework for situating repair in relation to consumer practices and design research" (2021) 294:126310 *Journal of Cleaner Production* 1-2 at 2.

[45] Stephen Graham & Nigel Thrift, "Out of Order: Understanding Repair and Maintenance" (2007) 24(3) *Theory, Culture & Society* 1-25 at 4.

[46] Matthew Rimmer, "The Right to Repair: Patent Law and 3D Printing in Australia" (2023) 20:1 *scripted* 130-202 at 182.

[47] Steven J Jackson & Lara Houston, "The Poetics and Political Economy of Repair", in Jeremy Swartz and Janet Wasko, eds, *Media: A Transdisciplinary Inquiry* (Intellect Books, 2021) at 250.

[48] Özçelik, Ayşegül, "Encountering the inner face of products: Computer repair practice and amateur computer repairers" (Masters Thesis, August 2018), online: https://open.metu.edu.tr/bitstream/handle/11511/69293/12625642.pdf at 119.

documenting the repair process and the techniques applied, the information generated by the repairer can be shared with others. This can be facilitated through participatory repair activities like repair cafes, written repair guides, or DIY tutorials that can be shared widely over the internet. Over time, reporting can help to transform experimental repairs into routine ones.

In practice, not all experimental repair activities conform neatly to these three stages.[49] But this categorization serves as a useful framework for understanding these conceptually distinct inquiries. It also more readily reveals the value of experimental repair as not merely an instrumental means to an end, but also in producing new knowledge and understanding. These benefits are often realized irrespective of whether a given repair is successful, as even negative results can produce new knowledge or understanding of a device's design and function.

While our primary focus is repair, these same activities can foster related interventions informed by device research. Diagnosis, implementation, and reporting can also be leveraged in product modification. Rather than simply returning a device to its original state, or a near approximation of it, modification alters or improves performance in some respect. Modification, in turn, is closely related to user innovation—the process by which users develop ancillary parts or products that build off of existing devices.[50] In his book Working Knowledge, Douglas Harper describes Willie, a skilled and experienced small-town mechanic. After performing countless repairs of Saab door handles, Willie designed an improved version, replacing weak components with a stronger metal alloy and eliminating a problematic plastic ball bearing.[51] Similarly, early twentieth century farmers repurposed Model Ts to power their agricultural tools.[52] In other instances, the skill and knowledge gained through device research can lead to entirely new devices. The Wright brothers, before their famous foray into aviation, ran a bicycle repair shop in Dayton, Ohio where they became familiar with the sprocket drive train they later incorporated into the first airplane.[53] While not a direct outgrowth of their bike shop, the

[49] For example, in some instances, reverse engineering may take place at both the diagnosis and implementation stages where the development of new parts, components, or software is required in order to complete an experimental repair.

[50] User innovation, where the latter activities are often classified using four stages: "need recognition", "idea formulation", "development", and "diffusion". Eric von Hippel, "The Dominant Role of Users in the Scientific Instrument Innovation Process" (1976) 5 Research Policy 212-239. *See also* Christopher A Voss, "The Role of Users in the Development of Application Software" (1985) 2:2 Journal of Product Innovation Management 113-121 at 114

[51] Douglas Harper, Working Knowledge: Skill and Community in a Small Shop 62 (1987).

[52] Kathleen Franz, Tinkering: Consumers Reinvent the Early Automobile (2011).

[53] Katherine White, What if Bicycles Held the Secret to Human Flight?, Henry Ford Museum, www.thehenryford.org/explore/stories- of-innovation/what-if/wright-brothers; Brittany McCrigler, The Wright Way: Repair Teaches Engineering, iFixit (Mar. 21, 2013), www.ifixit.com/News/4404/the-wright-way-to-teach- engineering.

Wrights' invention undoubtedly benefitted from the knowledge and skills they honed through repair.

These related research-informed practices differ from repair in important respects. User innovation, for example, often entails a dialogue between users and manufacturers, whereas experimental repair is an almost entirely user-driven process carried out in the absence of access to manufacturer-approved parts, tools, or information. An example of this type of experimental repair is Russian all-terrain vehicles known as "karakats". They are self-assembled vehicles using a mixture of self-made and manufactured components. Their significant modifications enable them to 'skate and swim'.[54] Karakats' modifications are the result of many decades of iterative self-repair practices and alterations in response to harsh winters, the arctic landscape, and the difficulty in obtaining official parts, tools and information.[55] This type of experimental and transformative repair can be considered "adaptation in use" that constitutes a distinct stage of user innovation. Nonetheless, they all emerge from the analytic engagement with a device characterized by repair practices specifically, and device research more generally.

In recent years, the user-generated knowledge of devices that emerged from these practices has become widely available through online communities and forums. For example, 3D printing has empowered users with new capabilities to design, share, and distribute design files for replacement parts that are otherwise unavailable. YouTube has also exploded as a source of information and how-to guides for repairing niche devices, particularly those for which no official documentation has been published or there is a need to improve upon the official repair procedures or tools recommended by manufacturers. At the same time, community-based and open-source research has also burgeoned in a whole host of scientific and technical fields such as the open-source hardware movement.[56] GitHub and Hackster.io are prime examples of community-led research, discovery, and innovation that is built largely on the contributions of individuals seeking to improve existing products and devices. Where experimental research results in innovations of this sort, it expedites and lowers the cost of innovation, and decentralizes technical knowledge.[57] Too often though, copyright law can interfere with these valuable forms of research.

