
**BEFORE THE DEPARTMENT OF COMMMERCE**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**

# COMMENTS OF THE OWNERS' RIGHTS INITIATIVE ON THE BENEFITS, CHALLENGES AND POTENTIAL ROLES FOR THE GOVERNMENT IN FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

The Owners' Rights Initiative (ORI) is an organization of over 20 companies and trade associations that have joined together to protect ownership rights in the United States.[1] We believe in the fundamental premise that **if you bought it, you own it**, and should have the right to sell, lend, or give away your personal property. ORI formed when the *Kirtsaeng v. Wiley* case was pending before the Supreme Court. We now are dedicated to preserving that holding, and making sure that it is not undermined in Congress, the executive branch, or in the courts. We also work to protect the principle of the first sale doctrine as technology continues to evolve, such as when software is incorporated into other products. Additionally, we try to prevent the misuse of IP law as a trade barrier that obstructs legitimate competition in other countries.

We appreciate this timely study on the Internet of Things. The Internet of Things consists of a wide variety of products that have networked connectivity that allow them to collect and exchange data. What enables these products to connect to communications networks is the software embedded in the products. Software is copyrightable subject matter, and the manufacturers of these software-enabled products can employ their control over the copyright in

[1] A list of ORI members can be found at http://ownersrightsinitiative.org/about/.

the software to control the use of these products after purchase. Currently, ORI members are most concerned about two forms of control. First, manufacturers can use their copyrights in the software to restrict the purchasers' right to transfer the products. This prevents the development of robust secondary markets for products in which purchasers—consumers and business alike—have invested billions of dollars. Second, manufacturers can take advantage of the Digital Millennium Copyright Act's prohibition on the circumvention of technological protection measures to restrict purchasers' ability to customize or repair the products they own. Amendments to title 17 would limit manufacturers' misuse of their copyrights to restrict competition in the Internet of Things.

Before proceeding, we note that NTIA should not draw false distinctions between consumer vs. industrial markets, as suggested in question 4. Such distinctions have little meaning in a world where individuals run businesses out of their homes on their laptop computers and where over 200 million Americans own smart phones that can operate millions of apps. Accordingly, in these comments we will not distinguish between industrial products and consumer products, nor between general-purpose computers and products with more limited functionality. The impact of copyright law on all these products is the same.

## I. PRESERVING THE FIRST SALE DOCTRINE IN THE INTERNET OF THINGS

The first sale doctrine is an exception to a copyright owner's exclusive right to distribute copies of her work. Under the first sale doctrine, a copyright owner's distribution right is exhausted with respect to a particular copy of a work after an authorized sale of that copy. Manufacturers must not be permitted to undermine the first sale doctrine with respect to devices attached to the Internet of Things.

### A. The Importance of the First Sale Doctrine

Justice Breyer, writing for the U.S. Supreme Court in *Kirtsaeng v. John Wiley & Sons, Inc*., 133 S. Ct. 1351, 1363 (2013), stated that the first sale doctrine "is a common-law doctrine with an impeccable historic pedigree." He quoted a 17th century articulation of "the common law's refusal to permit restraints on the alienation of chattels," *id*., and observed that "a law that permits a copyright holder to control the resale or other disposition of a chattel once sold is similarly 'against Trade and Traffi[c], and bargaining and contracting.'" *Id*. Justice Breyer underscored "the importance of leaving buyers of goods free to compete with each other when reselling or otherwise disposing of these goods." *Id*. Competition, "including the freedom to resell, can work to the advantage of the consumer." *Id*.

The first sale doctrine, codified at 17 U.S.C. § 109(a), operates at every level of our economy. It allows wholesalers to sell products covered by copyright, including products distributed in copyrighted packaging, to retailers without first securing distribution licenses from the manufacturers. The first sale doctrine likewise permits retailers to sell products to consumers without obtaining distribution licenses. Finally, the first sale doctrine permits consumers to rent or lend the products to other consumers, or to sell or give the products away when they no longer need them. The first sale doctrine reduces transaction costs and enables competition between sellers of new products as well as between new and used products. In *Kirtsaeng*, the Court recognized the importance of the first sale doctrine to libraries, used-book sellers, car dealers, technology companies, retailers, and consumers. The limitation on the distribution right provided by the first sale doctrine is critical to the functioning of our economy because the distribution right applies not only to products whose primary value is their protected expression, such as books, films, and sound recordings, but also to the protected expression in the packaging of

products and the software essential to the operation of products. The first sale doctrine is of particular relevance to the Internet of Things because virtually all the products that attach to the Internet of Things contain software that enable them to operate—and to interoperate with the Internet of Things.

