Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 33 | Issue 1

Article 1

10-6-2016

The Internet of Things: Where Privacy and Copyright Collide

Lidiya Mishchenko

Recommended Citation

Lidiya Mishchenko, *The Internet of Things: Where Privacy and Copyright Collide*, 33 Santa Clara High Tech. L.J. 90 (2016).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol33/iss1/1

THE INTERNET OF THINGS: WHERE PRIVACY AND COPYRIGHT COLLIDE

Lidiya Mishchenko[†]

Our Internet of Things ("IoT") devices are constantly monitoring our every move, collecting sensitive data about us in a way that we do not fully appreciate. Manufacturers of these devices have a huge financial incentive to collect as much data on us as they can, and to use and sell this data in its most identifiable form. Yet our privacy regulations currently provide no real checks on how data is collected and used by these companies. Furthermore, the Digital Millennium Copyright Act ("DMCA") actually creates a substantial roadblock in this instance, preventing users and the government from ever finding out what data is collected and how it used by device manufacturers. To create some transparency in this system, the DMCA should be amended to include a limited circumvention exception for privacy. The proposed exception attempts to incentivize above-board behavior by device manufacturers, while allowing the government's chief privacy agency, the Federal Trade Commission ("FTC"), to have at its disposal the tools and resources required to investigate improper practices. Under this proposal, the FTC can help create binding industry standards for data collection and dissemination, aligning the DMCA with the goals in our privacy regulations and filling in the regulatory gaps our current privacy laws leave for IoT device manufacturers.

[†] J.D., 2016, *summa cum laude*, The George Washington University Law School, Articles Editor for *The George Washington Law Review*. Ph.D., Applied Physics, 2012, Harvard University School of Engineering and Applies Sciences. The author thanks Prof. Dawn Nunziato for her valuable input.

TABLE OF CONTENTS

INTRODUCTION

You wake up. Your wearable device tells you that you did not sleep very well. You see that your first meeting got pushed back forty-five minutes and that your alarm let you sleep an extra fifteen minutes. You walk into the kitchen where the coffee, triggered by your alarm, has already been brewed. Your fridge tells you that you're low on milk and that more has been ordered online. After breakfast, you head to your car. As you leave, the lights in your apartment go off automatically and the temperature is lowered. Your car is already warmed up enough to melt the ice off of the windshield. The car tells you how to avoid the accident on your route and reminds you to call your mom.[1]

But this idyllic world is interrupted when you arrive at work and find out, while reading an internet blog, that all the activities you have been manually inputting into your wearable device are now available online for everyone to see. Apparently, the device company has made such data public by default. Some of those activities you input were sexual in nature. This has quickly turned into a nightmare—your boss reads the same blog! And unfortunately, this last part of the story is

[1] This example is loosely based on Cisco's Blog post from 2011. *See* Dave Evans, *The internet of Things*, CISCO BLOG (July 15, 2011), http://bit.do/CiscoIoT.

not science fiction. In 2011, Fitbit users found out that the sexual activity records of approximately 200 customers were showing up in Google search results.[2] Fitbit quickly remedied the problem, but no one can really erase the embarrassment those users must have felt.

We live in a world surrounded by devices that monitor our every move. These devices can connect to the internet and thus coordinate with one another, creating the Internet of Things ("IoT").[3] They provide enormous benefits and efficiency, but they also completely shift our concept of privacy. Wearable devices in particular raise new privacy concerns. Senator Chuck Schumer warned that wearable devices such as Fitbit are "a privacy nightmare" because they collect such sensitive information as GPS location and sleep patterns, which can then be sold to third parties.[4]

Fitbit has in the past responded to scandals in a timely fashion. On the same day as Senator Schumer's statement, Fitbit updated its privacy policy stressing that the company does not sell data that can be used to identify its users.[5] Chuck Schumer responded by saying that Fitbit is doing "exactly the right things" with its updated privacy pledge.[6] Despite Chuck Schumer's retreat and Fitbit's expedient response, Fitbit and wearable devices like it may still pose a "privacy nightmare" for consumers. Although the company has revised its privacy policy, explaining that it only "share[s] or sell[s] aggregated, de-identified data that does not identify you," there is still plenty of room for concern. Fitbit collects all sorts of data—some data you provide yourself and other data the device measures on its own, e.g., with accelerometers.[7] Fitbit devices collect data about your location, the number of steps you take, your weight, height, gender, and how you sleep.[8] This type of data can be used to figure out, for example, your gait, which is completely unique to you, when you take the bus or ride a bike,[9] your mood,[10] or if you might be pregnant (sometimes,

[2] Kashmir Hill, *Fitbit Moves Quickly After Users' Sex Stats Exposed*, FORBES (July 5, 2011), http://bit.do/ForbesFitbitStatsExposed.

[3] Scott R. Peppet, *Regulating the internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88–89 (2014).

[4] Lance Duroni, *Fitbit Doing 'Right Thing' With Privacy Policy, Schumer Says*, LAW360 (Aug. 25, 2014), http://bit.do/FitbitRightThing.

[5] *Id.*

[6] *Id.*

[7] *Privacy Policy*, FITBIT (Dec. 9, 2014), http://bit.do/FitbitPrivacyPolicy; *Fitbit Help: How does my tracker count steps?,* FITBIT (Oct. 26, 2015), http://bit.do/FitbitHelpTrackerCount.

[8] *Fitbit Help, supra* note 7.