---

[54] Patrick Laviolette & Alla Sirotina, "Karakats: The Bricolage of Hybrid Vehicles that Skate and Swim" (2015) 9:1 Journal of Ethnology and Folkloristics 21-40.

[55] Sampsa Hyysalo & Svetlana Usenyuk, "The user dominated technology era: Dynamics of dispersed peer-innovation" (2015) 44:4 Research Policy 560-576.

[56] OpenGears, "Open-Source Hardware for a better Future of Repair" (14 October 2022) *Medium.com,* online: https://medium.com/codex/open-source-hardware-for-a-better-future-of-repair-international-repair-day-on-sat-15-october-2022-b0c28af169d6

[57] Jono Bacon, The Art of Community: Building the New Age of Participation, 2nd ed, (O'Reilly, 2012) at xi.

III. COPYRIGHT AS AN IMPEDIMENT TO DEVICE RESEARCH

Despite the social, economic, and environmental benefits of experimental repair, copyright's role in impeding repair manifests in at least three ways. The first is in limiting or denying access to repair information, including repair instructions, parts lists, wiring diagrams, schematics, and diagnostic tables. Though this type of information may lack the requisite originality to receive copyright protection, it is often incorporated into repair guides and manuals that are protected. Copyright in these works can serve as a powerful tool by manufacturers to prevent the diffusion of technical knowledge and control access to repair.[58]

The second copyright impediment to repair is in reproducing, modifying, or distributing device software. As was well canvassed by the United States Supreme Court in *Google LLC v Oracle America, Inc.* saga, even primarily utilitarian and functional aspects of software code can attract copyright protection.[59] As a literary work, software in turn grants rightsholders with all the available enforcement and control mechanisms under copyright law, including TPMs and anti-circumvention rules.

This leads us to the third and most prominent way that copyright impacts device research and repair—TPMs. While at the turn of the millennium it may have been possible to distinguish a computer from other devices and appliances, the rise of embedded system design and ubiquity of semiconductors means that seemingly every object is now a purpose-specific computer. One consequence of this transformation is that software dictates more and more of the functionality of the devices we rely upon, from medical equipment to voting machines. Many of these devices also rely on hardware-based security mechanisms that are shielded by anti-circumvention laws. When put together, the effect is to imbue an increasing number of the devices, products, and machinery in our tangible world with copyright governance. Thus, while much of copyright law and policy over the past two decades has been focused on the dematerialization of copyrightable subject matter into the digital realm, a concurrent theme has been the gradual re-materialization of intellectual property to control the use and function of tangible objects.[60]

This phenomenon has a significant impact on both the practical ability

---

[58] Kevin Truong, "A Medical Device Maker Threatens iFixit Over Ventilator Repair Project" (16 June 2020) *Vice*, online: https://www.vice.com/en/article/akze8j/a-medical-device-maker-threatens-ifixit-over-ventilator-repair-project For a discussion of these issues under EU copyright law, see Anthony D Rosborough, "Zen and the Art of Repair Manuals: Enabling a participatory Right to Repair through an autonomous concept of EU Copyright Law" (2022) 13:3 JIPITEC 113-131.

[59] *Oracle Am., Inc. v. Google LLC*, No. 2017-1118, 2021 WL 1941874 (Fed. Cir. May 14, 2021).

[60] Guido Noto La Diega, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies* (Routledge, 2023) 2, and see Jennifer Gabrys, 'Re-Thingifying the Internet of Things' in Nicole Starosielski and Janet Walker (eds), Sustainable Media: Critical Approaches to Media and Environment (Routledge 2016) 180.

and legal authorization to repair things. Unlike analog mechanical devices, computerization obscures the inner workings of devices as software code, often embedded in silicon. This creates a need for distinct skillsets and methodologies in diagnosis and repair.[61] Unlike traditional aptitudes like spatial reasoning or mechanical comprehension, diagnosing and testing computerized devices involves many more layers of abstraction and interdependent systems. These barriers to diagnosis and repair reduce the extent to which device research and the information it yields are accessible, democratized, and decentralized.

The DMCA §1201

The U.S. approach to anticircumvention is embodied in § 1201 of the Digital Millennium Copyright Act (DMCA).[62] The DMCA supplements copyright law's standard exclusive rights by prohibiting the circumvention of technological protection measures as well as the creation and distribution of tools that enable circumvention. [63] Section 1201 distinguishes between two types of TPMs. Access controls are measures intended to prevent unauthorized access to copyrighted works, whereas copy controls are designed to prevent reproduction or other acts that infringe copyright.[64] With respect to access controls, the DMCA prohibits both circumvention—the act of decrypting an encrypted work, or otherwise disabling, removing, or avoiding a TPM—and trafficking—the manufacture, distribution, sale, or offering to the public of devices, tools, or technologies that enable circumvention. [65] When it comes to copy controls, the DMCA also bans trafficking in circumvention tools.[66] Although the statute does not ban the act of circumventing a copy control, it may nonetheless constitute traditional copyright infringement.

The DMCA also includes a number of statutory exceptions intended to limit its scope. But because of parsimonious drafting and narrow interpretations by courts, those exceptions have been of limited value to those hoping to engage in the sort of device research we have outlined. Three of those provisions merit further discussion.