### B. The First Sale Doctrine and Software-Enabled Products

Many products, ranging from high-end servers to toasters, rely on software for their operation. Even though the consumers buy the physical products, some manufacturers claim that they are just licensing the software essential to the products' operation.[2] These licenses could contain a variety of restrictive terms that limit ownership rights by interfering with resale of the products, thereby harming the consumers that want to sell equipment they no longer want and the secondary market consumers that want to buy that equipment.[3] Often, these secondary market consumers are federal, state, and local government entities. ORI believes that manufacturers should not be permitted to use software licenses to interfere with the resale of products.

Manufacturers currently employ software licenses to place the following impediments on the alienability of physical products:

- **Prohibition on transfer.** Some license agreements provide that the software license is non-transferable. For example, the license for the software that comes installed on a NetApp disk storage device is not transferable. As a practical matter, NetApp gets paid twice for the right to use the same software: once by the original purchaser of the

[2] The software often is pre-installed into the product by the manufacturer or the vendor. However, sometime the user must install the software provided by the manufacturers via the Internet or storage media such as DVDs.

[3] These licenses also interfere with the sale of unused products by resellers. Further, the licenses often require that product repairs be performed by authorized maintenance centers, thereby restricting the freedom of product owners to repair the products themselves or to use independent repair facilities.

product, and a second time by the purchaser of the used product. Purchasers of Cisco equipment often find that it is cheaper to buy new equipment than pay the excessively high price for a license for the software essential to the operation of the used equipment.

- **Refusal to provide updates.** Some license agreements specify that routine updates such as security-patches will be provided only to the original licensee. For example, Oracle refuses to supply routine updates to the purchasers of used hardware products containing essential Oracle software, unless they make an additional payment.
- **Bundling of maintenance contracts.** Some manufacturers will use control over the essential software as a means of forcing purchasers of used equipment to buy additional services from them. IBM, for example, will charge purchasers of used equipment a fee for software updates, but will provide the updates for free to purchasers that enter into maintenance agreements.[4]

The legal fiction on which these restrictive practices is based is that the essential software is licensed, not sold, to the purchaser of the hardware in which the software is installed. The manufacturers argue that because the purchaser is merely a licensee of the copy of the software, it does not have rights that normally accrue to the owner of a copy, such as the first sale doctrine or the right to make temporary internal copies necessary for the operation of a computer. *See* 17 U.S.C. §§ 109(a) and 117(a).

Cisco's own Frequently Asked Questions (FAQs), updated on May 4, 2015, make this argument in response to a question by a customer who had been approached by a third party

[4] Here are links to examples of these restrictive licenses: Palo Alto Networks (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html); and EMC (http://www.emc.com/collateral/software/warranty-maintenance/h2483-sw-use-rights.pdf).

hardware reseller who is not a Cisco-authorized channel partner. Cisco defended the lawfulness of its licensing policy as follows:

> The United States Court of Appeals for the 9th Circuit recently upheld the right of intellectual property owners such as Cisco to place reasonable restrictions on the licensing (and transferability) of their software, even where embedded in hardware, in the landmark case of Autodesk v. Vernor. In Vernor, the Court ruled that when a company sells its software with a license agreement (as Autodesk did - and as Cisco does), then the original user of the software is a licensee and not an owner. This means that the original user cannot transfer/sell the software without the permission of the owner of the intellectual property being licensed (i.e., AutoDesk or Cisco). In sum, the entity that is trying to sell you the hardware does not own the software on the product - and therefore has no rights to sell it to you. This means that if you purchased the product from that seller, your company would not have a license to use the software and would be in violation of Cisco's intellectual property rights. Cisco's licensing policy is in 100% alignment with this legal precedent.[5]

Cisco's FAQ neglects to mention that the U.S. circuit courts are split on the validity of this argument. While the Ninth Circuit has accepted it in *Vernor v. Autodesk*, 621 F.3d 1102 (9th Cir. 2010), the Second Circuit has rejected it in *Krause v. Titleserv*, 402 F.3d 119 (2d Cir. 2005). Underlying this split concerning whether a person who acquires a copy of a computer program is an owner or a licensee of the copy is an even more profound split concerning preemption of contract terms inconsistent with the Copyright Act. *Compare Bowers v. Baystate Techs., Inc.,* 320 F.3d 1317 (Fed. Cir.), *cert. denied*, 539 U.S. 928 (2003) (holding that the Copyright Act does not preempt contractual terms prohibiting actions permitted under fair use), with *Vault Corp. v. Quaid Software Ltd.,* 847 F.2d 255 (5th Cir. 1988) (holding that under the Supremacy

[5] http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Third_Party_Maintenance_Services_FAQ.pdf. Cisco further suggests these resellers "may sell equipment that purports to be "Cisco Product" but is in fact non-genuine or counterfeit." HP's FAQs also discuss the fees it charges for "software license transfers" for its server software. http://www.hp.com/softwarereleases/releases-media2/slt/americas/faq.html#12.