First, § 1201(f) creates an exception to the anti-circumvention and anti-trafficking provisions for reverse engineering when undertaken "for the sole purpose of identifying and analyzing those elements of [a computer] program that are necessary to achieve interoperability of an independently created computer program with other programs."[67] This provision, however, does not

[61] Stephen Graham & Nigel Thrift, "Out of Order: Understanding Repair and Maintenance" (2007) 24(3) *Theory, Culture & Society* 1-25 at 4.
[62] 17 U.S.C. § 1201.
[63] Id.
[64] Id.
[65] Id.
[66] Id.
[67] Id. § 1201(f).

permit reverse engineering meant to identify and extract information for pure research purposes or to create independent, noninteroperable products. Moreover, § 1201(f) only permits the circumvention of TPMs applied to computer programs, not "works generally, such as music or audiovisual works . . . distributed in digital form." The result is a reverse engineering provision that affords considerably less leeway than pre-DMCA copyright decisions.[68] To date, no defendant has successfully asserted a defense under § 1201(f).[69]

Second, § 1201(g) permits circumvention and the creation of related tools "in the course of an act of good faith encryption research," where such research is defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[70] Research that satisfies that definition is permitted, but only so long as a number of additional criteria are satisfied. The researcher must lawfully obtain a copy of the encrypted work and make "a good faith effort to obtain authorization before the circumvention." In addition, any otherwise prohibited must be necessary to conduct the research and cannot constitute copyright infringement of a violation of the Computer Fraud and Abuse Act. No defendant has prevailed on an encryption research defense.

Finally, § 1201(j) offers defenses to the anti-circumvention and anti-trafficking provisions for those "engage[d] in an act of security testing," which the statute defines as "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability."[71] Such testing requires "the authorization of the owner or operator" of the computer, system, or network. Additionally, courts are instructed to consider whether the information derived from the testing "was used solely to promote the security of the owner or operator of such computer … or shared directly with the developer of such computer" and whether that information "was used or maintained in a manner that does not facilitate infringement [or] a violation of privacy or breach of security."[72] To the extent security testing is undertaken to protect the interests of the public broadly or the researcher engages in widespread publication of vulnerabilities, defendants may jeopardize any defense under § 1201(j). Like

[68] See Sega v. Accolade; Sony v. Connectix.

[69] Although ultimately decided on other grounds, the Sixth Circuit disagreed with the district court's rejection of the 1201(f) defense in Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 550 (6th Cir. 2004).

[70] 17 U.S.C. § 1201(g).

[71] Id. § 1201(j).

[72] The Conference Report on the DMCA supports a narrow reading the security testing provision. H.R. REP. NO. 105-796, at 67 (1998) (Conf. Rep.) (explaining that "It is not unlawful to test the effectiveness of a security measure before it is implemented to protect the work covered under title 17. Nor is it unlawful for a person who has implemented a security measure to test its effectiveness.").

its counterparts, this provision has yet to be successfully asserted in litigation. On the whole, these statutory defenses recognize the DMCA's potential to disrupt legitimate reverse engineering, research, and testing activities. In practice, however, their narrow scope offers researchers little meaningful insulation from potential liability.

Congress anticipated the risk that § 1201 would interfere with otherwise lawful behavior, so it created a rulemaking process that empowers the Library of Congress, acting on a recommendation from the Register of Copyrights, to craft temporary, three-year exemptions to § 1201's anti-circumvention provision for classes of copyrighted works the noninfringing uses of which are likely to be adversely affected.[73] In addition to a series of exemptions permitting circumvention in order engage in "good-faith testing, investigating, or correcting" of security flaws and "good-faith security research," the rulemaking process has secured a number of temporary exemptions that permit circumvention to facilitate repair of vehicles, smartphones, home appliances, video game consoles, and consumer devices generally. Crucially, while these exemptions allow the act of circumvention, they do not permit the creation or distribution of tools or technologies that would enable others to circumvent. This limits how researchers use and perhaps even how they publish their findings.[74]

Both the text of the DMCA and the decades of rulemaking that came in its wake reflect the impediments to device research anti-circumvention can creates. But neither the statutory exceptions nor the temporary exemptions have succeeded in eliminating those barriers.

The EU's TPM Framework

As the result of the 1996 WCT and earlier legislation extending copyright to computer programs, TPMs are also the subject of EU copyright laws. There is no single legislative source of copyright law in the EU. Instead, copyright is fragmented across several directives and regulations that address distinct subject matter. When it comes to TPMs, they are recognized under EU copyright law in the InfoSoc Directive[75] and the Computer Programs

[73] See § 1201(a)(1)(C). See also H.R. REP. NO. 105-551, pt. 2, at 37 (1998) (noting that the "primary goal of the rulemaking proceeding is to assess whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use these works in ways that are otherwise lawful.").

[74] In Felten v. RIAA, a case involving an academic encryption researcher, the Department of Justice argued against an interpretation of the anti-trafficking provision that would reach "normal scientific research" and publishing. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss, at 17, Felten v. Recording Indus. Ass'n of Am., No. 01- CV-2669 (D.N.J. Sept. 25, 2001) ("[t]he Plaintiffs are scientists attempting to study ac- cess control technologies. The DMCA simply does not apply to such conduct."). But the DOJ did rule out the possibility that "making available a publication that describes in detail how to go about circumventing a particular technology could be prosecuted under the statute. Id. at 17 n.5.

[75] Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects

Directive.[76] The former addresses most of the copyrightable subject matter like audio visual and creative works, while the latter creates a distinct set of rules and exceptions for software. Each directive has its own framework for TPMs. The effect is to create two parallel regimes for TPMs where separate exceptions and limitations apply depending on subject matter of TPM control.