Clause of the U.S. Constitution, contract terms prohibiting copyright exceptions are unenforceable).[6]

Congress previously dealt with a similar issue in the context of software rental. In 1990, when Congress was considering amending the Copyright Act to prohibit the rental of software because it facilitated infringement by consumers, companies that rented cars and other equipment that contained software expressed concern that the amendment could prevent these rentals. Accordingly, Congress added an exception to the software rental prohibition that applies to "a computer program which is embodied in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product." 17 U.S.C. § 109(b)(1)(B)(i).

Preserving the resale rights of consumers of physical products that contain software is important for reasons that go beyond the protecting the economic interests of these consumers and the secondary market consumers who would purchase these products. If the manufacturer refuses to provide to the secondary market consumer the security patches it provides to the original consumer, the security of the secondary consumer's computer system could be compromised.[7] Such security patches typically are provided to the original consumer free of charge. In essence, the original purchase price entitles the consumer to receive security patches and other patches that fix bugs in the program.

Preserving a secondary market in these physical products is also important for the environment. If older products can be refurbished and resold, those products stay out of landfills. Moreover, the recycling of the older products reduces the need to mine raw materials and produce new components.

---

[6] This issue is discussed in great detail in Section I.D. below.

[7] Cisco's FAQ makes clear that a reseller "is not authorized to provide you with Cisco bug fixes, patches, and updates."

We recognize that the problem of restrictions placed on software essential to the operation of hardware implicates complex issues of legal theory at the intersection of Constitutional preemption, the Copyright Act, antitrust law, and contract law.[8] Nonetheless, this is a very concrete practical problem of manufacturers attempting to leverage the copyright in a component into perpetual control over a much larger device. At present, primarily manufacturers of computer and telecommunications equipment misuse software license agreements to interfere with resale. Yet as the Internet of Things continues to grow and to encompass more software-enabled products, this problem will become more widespread.

### C. The Solution: YODA

We believe that this problem can be addressed by a relatively simple amendment to the Copyright Act, such as the You Own Devices Act (YODA), H.R. 862. YODA, introduced Congressmen Blake Farenthold (R-TX) and Jared Polis (D-CO), solves this problem by adding a new subsection to section 109 of the Copyright Act, which contains the first sale doctrine. New subsection (f)(1) would provide that if a computer program enables any part of a machine or other product to operate, the owner of the machine is entitled to transfer the computer program when he sells or otherwise transfers the machine. This right to transfer the program cannot be waived by license or other agreement.

New subsection (f)(2) would provide that the purchaser of the machine is entitled to receive any bug patches or security fixes that the person who sold him the machine was entitled to receive from the manufacturer.

[8] These are discussed in Section I.D. below.

New subsection (f)(3) would make clear that nothing in this subsection allows the seller of the machine to retain an unauthorized copy of the computer program after he transfers the machine to the purchaser.

YODA is not retroactive; it would apply only to transfers of software that occur after its enactment. YODA thus appropriately balances the interests of the original equipment manufacturer, the reseller, and the consumer.

### D. The Enforceability of Contractual Restrictions on Copyright Exceptions

The alternative to YODA is to allow the courts to sort out the complex and unresolved issue of the enforceability of contractual terms limiting copyright exceptions. There is little doubt that a restriction contained in a negotiated agreement between parties of equal bargaining strength would be enforceable. But what about a non-negotiated agreement between parties of unequal bargaining position?

#### 1. Enforceability under state contract law

Some courts have viewed this issue as a matter of state contract law: has the licensee truly manifested assent to the agreement? Because a user cannot use a program without "agreeing" to these license terms either by opening the package or clicking the "I agree" icon, significant questions arise whether the user has in fact manifested assent to the license's terms. Courts around the country have considered the enforceability of shrink-wrap and click-on licenses for two decades, but a consensus has not yet emerged.[9] Moreover, numerous

[9] *Compare Novell, Inc. v. Network Trade Ctr., Inc*., 25 F. Supp. 2d 1218, 1230 (D. Utah 1997); *Morgan Labs., Inc. v. Micro Data Base Sys., Inc*. 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997); *Arizona Retail Sys., Inc. v. The Software Link, Inc*., 831 F. Supp. 759, 764-66 (D. Ariz. 1993); *Step-Saver Data Sys. v. Wyse Tech*., 939 F.2d 91, 98-100 (3d Cir. 1991); *Foresight Resources Corp. v. Pfortmiller*, 719 F. Supp. 1006, 1010 (D. Kan. 1989); *Ticketmaster Corp. v. Tickets.com, Inc*., 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. August 10, 2000), *aff'd*, 248 F. 3d 1173 (9th Cir. 2001); *Specht v. Netscape Communications Corp*., 306 F.3d 17 (2d Cir. 2002); *Softman Prods.*

commentators have questioned the enforceability of such contracts.[10] If the contracts are not enforceable, then obviously their terms prohibiting fair use and other user rights have no effect.

To the extent any pattern can be discerned in these cases, courts seem more willing to enforce click-on licenses than browse-wrap or shrink-wrap licenses, largely because it is difficult for a licensee to argue that he did not manifest assent when he clicked on an "I agree" icon. Additionally, courts seem more willing to enforce these licenses against corporate licensees than against consumers, presumably because they feel that corporate licensees are better able to protect their interests.

### 2. Preemption

Other courts have examined this question from the perspective of preemption – either preemption under Section 301(a) of the Copyright Act or the U.S. Constitution. With both theories, courts are split on whether contractual restrictions on copyright exceptions are preempted.

#### a. Section 301(a) Preemption

Courts have interpreted Section 301(a) as not preempting a state cause of action that requires proof of "extra elements" not present in a copyright claim. The Seventh Circuit in

---

*Co. v. Adobe Systems, Inc*., 171 F. Supp. 2d 1075 (C.D. Cal. 2001); and *Klocek v. Gateway, Inc*., 104 F. Supp. 2d 1332, 1338-39 (D. Kan. 2000); *with ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996), *Register.com, Inc., v. Verio, Inc*., 356 F.3d 393 (2d Cir. 2004); *cf. Hill v. Gateway 2000, Inc*., 105 F.3d 1147, 1150 (7th Cir. 1997), *cert. denied*, 522 U.S. 808 (1997).

[10] *E.g.*, Michael J. Madison, *"Legal Ware": Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV.1025 (Dec. 1998); Robert J. Morrill, Comment, *Contract Formation and the Shrink Wrap License: A Case Comment on ProCD, Inc. v. Zeidenberg*, 32 NEW ENG. L. REV. 513, 537-50 (1998); Apik Minassian, *The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements*, 45 UCLA L. REV. 569 (1997); Christopher L. Pitet, Comment, *The Problem With "Money Now, Terms Later": ProCD, Inc. v. Zeidenberg and the Enforceability of "Shrinkwrap" Software Licenses*, 31 LOY. L.A. L. REV. 325 (1997); L. Ray Patterson & Stanley W. Lindberg, *The Nature of Copyright: A Law of Users' Rights,* 220 (1991).

*ProCD, Inc. v. Zeidenberg*[11] ruled that Section 301(a) did not preempt enforcement of a contract prohibiting the copying of telephone listings because the contract claim required proof of an extra element -- the existence of an enforceable contract.

However, in *Data General Corp. v. Grumman Systems Support Corp.*,[12] the First Circuit noted that not every extra element will establish a qualitative variance between rights under copyright and those protected by state law. Thus, if the extra elements are "illusory … mere labels attached to the same odious business conduct," then preemption will occur. Likewise, some scholars have rejected the *ProCD* analysis:

> [A]t times a breach of contract cause of action can serve as a subterfuge to control nothing other than the reproduction, adaptation, public distribution, etc. of works within the subject matter of copyright. That situation typically unfolds when the "contract" at issue consists of a "shrinkwrap license" to which the copyright owner demands adhesion as a condition to licensing its materials. To the extent that such a contract is determined to be binding under state law, then that law may be attempting to vindicate rights indistinguishable from those accorded by the Copyright Act. Under that scenario, the subject contract cause of action should be deemed pre-empted .... Although the vast majority of contract claims will presumably survive scrutiny ... nonetheless pre-emption should strike down claims that, although denominated "contract," nonetheless complain directly about the reproduction of expressive materials.[13]

Relying on this passage, the court in *Selby v. New Line Cinema*[14] declined to enforce an implied-in-fact contract prohibiting the use of an idea without attribution. Similarly, the court in *Symantec Corp. v. McAffee Associates*[15] declined to enforce a contractual restriction on reverse engineering. The court found that the mere existence of the agreement was insufficient to