The InfoSoc Directive defines TPMs somewhat narrowly as tools for restricting acts related to copyright and related rights. Though it includes a blanket prohibition on private acts of circumvention, it requires that rightsholders enable users to take advantage of certain copyright exceptions for non-infringing purposes.[77] But the Computer Programs Directive takes a different approach. It isolates computer program TPMs from other copyright exceptions and defines TPMs very broadly as any "technical device applied to protect a computer program". Of the two directives, the Computer Programs Directive's open-ended TPM concept aligns more closely with the access control approach in the US' DMCA. Private acts of circumvention are permitted, but the directive prohibits "putting into circulation" or "possession for commercial purposes" of the means of facilitating the unauthorized removal or circumvention of technical devices.[78] Despite the breadth of computer program TPMs, the Directive does not mirror the DMCA in offering a system for granting exemptions. It instead relies on a blanket exception permitting "acts necessary to observe, study or test the functioning of the program", leaving it unclear whether 'functioning' extends also to the physical or tangible aspects of computerized devices.

The prevalence of complex works that blend computer programs with other copyrightable subject matter has made it difficult to discern which set of rules should apply in some cases. Though jurisprudence at the EU level has clarified that video games fall within the ambit of InfoSoc's framework[79], it is not clear how EU copyright law should treat other complex works like operating systems or device software with graphical user interfaces and sound elements. EU anticircumvention law has not seen the same degree of contention and litigation as it has in the US, but the confusion and uncertainty created by its TPM framework can produce a chilling effect on device research and repair.[80]

Across both jurisdictions, access control TPMs evidence an important

---

of copyright and related rights in the Information Society OJ L167/10 (InfoSoc Directive).

[76] Council Directive 91/250/EC of 14 May 1991 on the legal protection of computer programs OJ L122/42 (Computer Programs Directive).

[77] Infosoc Directive, Art 6(4).

[78] Computer Programs Directive, Article 7(1)(c).

[79] *Nintendo Co Ltd and Others v PC Box Srl* (C-355/12) EU:C:2014:25; [2014] EUECJ C-355/12 (CJEU).

[80] Anthony D Rosborough et al., "Achieving a (copy)right to repair for the EU's green economy" (2023) 034 JPAD 1-9, online: https://academic.oup.com/jiplp/advance-article/doi/10.1093/jiplp/jpad034/7147057

nexus between copyright and device research. Though they were intended primarily to prevent infringement of copyrighted entertainment content, they have extended copyright owners' exclusive rights to cover adjacent and uncopyrightable technologies.[81] This has permitted copyright to serve as a tool for controlling technological platforms, including the flow of information related to device research and repair. This information has enormous social, economic, and environmental benefits. TPMs confine device research and repair information to exclusive distribution channels, limiting competition and innovation.[82] When mobilized for these purposes, TPMs fail to uphold a cornerstone of intellectual property – to incentivize bringing information, knowledge, and ideas into the public realm.

IV. CASE STUDIES

The following case studies and examples canvas copyright impediments to device research, with a particular focus on repair-related inquiries. They are separated according to the three stages of experimental repair described in Part II (diagnosis, implementation, and reporting). At each of these stages, copyright is implicated in one way or another, although TPMs and anticircumvention persist as a dominant theme. By grounding our conceptual framework of experimental repair with these specific examples, our aim is to shed light on the breadth of copyright interference in device research.

A. *Diagnosis*

Potential liability under the DMCA chills valuable research that could otherwise identify, diagnose, and ultimately correct failures and vulnerabilities in a range of devices and systems. Security researchers in particular have been sounding the alarm over the ways in which anti-circumvention laws impede their work for decades. By shrouding software code behind technological and legal barriers, TPMs can help firms hide security flaws from the prying eyes of researchers. And in some cases, those TPMs introduce their own security vulnerabilities that threaten individual consumers and critical network infrastructure.[83] Consumer electronics, webcams, and children's toys commonly ship with significant security vulnerabilities that could be addressed through independent research.[84] More troublingly, these vulnerabilities open other devices and systems—from medical devices and voting machines to the electrical grid and nuclear power plants—to potential attacks by bad actors.[85]

---

[81] Dan L Burk, "Anticircumvention Misuse" (2003) 50 UCLA Law Review at 1136.

[82] Margaret Ann Wilkinson, "Is protection of data through data exclusivity, technological protection measures or rights management information actually intellectual property?", in Daniel J Gervais, ed, The Future of Intellectual Property (Edward Elgar, 2021) at 169-192.

[83] See generally, Deidre K. Mulligan & Aaron K. Perzanowski, The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident

[84]

[85]

When software code is cloistered behind TPMs, researchers face significant barriers to identifying and diagnosing potential vulnerabilities. As a technical matter, removing or bypassing most TPMs is straightforward, if not trivial. But this act of circumvention, which is often a necessary first step in analyzing the underlying code or its outputs, carries with it real legal risk. That risk manifests itself in a variety of ways, all of which can slow, frustrate, or prevent research projects aimed at protecting the public from harm. First, the hassle and risk of investigating a TPM-encumbered device may dissuade researchers from taking on a project, steering them towards areas of inquiry that are less legally fraught.[86] Second, researchers who choose to pursue such projects may well find department chairs, administrators, funders, and even government agencies less than enthusiastic about the prospect of research that could trigger litigation.[87] And finally, even once a project is underway, protracted debates over potential liability and risk tolerance—discussions that can include both university general counsel and the researchers' own outside lawyers—throw considerable sand in the gears of the research enterprise.[88]