---

[11] 86 F.3d 1447 (7th Cir. 1996).
[12] 36 F.3d 1147 (1st Cir. 1994).
[13] 1 Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT, § 1.01[B][1][a] at 1-19 and 1-22 (2001) (citations omitted).
[14] 96 F. Supp. 2d 1053 (C.D. Cal. 2000).
[15] 1998 WL 740798 (N.D. Cal. June 9, 1998).

transform "what essentially is a copyright infringement claim" into "something more."[16] *See also Ass'n for Info. Media and Equip. v. Regents of the Univ. of California*, No. 2:10-CV-09378-CBM, 2012 WL 7683452 (C.D. Cal. Nov. 20, 2012).

**b. Constitutional Preemption**

Courts have also preempted contractual terms on Constitutional grounds. In 1988, the U.S. Court of Appeals for the Fifth Circuit set aside a contractual restriction on reverse engineering in *Vault Corp. v. Quaid Software Ltd*.[17] The *Vault* court cited *Sears, Roebuck & Co. v. Stiffel Co*.,[18] where the Supreme Court relied on the U.S. Constitution's Supremacy Clause to conclude that "[w]hen state law touches upon an area of [the copyright statutes], it is 'familiar' doctrine' that the federal policy 'may not be set at naught, or its benefits denied' by state law."[19] The *Vault* court held that a reverse engineering prohibition in a shrinkwrap license "conflicts with the rights of computer program owners under Section 117 and clearly 'touches upon an

---

[16] *Id.* at *5. *See also Kabehie et al., v. Zoland, et al.,* 125 Cal. Rptr. 721 (Cal.App.2nd Dist. 2002):

> The cases that have decided the issue of federal copyright preemption of state breach of contract causes of action can be roughly divided into two groups: (1) a minority of the cases hold state breach of contract causes of action are never preempted by federal copyright law; and (2) a majority of the cases hold state breach of contract actions are not preempted by federal copyright law when they seek to enforce rights that are qualitatively different from the exclusive rights of copyright. …. We adopt the majority view.… The promise alleged to have been breached in a breach of contract action does not always make the contract action qualitatively different from a copyright infringement action. If the promise was simply to refrain from copying the material or infringing the rights protected by copyright, then the promisor has promised nothing more than that which was already required under federal copyright law. The promise not to infringe adds nothing to a breach of contract action for copyright infringement. A breach of contract action based on this type of promise must be preempted in order to prevent parties from circumventing federal copyright law and nullifying the preemption provided for in section 301.

[17] 847 F.2d 255 (5th Cir. 1988).

[18] 376 U.S. 225 (1964).

[19] *Sears*, 376 U.S. at 229 (citations omitted).

area' of federal copyright law."[20] Likewise, the Supreme Court relied on the Supremacy Clause to preempt a Florida plug mold statute it found inconsistent with the federal intellectual property system.[21]

On the other hand, the courts in *Bowers v. Baystate Techs., Inc.*[22] and *Davidson & Assoc. v. Jung*[23] rejected constitutional preemption arguments with respect to contractual restrictions on copyright exceptions. Judge Dyk, however, wrote a powerful dissent in *Bowers*, stating that a software firm could not eliminate a user's privileges under the Copyright Act simply "by printing a few words on the outside of its product…."[24] Such an approach "permits state law to eviscerate an important federal copyright policy reflected in the fair use defense…."[25]

**3. Copyright Misuse**

The courts could also employ the copyright misuse doctrine to address manufacturers' attempts to use their copyright in the software embedded in networked products to prevent resale of those products. The misuse doctrine prohibits the enforcement of a copyright for the purpose of preventing legitimate competition—here, by resellers of legitimate products.

The Fourth Circuit in *Lasercomb America v. Reynolds*, 911 F.2d 970, 977 (4th Cir. 1990), found that the copyright misuse doctrine is premised on the principle that public policy "forbids the use of the [copyright] limited monopoly to secure an exclusive right or limited monopoly not granted by the [Copyright] Office and which is contrary to the public policy to grant." In *Lasercomb*, the plaintiff's standard software license prohibited the licensee from developing competing software for 99 years. This prohibition went beyond any reasonable need to protect

---

[20] *Vault*, 847 F.2d at 270.
[21] *Bonito Boats Inc., v. Thunder Craft Boats Inc.*, 489 U.S. 141 (1989).
[22] *Bowers v. Baystate Techs., Inc.,* 320 F.3d 1317 (Fed. Cir.), *cert. denied*, 539 U.S. 928 (2003).
[23] 422 F.3d 630 (8th Cir. 2005).
[24] 320 F.3d at 1337 (Dyk, J., dissenting).
[25] *Id*. at 1335.