To take one example, the security and proper functioning of voting machines is an issue of crucial importance to democratic systems. The ability to identify and address genuine vulnerabilities, as well as the capability to distinguish real flaws from rumor, fantasy, and propaganda, depends on device research. According to researchers, voting machines have "serious exploitable vulnerabilities . . . that could be used to undetectably alter the outcome of an election."[89] But the firms that market these devices have strong incentives to obscure their vulnerabilities from public view. When internal emails from voting machine company Diebold were leaked in 2003, they

[86] "Submitters have chosen not to perform specific acts of security research that they believe would have prevented harms to and benefited safety of human persons. Consequently, the Submitters have failed to produce and share the results of this research with the public. They perceive the DMCA to penalize the creation of potentially life- saving security research." https://cdn.loc.gov/copyright/1201/2014/petitions/Bellovin_1201_Intial_Submission_2014.pdf

[87] "CDT asserts that the DMCA's anticircumvention rule "discourages both academic institutions and government entities from funding critical security research." https://cdn.loc.gov/copyright/1201/2015/registers-recommendation.pdf; https://cyberscoop.com/voting-machine-dmca-exemption-security-research-hearing/ ("There absolutely have been cases where local governments have wanted to conduct independent security testing on voting systems and have either been denied permission or have refrained from seeking permission because they were convinced it would be denied if sought.").

[88] Rootkit ("In the weeks and months prior to the public disclosure of the XCP rootkit, two prominent computer security and DRM researchers, Professor Ed Felten and J. Alex Halderman, were forced to divide their energy be- tween researching and publicizing the dangerous implications of Sony BMG's protection measures, on the one hand, and engaging in protracted discussions of potential DMCA liability with both their outside legal team and the general counsel of their academic institution, on the other.")

[89] 2015 Rec

acknowledged flaws in Diebold's machines. The company promptly issued dozens of copyright takedown notices in hopes of scrubbing the damning emails from the internet. Eventually, a court held that the posting of the emails was a fair use and that Diebold abused the notice and takedown process.[90]

If firms are willing to aggressively assert copyright law to prevent the dissemination of their own emails, there is little reason to think they would hesitate to target researchers who crack open their devices to unearth their hidden flaws.[91] Since voting machines typically rely on TPMs to restrict access to the software that tabulates and verifies vote totals, ensuring that those processes are reliable and secure requires circumvention. Those acts of circumvention would be lawful if a vendor gives independent researchers permission to inspect the inner workings of their machines.[92] Otherwise, researchers are forced to rely on some applicable defense. As the Copyright Office itself has recognized, the existing statutory exemptions are not "sufficiently robust" and "do not cover the full range of proposed [noninfringing] security research activities."[93] The temporary exemptions adopted via rulemaking have created some additional breathing room for researchers, but their scope is limited. And the time and effort necessary to secure such exemptions are considerable, increasing the costs of security research and dissuading potential researchers.

Even when defendants ultimately prevail against allegations of circumvention, the risks of engaging in unauthorized diagnosis of a device are apparent. StorageTek sold tape-based data storage systems. When a competing repair provider, Custom Hardware Engineering & Consulting (CHE), captured and deciphered the error codes thrown by StorageTek's devices, the company sued, alleging CHE had overridden the technological protection measure that locked down the devices.[94] After years of litigation, CHE ultimately prevailed on appeal to the Federal Circuit. The court held that StorageTek failed to establish the "critical nexus" between CHE's circumvention and any potential copyright infringement. Notably, other U.S.

---

[90] Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004

[91] In one early dispute, the Secure Digital Music Initiative (SDMI) challenged security researchers to find vulnerabilities in their digital music TPMs. After a team of Princeton researchers led by Ed Felten defeated those TPMs, SDMI sent letters threatening legal action if the researchers results were presented at an academic conference. Felten filed a declaratory judgment action to establish that his research did not violate the DMCA. After the RIAA disavowed any intent to pursue claims against him, the case was dismissed. See Tinkerers' Champion, THE ECONOMIST, June 22, 2002; First Amended Complaint, Felten v. Recording Indus. of Am., Inc., No. CV-01-2660 (D.N.J. June 26, 2001), available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010626_eff_felten_amended_complaint.html.

[92] Doris Estelle Long, Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?, 23 J. Computer & Info. L. 533 (2006)

[93] https://cdn.loc.gov/copyright/1201/2015/registers-recommendation.pdf

[94] Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

courts have declined to adopt the Federal Circuit's nexus requirement, leaving liability for diagnostic research unclear.

Putting anti-circumvention aside, diagnostic research can lead to potential copyright liability. Corellium produces virtualization software that allows researchers and developers to emulate Apple's iOS mobile operating system on non-Apple hardware. Corellium's stated goal was the creation of "a good environment for security researchers to do their work." Beyond merely running iOS on non-Apple devices, Corellium's security research platform offered a range of technical features that "enable[] researchers to holistically view and comprehend all system calls made by the operating system and the apps running on it, giving researchers the ability to examine and understand both iOS itself and iOS-based applications in advanced new ways." In 2019, after a failed attempt to acquire Corellium, Apple sued the company. It alleged infringement of its iOS copyrights and circumvention of its TPMs. The parties eventually settled the DMCA claims, but Apple continued to pursue its copyright infringement theory.[95] In 2023, the Eleventh Circuit affirmed a fair use determination in Corellium's favor with respect to direct infringement of the iOS code.[96] Apple's claim of contributory infringement, as well as its contention that Corellium infringed the copyright in Apple's icon and wallpaper designs, remain live questions.