Lasercomb's own software, and was directed at limiting competition from independently developed, non-infringing software. Lasercomb, by the terms of its copyright license agreement, was attempting to monopolize something which clearly was not part of the bundle of rights granted by copyright: the right to develop competing software utilizing the same ideas. Because Lasercomb used its copyright to force Reynolds to agree to these anticompetitive license terms, the court excused Reynold's copying of the Lasercomb's software.

Similarly, in *DSC Communications Corp. v. DGI Technologies, Inc.*, 81 F.3d 597, 601 (5th Cir. 1996), the Fifth Circuit found copyright misuse when DSC used its copyright to gain control over a competitor's use of its microprocessor cards. DGI developed microprocessor cards that could be used on DSC's phone switches. To ensure that the cards were compatible with the DSC's phone switch operating system, DGI had to test its card on a DSC phone switch. Such a test necessarily made a copy of DSC's operating system in the memory of DGI card when the card was "booted up." DSC sued DGI for infringing the copyright in its operating system. The Fifth Circuit found that "if DSC is allowed to prevent such copying, then it can prevent anyone from developing a competing microprocessor card, even though it has not patented the card." *Id*. at 601. The court observed that "DSC seems to be attempting to use its copyright to obtain a patent-like monopoly over unpatented microprocessor cards." *Id*. Quoting *Lasercomb*, the Fifth Circuit held that copyright misuse doctrine "forbids the use of a copyright to secure an exclusive right or limited monopoly not granted by the Copyright Office." *Id*.

Likewise, the Ninth Circuit in *Practice Management Information Corporation v. American Medical Association*, 121 F.3d 516 (9th Cir. 1997), found that the AMA misused its copyright when it negotiated a contract with the Health Care Financing Administration under which AMA licensed its coding system to HCFA in exchange for HCFA agreeing not to use any

other coding system. When publisher PMI could not reach an agreement with AMA to republish the coding system, PMI filed a declaratory judgment action, seeking a declaration that AMA's copyright was invalid because AMA had misused it. The Ninth Circuit agreed with PMI:

> What offends the copyright misuse doctrine is not HCFA's decision to use the AMA's coding system exclusively, but the limitation imposed by the AMA licensing agreement on HCFA's rights to decide whether or not to use other forms as well. Conditioning the license on HCFA's promise not to use competitors' products constituted a misuse of the copyright by the AMA.

*Id*. at 519.

The district court in the complex litigation between Omega and Costco likewise found that Omega misused its copyright. Costco, the discount retailer, sold luxury Omega watches without the authorization of the Swiss watchmaker. In an effort to prevent Costco from importing and selling its watches, Omega began engraving an "Omega Globe" logo on the back of its watches. When Costco started importing and selling the watches bearing the logo, Omega sued Costco for infringing the importation right under the Copyright Act. Costco responded that the importation right was a subset of the distribution right, and that the first sale doctrine provided it with an exception to the distribution right. The first sale doctrine provides that the distribution right with respect to any particular copy of a work extinguishes with the first authorized sale of that copy. 17 U.S.C. § 109(a). The district court granted summary judgment in favor of Costco on the basis of the first sale doctrine. The Ninth Circuit reversed, finding that the first sale doctrine did not apply to copies manufactured outside of the United States. Costco appealed to the Supreme Court. With Justice Kagan recusing herself, the Supreme Court in 2010 reached a 4-4 tie.

On remand, the district court once again granted summary judgment to Costco, this time on a copyright misuse theory. *Omega S.A. v. Costco Wholesale Corp*., 2011 WL 8492716 (C.D.

Cal. 2011). It noted that the Ninth Circuit held that "the misuse defense prevents copyright holders from leveraging their limited monopoly to allow them to control areas outside of their monopoly." *A&M Records, Inc. v. Napster, Inc*., 239 F.3d 1004, 1026 (9th Cir. 2001). The district court found that Omega misused its copyright in the logo "by leveraging its limited monopoly in being able to control the importation of that design to control the importation" of its watches. The district court also awarded Costco $396,000 in attorneys' fees.

Omega appealed the misuse finding and the fee award to the Ninth Circuit. While the case was pending before the Ninth Circuit, the Supreme Court handed down its decision in *Kirtsaeng v. John A. Wiley & Sons*. In that 2013 decision, the Supreme Court held that the first sale doctrine applied to noninfringing copies, regardless of where they were manufactured. In other words, the Supreme Court in *Kirtseang* agreed with the district court's original decision in favor of Costco.

In January 2015, the Ninth Circuit finally ruled on Omega's appeal of the district court's 2011 decision. *Omega S.A. v. Costco Wholesale Corp*., 776 F.3d 692(9th Cir. 2015). Because the Supreme Court's *Kirtsaeng* holding provided Costco a complete defense to the Omega's infringement claim, the Ninth Circuit did not reach the district court's misuse holding. It did, however, affirm the award of attorneys' fees to Costco. The Ninth Circuit noted that the district court had observed that Omega had not sought to provide creative works to the general public. Rather, Omega sought to exert control over the distribution of its watches. The Ninth Circuit held that the district court had not erred when it concluded that "it should have been clear to Omega that copyright law neither condoned nor protected its actions, and the imposition of fees would thus further the purpose of the Copyright Act."

Of particular relevance here is Judge Wardlaw's concurring opinion, where she argued that the panel should have affirmed the district court's copyright misuse finding rather than decide the case on the basis of *Kirtsaeng*. Judge Wardlaw agreed with the district court that "Omega impermissibly used the defensive shield of copyright as an offensive sword."

In the closing paragraph of her concurrence, Judge Wardlaw stated that Omega's attempt to expand the scope of its statutory monopoly by misusing its copyright in its logo would upset the balance the copyright law establishes between rewarding creative work and promoting the broad public availability of literature, music, and the other arts. Omega's "anticompetitive acts promoted neither the broad public availability of the arts nor the public welfare." Rather, they were designed to eliminate price competition in the retail market for Omega watches and deprive consumers of the opportunity to purchase discounted gray market Omega watches from Costco.

The elimination of price competition from the sale of used products is exactly what manufacturers are attempting to do through their restrictions on the resale of the software embedded in their products. Courts may well conclude that such practices constitute misuse.

**4. YODA Is A Better Approach**

Rather than force resellers and consumers to spend decades in the courts resolving these thorny issues of preemption and misuse, Congress should adopt targeted legislation such as YODA. It bears emphasis that permitting the transfer of software-enabled products would not lead to the unauthorized copying of the software. The product already contains the software, there typically are technological protections that inhibit the copying of the software, and the software usually has no independent economic value. Accordingly, resale of software-enabled products does not facilitate software "piracy."

## II. PREVENTING THE DMCA FROM UNDERMINING THE INTERNET OF THINGS

As currently drafted, section 1201 of the Digital Millennium Copyright Act (DMCA) interferes with the rights of owners of products whose operation is enabled by software—the products that make up the Internet of Things. This was clearly demonstrated in the last rulemaking cycle, where the majority of the 27 proposed exemptions addressed situations far from Congress's intended target of online infringement when it adopted the DMCA in 1998. This indicates that Congress drafted the DMCA far too broadly, and that the Copyright Office is implementing the exemption process far too narrowly. The DMCA must be recalibrated so that it does not interfere with the emergence of the Internet of Things.

### A. Section 1201's Overbreadth

In an effort to protect the economic interests of copyright owners in the digital age, Congress prohibited the circumvention of technological protection measures (TPMs) in order to get unpaid access to copyrighted works. However, the DMCA is worded so broadly as to prohibit owners of copies of works from circumventing the TPMs limiting access to their own copies. Manufacturers of a wide range of devices have exploited this overbreadth to exercise after-market control over the devices in a manner that has nothing to do with copyright protection. Many devices include software essential to their operation. Manufacturers have placed TPMs on this software in an effort to tether the device to complementary networks or products. The DMCA makes unlawful the circumvention of these TPMs for the purpose of untethering the devices.

Congress recognized that there may be legitimate reason for circumventing TPMs, so it authorized the Librarian of Congress to conduct a rulemaking every three years to adopt appropriate exemptions to the DMCA's circumvention prohibition. In this last rulemaking cycle, 14 of the 27 proposed exemptions concerned situations where the work protected by the TPM is

a software component of a hardware device owned by the user. In other words, the exemption would allow the owner of a hardware product to make a use of her personal property obstructed by the DMCA.

Five of the proposed exemptions involved the "unlocking" of different kinds of devices so as to connect them to an alternate wireless network. The devices included telephone handsets, tablet computers, wearable computing devices, mobile connectivity devices, and consumer machines such as smart meters.

Another five of the proposed exemptions involved the "jailbreaking" of devices so that they can access alternate lawful content. The devices included telephone handsets, all-purpose mobile computing devices, dedicated e-book readers, video game consoles, and smart televisions.