B. *Implementation*

Experimental repair's implementation stage takes place after a repairer has clarified the cause or source of fault. Attention and energy are then devoted to implementing a remedy or solution, sometimes through trial and error. In many instances, the solution decided upon at the implementation stage is influenced by the lack of access to manufacturer-approved parts or tools, necessitating some form of improvisation. A clear example of these type of scenario is in the independent and "unauthorized" repair of John Deere combines and tractors.

The increasing digitalization and corresponding difficulty of repairing John Deere tractors and other equipment has been well documented in recent years.[97] According to Willie Cade—a staunch Right to Repair advocate and grandson of Theo Cade, a longtime John Deere engineer who patented more than 150 inventions—the company's X9 1100 series combine makes use of 325 sensors and 36 controllers, while the 9RT-570 tractor incorporates 29

---

[95] https://www.washingtonpost.com/technology/2021/08/10/apple-drops-corellium-lawsuit; https://www.theverge.com/2021/8/11/22620014/apple-corellium-security-virtual-iphone-dmca-lawsuit-settled

[96] Apple Inc. v. Corellium, LLC, 510 F. Supp. 3d 1269, 1293 (S.D. Fla. 2020), aff'd in part, vacated in part, remanded sub nom. Apple Inc. v. Corellium, Inc., No. 21-12835, 2023 WL 3295671 (11th Cir. May 8, 2023)

[97] See, e.g., Kevin O'Reilly, "Deere in the Headlights: How Software That Farmers Cannot Access Has Become Necessary To Tractor Repair" (2021) U.S. PIRG, online: https://pirg.org/edfund/wp-content/uploads/2023/01/Deere-in-the-Headlights.pdf

controllers and 570 sensors.[98] These controllers are all interconnected and play a crucial role in communicating with and sending data to the machine's central computer. This data refers to levels of moisture, rotation, temperature, oil pressure, and hundreds of other measurements. Importantly, each of the controllers require machine instructions dictated by software.

The sophistication of these machines is the primary reason that they are so much more difficult to repair independently when compared to their analog ancestors. When a physical part or component of the machine is replaced or modified for repair purposes, those machine instructions need to be updated or recalibrated.[99] These machine instructions are encrypted and packaged as "payload files" that are paired to the serial numbers of components. Given John Deere's tight network of dealers and authorized technicians[100], however, farmers and repairers do not have access to the tools necessary to decrypt or modify payload files.

Farmers have responded to this lack of access with their traditional ingenuity, and online forums have helped them disseminate self-made solutions. An online community comprised of grey hat hackers, encryption researchers, and agricultural technologists built and distributed a payload encryptor/decryptor tool. This is a small software application that allows farmers to edit and update payload files necessary for activating new components once they are installed in the machine. This payload encryptor/decryptor tool has provided independent repairers has provided a solution to some of the software-imposed barriers that arise when trying to fix these machines.

Despite its enormous benefit, copyright prohibits wider access to the encryptor/decryptor tool. It is presently only available through grey market online sellers based mostly in Eastern Europe and Russia. In the US, circulation of the tool remains unlawful even though John Deere agreed to a Memorandum of Understanding (MOU) with the American Farm Bureau Federation (AFBF) in 2023. This is because the MOU includes a carve out that preserves Deere's intellectual property and protection from "illegal infringement through modification of Embedded Software".[101] Though the United States' LoC granted a § 1201 DMCA exemption in 2018 for accessing computer programs in agricultural vehicles for repair purposes, circulation of the tool is still unlawful under the DMCA. This is because the LoC rulemakings apply exempt only 'private' acts of circumvention, leaving the distribution or "trafficking" of the encryptor/decryptor tool unlawful. The result is that even where a DMCA circumvention exemption applies, it is of little help to experimental repair and device research. The situation is the

[98] https://www.youtube.com/watch?v=aB_xSiGIL1s

[99] Kevin O'Reilly, Deere in the Headlights at 11.

[100] Kevin O'Reilly, "Deere in the Headlights II: How Dealership Consolidation Reduces Repair Choice for Farmers" (2022) U.S. PIRG, online: https://publicinterestnetwork.org/wp-content/uploads/2022/02/Deere-In-The-Headlights-II.pdf

[101] https://www.fb.org/files/AFBF_John_Deere_MOU.pdf

same in Europe, where the Computer Programs Directive clearly prohibits "any act of putting into circulation…any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program".[102] The challenges facing farmers are just one example of the ways in which TPMs and anticircumvention restrictions interfere with the implementation of repairs even after a successful diagnosis.

C. *Reporting*

Beyond a framework for exclusive rights, copyright can also be used as a tool for censorship.[103] In the context of security research, this is probably best exemplified by litigation threats received by Ed Felten in relation to the Secure Digital Music Initiative (SDMI). Felten and a team of researchers entered a contest to try and break the digital audio watermark encryption technology that was being developed in 2000. After successfully breaking the digital audio watermark, Felten and his team sought to publish their findings in a scientific paper for presentation at a conference but faced legal threats from the SDMI, the Recording Industry of America (RIAA) and others pursuant to the DMCA. This prompted Felten and the team to withhold the paper from publication and instead file a declaratory judgment action seeking to establish the legality of sharing the results of their research. Though Felten's paper was eventually released the following year upon assurances from the RIAA and the US Department of Justice, the Felten case nevertheless serves as a powerful example of the censorship function of copyright law.[104]

Like Felten, independent repairers can also be threatened and intimidated by copyright claims after sharing repair methods, schematics, and how-to online. While there are many cases where manufacturers have sought to prevent the distribution of their own published materials[105], user-created

---

[102] Computer Programs Directive, Article 7(1)(c).

[103] Stephen McLeod Blythe, "Freedom of Speech and the DMCA: Abuse of the Notification and Takedown Process" (2019) 41:2 EIPR 70-88 at 71-72.

[104] See Tinkerers' Champion, THE ECONOMIST, June 22, 2002; First Amended Complaint, Felten v. Recording Indus. of Am., Inc., No. CV-01-2660 (D.N.J. June 26, 2001), available at http:/ www.eff.org/IP/DMCA/Felten v RIAA/20010626_eff feltenamended_complaint.html.

[105] For example, in 2012 Tim Hicks, a laptop refurbisher who ran an online resource for repair information, received a cease and desist letter from Toshiba asserting copyright in their repair documentation, commenting that these documents are provided only to authorised service providers under 'strict confidentiality agreements'. See, Kyle Wiens, "The Shady World of Repair Manuals: Copyrighting for Planned Obsolescence" (12 November 2012) *Wired*, online: https://www.wired.com/2012/11/cease-and-desist-manuals-planned-obsolescence/ During the early stages of the COVID-19 pandemic, iFixit received a similar cease and desist in relation to repair manuals for medical equipment. See, Kit Walsh, "Medical Device Repair Again Threatened With Copyright Claims" (11 June 2020) *Electronic Frontier Foundation*, online: https://www.eff.org/deeplinks/2020/06/medical-device-repair-again-threatened-copyright-claims

repair information developed through device research has also been placed in the crosshairs.[106] A powerful and extortive tool for manufacturers and rightsholders to achieve these ends is YouTube's copyright takedown system, known as a "removal request".[107] Notorious for siding with copyright claimants, the effect of this system can facilitate copyright misuse through takedowns grounded in ulterior motives.[108] In these situations, copyright infringement becomes a readily accessible shorthand for the dissemination of technical knowledge that device manufacturers would rather keep private.

For example, in 2020 Danish YouTuber and electronics technician Mads Barnkob was the recipient of an abusive invocation of YouTube's copyright removal request system. Barnkob's YouTube channel involves the technical dissection and teardown of various electronic devices and components. In one video, he carried out a teardown of an Ericsson RBS3202 Base Station that he owned.[109] This device is commonly used on mobile telecommunications towers. The video explains the signal and current paths across various circuit boards, and the hardware configuration of the device. Shortly after publishing the video, Barnkob received a copyright strike notice from YouTube filed by Ericsson. Barnkob revealed in a public forum posting that in Ericsson's complaint, the company alleged that the video includes "detailed information about the product…which belong to an area where our company holds many IPR rights".[110] Though Ericsson eventually withdrew the removal request, Barnkob's first course of action was to remove or disable all his videos involving the company's equipment. This example reveals the relative ease with which manufacturers can prevent, or at least interfere with, the dissemination of device research online.

Barnkob's experience was not without precedent. Well-known YouTuber and Right to Repair advocate Louis Rossmann was the recipient of similar coercive tactics from Apple in 2016. Rossmann's long-running YouTube channel shows intricate board-level repairs of Apple devices, accompanied by Rossmann's complaints against the manufacturer for its business practices that make user repair inaccessible or impractical. He often refers to Apple's schematics and wiring diagrams to carefully teach viewers how to repair various devices. In 2016, Rossmann received an ambiguous notice from Apple's intellectual property lawyers, suggesting that there were

---

[106] Leah Chan Grinvald & Ofer Tur-Sinai, "Intellectual Property and the Right to Repair" (2019-2020) 88 Fordham Law Rev 63-128 at 67.

[107] Shoshana Wodinsky, "YouTube's copyright strikes have become a tool for extortion" (11 February 2019) *The Verge*, online: https://www.theverge.com/2019/2/11/18220032/youtube-copystrike-blackmail-three-strikes-copyright-violation

[108] Tim Cushing, "YouTube Finally Demands Specificity From Copyright Claimants" (11 July 2019) *TechDirt*, online: https://www.techdirt.com/2019/07/11/youtube-finally-demands-specificity-copyright-claimants/

[109] https://www.youtube.com/watch?v=0mlNHPbEfrs

[110] https://www.eevblog.com/forum/chat/ericsson-slammed-me-with-a-copyright-strike-on-a-teardown-video-help!/

issues with his channel.[111] In a cryptic YouTube video[112], Rossmann suggested that his followers consider downloading his content in order to preserve it – indicating his concern that his channel may be removed from YouTube. After considerable online controversy and concern, Rossmann reported that Apple's lawyers later claimed that their intention was simply to express their appreciation for his videos. But by creating confusion and uncertainty, Apple's communications look more like an effort to intimidate a prominent voice sharing the results of device research.

Compounding the power of manufacturers to wield copyright as a tool to suppress device research is the difficulty in documenting and report on the abusive practices themselves. For YouTube creators who fall victim to this intimidation, there is a disincentive to report on it publicly. And even for those like Barnkob who successfully defend their content, the hostility of the interaction is often enough to dissuade them from risking further confrontation.[113] In sum, copyright and the content removal tools made available to manufacturers can act as a significant barrier to reporting and disseminating technical knowledge gained through device research.