Two of the proposed exemptions involved vehicle software. One exemption would permit the circumvention of TPMs on software that controls the function of motorized land vehicles for the purpose of diagnosis and repair, or after-market personalization. A second exemption would allow the circumvention of the TPMs on such software for the purpose of researching the safety or security of the vehicles.

The final two proposed exemptions would enable the use of alternative feedstock for 3D printers and research into the safety, security, and effectiveness of medical devices.

Fortunately, the Librarian granted these all exemptions, at least in part, with the exception of the proposed exemption for the jailbreaking of dedicated e-book readers. Where the Librarian granted an exemption, he recognized that the enabled uses would be lawful, and that the granting of these exemptions would not facilitate widespread infringement.

However, as a policy matter, it makes no sense to force all those who desire to unlock devices with embedded software to apply for a device-specific exemption every three years. Congress did not enact the DMCA to prevent these sorts of uses; it did not intend to restrict owners of hardware products from making full use of their personal property. To be sure, in certain specific situations there may a governmental interest in limiting access to the embedded software, *e.g*., to prevent tampering with safety technologies. But in such situations, the government should adopt appropriate regulations, rather than rely on the sweeping effect of the DMCA.

The source of the problem is the wording of the prohibition on circumvention in Section 1201(a). The Federal Circuit interpreted Section 1201(a) as requiring a nexus between circumvention and infringement before circumvention liability could attach. In *Chamberlain v. Skylink*, 381 F.3d 1178 (Fed. Cir. 2004), the Federal Circuit found that the circumvention of the TPM on the software in a garage door opener motor by the manufacturer of universal garage door opener remote controls did not violate the DMCA because there was no possibility of infringement. The Sixth Circuit concurred with this interpretation in *Lexmark v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004). However, the Ninth Circuit rejected this approach in *MDY v. Blizzard,* 629 F.3d 928 (9th Cir. 2010). Judge Donald's dissent in *U.S. v. Reichert*, 747 F.3d 445 (6th Cir. 2014), discussed these "competing interpretations" of Section 1201(a) at length.

Because the Supreme Court is unlikely to resolve this circuit split in the near future, in may be necessary for Congress to amend the DMCA to explicitly require a nexus between circumvention and infringement, as in *Chamberlain*. Alternatively, it could adopt a permanent exception for the circumvention of TPMs on software essential to the operation of hardware.

### B. The 1201 Rulemaking

Until Congress or the Supreme Court addresses this issue, NTIA should urge the Copyright Office to take a more pragmatic approach toward exemptions for software components of hardware products. For example, the Copyright Office could recommend that the Librarian of Congress grant a broad exemption for all software essential to the operation of hardware in the lawful possession of the user. Regrettably, in the past rulemaking cycle the Copyright Office went in the opposite direction, drawing up classes as narrowly as possible. For the unlocking of devices from wireless networks, the Copyright Office identified five separate classes for five different kinds of devices. It did the same for jailbreaking. For vehicle software, the Copyright Office considered only land vehicles, when the same issue obviously will apply to boats and aircraft.

By Balkanizing the essential software problem in this manner, the Copyright Office places a much greater burden on the applicants of each narrow class to meet the preponderance of the evidence standard the Office imposes. Section 1201(a)(1)(C) certainly does not require the identification of such narrow classes.

Another problem is that the Copyright Office requires anyone who wants to extend an exemption for an additional three-year period to prove her case all over again, or the exemption will lapse. Section 1201(a)(1)(C), however, does not expressly require such *de novo* evaluation. The statute is broad enough to allow a rebuttable presumption that an exemption should be renewed. A presumption in favor of renewal would certainly lessen the burden of the rulemaking process on resellers and end-users seeking an exemption related to software-enabled products. Several of the exemptions, including for jailbreaking and device unlocking, have been renewed multiple times, underscoring the inefficiency of the Copyright Office's *de novo* rulemaking

approach. Of course, copyright owners would have the opportunity to introduce new evidence arguing against renewal.

## III. CONCLUSION

In the green paper it develops subsequent to this request for comments, NTIA must carefully consider the adverse impact copyright law may have on the development of the Internet of Things. As discussed above, manufacturers can use their copyright in the software contained in products that connect to the Internet of Things to restrict the resale of the products. Further, manufacturers can use the DMCA to restrain how an owner uses her software-enabled product, including what apps she can install, to what networks she can connect, and her freedom in customization and repair. Unless amended, title 17 has the potential of crippling the development of the Internet of Things.