CONCLUSION

This paper's core assertion is that a Right to Research in copyright law must embrace not only the access and use of expressive works, but also the analysis of physical devices and the software that drives them. Experimental device repair is one acute example of copyright impeding research and restricting the flow of the information that results. Building upon a line of scholarship from the Information Studies field, we have put forward an analytical framework for experimental repair that demonstrates its relationship to research at three discernable stages. We have also revealed how copyright can impede research at each of these stages. Whether through restricting access to published repair information, TPMs cordoning off onboard software, or litigation threats preventing researchers from reporting and disseminating their findings, copyright can have a profound effect on our ability to learn about the inner workings of devices. A Right to Research in

---

[111] Julia Bluff, "Louis Rossmann Might Lose His Repair Videos After Legal Threat" (1 July 2016) *iFIxit*, online: https://www.ifixit.com/News/8210/rossmann-repair-legal-threat

[112] https://www.youtube.com/watch?v=F7N254MTA4Q

[113] Beyond discouraging researchers to report on copyright claims of this sort, there are also enormous demands, opportunity costs, and time constraints placed on researchers when they are required to respond to legal claims and threats of action. See, e.g., Deirdre K Mulligan & Aaron Perzanowski, "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident" (2007) 22 BTLJ 1157-1232 at 1198 where the authors write: "In the weeks and months prior to the public disclosure of the XCP rootkit, two prominent computer security and DRM researchers, Professor Ed Felten and J. Alex Halderman, were forced to divide their energy between researching and publicizing the dangerous implications of the Sony BMG's protection measures, on the one hand, and engaging in protracted discussions of potential DMCA liability with both their outside legal team and the general counsel of their academic institution, on the other."

copyright law therefore must not lose sight of these new and emerging areas of copyright governance. "Research" must be given a broad and purposive interpretation that enables both general and domain specific fields of inquiry, while also applying to both institutionalized and informal actors.

A necessary implication of these assertions is that the same dynamics work in the opposite direction. Through device research and experimental repair, the absence of copyright can equally encourage new applications and uses for technologies. For example, the Linksys WRT54G router reveals the benefits of device research and experimental repair and its connection to innovation and the development of new technologies. Coined the 'best-selling router of all time'[114] the WRT54G was a common relic of workplaces and households during the early 2000s.[115] Due to its use of firmware that had been built on a GNU General Public License[116], its manufacturer was forced to release the source code after threats of litigation by the Free Software Foundation.[117] In the years following, the WRT54G became a learning device for hacking, security testing, and programming. The open-source firmware led to the creation of the OpenWRT project, an open-source Linux-based operating system that can be used on routers, smartphones, personal computers, and other small embedded systems. Innovative projects using OpenWRT include a connected plant health monitor[118], a home power consumption monitor[119], and a Wi-Fi-controlled robot with motorized wheels and a camera.[120] This reveals that where device research is left unimpeded by copyright, enormous social and economic benefits can be realized.

Beyond these assertions and findings, this paper also serves as a foundation for several divergent future inquiries. For example, future research may further explore the relationship and overlap between different activities that can fall under the common banner of device research. This includes activities like repair, user innovation, modification, and tinkering. Though our primary focus has been to reveal the central and unifying role

---

[114] Nick Farrell, "Belkin resurrects "best selling router of all time" (7 January 2014) *Fudzilla*, online: https://www.fudzilla.com/news/33591-belkin-resurrects-%E2%80%9Cbest-selling-router-of-all-time%E2%80%9D

[115] Ernie Smith, "The Default Router: How Linksys' most famous router, the WRT54G, tipped into legendary status because of an undocumented feature that slipped through during a merger" (13 January 2021), *Tedium*, online: https://tedium.co/2021/01/13/linksys-wrt54g-router-history/

[116] David Cassel, "The Open Source Lesson of the Linksys WRT54G Router" (24 January 2021), *TheNewStack*, online: https://thenewstack.io/the-open-source-lesson-of-the-linksys-wrt54g-router/

[117] Matt Lee, "Free Software Foundation Files Suit Against Cisco for GPL Violations" (11 December 2008), *Free Software Foundation*, online: https://www.fsf.org/news/2008-12-cisco-suit

[118] https://hackaday.io/project/8657-open-source-hardware-plant-health-monitor

[119] https://hackaday.io/project/9367-house-power-consumption-monitoring

[120] Caleb Kraft, "WiFi Robot: A Hacked WRT54G Router" (*Hackaday*, 28 August 2008) at https://hackaday.com/2008/08/28/wifi-robot-a-hacked-wrt54gl-rover/ (last visited 23 December 2021).

played by repair, future research may explore the ways in which these related activities are intertwined and support one another. In addition, future empirical research may further explore the impact of litigation threats on the dissemination of device research online.

In conclusion, the products and devices that surround us are now increasingly containers of vast amounts of information. Digitalization means that devices are no longer subject only to mechanical limitations but are also the product of hidden inscriptions and information in the form of software and technical know-how. When this information is kept private or confined to exclusive distribution channels through copyright, the effect is to shut users, device owners, and the public out of learning processes, inquiries, and research. Experimental repair is a prime example of these activities because it requires the ability to read, write, and interpret the hidden inscriptions and information contained in devices. It also clearly exemplifies the material existence of copyright impediments to research that follow from copyright's embrace of software and the widespread computerization of products and devices.

In recent years, the materiality and tangible impacts of information exclusivity have propelled the Right to Repair toward burgeoning public relations and political success. Legislative reform is currently underway in numerous jurisdictions around the world. On this point, the Right to Research in copyright movement may find success in recognizing and embracing the information processes central to repair as part of its agenda. It is imperative that a Right to Research not lose sight of the far-reaching and tangible implications of copyright governance, including its impacts beyond the access and use of expressive works.