[9] Peppet, *supra* note 3, at 129–30.

[10] *Id.* at 115.

even before you know).[11] This data is invaluable, both to companies like Fitbit, and to third parties that buy such data.[12] And there is a strong incentive for Fitbit not to aggressively de-identify its data: the less anonymous the data is, the more valuable it is.[13]

For example, imagine Fitbit sells only your accelerometer data to a third party. Even if Fitbit removes all "identifying information," such as your name and address, a company may still be able to couple this data with other publicly-available data, like your public social media profiles, to identify you. Many entities such as insurance companies, advertisers, and possibly even your future employers have incentives to re-identify de-identified data.[14] Even techniques such as data aggregation, depending on how it is accomplished, can allow for re-identification.[15]

What happens if you try to find out what data is being collected, or if it is accurate? Fitbit is better than most companies in that sense—it lets you export your fitness data and says "[y]ou own your data."[16] But what about your Fitbit's raw accelerometer data, which, for example, allows for identification of your unique gait pattern? Fitbit doesn't allow you to access this output data.[17] In some ways, your Fitbit, and other wearable devices, are black boxes. You don't know what's being collected or how that data is being analyzed, aggregated, or sold.

The "nightmare" doesn't end there. Not only are there concerns that wearable devices like Fitbit may evade current privacy regulations,[18] copyright law poses an additional obstacle to transparency. The data and software of wearable devices are protected

[11] *See* Amanda Jackson, *Husband and wife never expected their Fitbit would tell them this ...,* CNN (Feb. 11, 2016), http://bit.do/FitbitPregnancy.

[12] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE FTC REP. 38 (2012), http://bit.do/FTCProtectingConsumer [hereinafter 2012 FTC REPORT] (discussing the fact that restricting data collection "risk[s] undermining companies' incentives to innovate and develop new products and services to consumers").

[13] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) ("Data can be either useful or perfectly anonymous but never both.").

[14] *See* Salvador Ochoa, Reidentification of Individuals in Chicago's Homicide Database: A Technical Legal Study (May 5, 2001) (unpublished student paper, M.I.T.), http://bit.do/ReidentificationIndividuals (listing motives for identification).

[15] Ohm, *supra* note 13, at 1756.

[16] *Fitbit Help: Can I export my fitness data to my computer?,* FITBIT (Mar. 2, 2016), http://bit.do/FitbitHelpExportData.

[17] Dan Chen, *Product Development: Web API: Get the raw accelerometer data*, FITBIT COMMUNITY DISCUSSION FORUM (July 17, 2014), http://bit.do/FitbitCommunityRawData.

[18] Peppet, *supra* note 3, at 117–47 (discussing unique privacy regulation problems that IoT devices present).

by technological protection measures (“TPMs”).[19] These TPMs are often used by companies to protect user privacy, but are also used to protect the company’s intellectual property,[20] and may even be used by companies to limit consumer choice in the aftermarket,[21] or even to hide wrongdoing.[22] The Digital Millennium Copyright Act (“DMCA”) generally makes it illegal to circumvent these TPMs.[23] Thus, Fitbit could theoretically sue you for hacking one of their devices, even if you were only trying to figure out what the device was measuring and what data was being stored.

Given the enormous financial incentive for Fitbit and other IoT device companies to collect, use, and sell our personal data, we need some way of making sure these companies are protecting our privacy. This article proposes a revised privacy circumvention exception to the DMCA that may help keep these companies in line. Part I of this article explains the current legal shortcomings with regulating the IoT in the privacy space. Part II details how the DMCA and copyright further inhibit our ability to regulate IoT devices. It also explains how the DMCA currently addresses privacy. Part III discusses the proper place for the DMCA in the privacy space and proposes legislative amendments to the DMCA that would improve our ability to regulate how IoT devices collect and use our personal data.

[19] *Terms of Service*, FITBIT (Oct. 28, 2015), http://bit.do/FitbitTOS (discussing “technological measure[s] implemented by Fitbit or any of Fitbit’s providers … to protect the Fitbit Service or Fitbit Content”).

[20] Darin Bartholomew, Deere & Co., *Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, COPYRIGHT OFFICE 2 (Mar. 3, 2016), http://bit.do/CommentJohnDeere [hereinafter John Deere Comment] (“For example, in the absence of TPMs third-party software developers could purchase vehicles to access instantly copyrighted, safe and regulatory-compliant software that is the result of years of extensive research and development by manufacturers and suppliers.”).

[21] *EFF Wins Petition to Inspect and Modify Car Software*, ELECTRONIC FRONTIER FOUNDATION (Oct. 27, 2015), http://bit.do/EFFWinsPetition; Declan McCullagh, *Lexmark invokes DMCA in toner suit*, CNET (Jan. 9, 2003), http://bit.do/LexmarkInvokesDCMA (“Printer maker Lexmark has found an unusual weapon to thwart rivals from selling replacement toner cartridges: the Digital Millennium Copyright Act.”).

[22] James Grimmelmann, *Harry Potter and the Mysterious Defeat Device*, SLATE (Sept. 22, 2015), http://bit.do/VolkswagenEmission (“[T]ech companies try to use copyright threats under the DMCA to shut it down, keeping the security community in the dark about vulnerabilities in the devices we use every day.”).

[23] 17 U.S.C. § 1201(a)(1)(A) (“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”).

I. PRIVACY AND THE INTERNET OF THINGS

A. The Reidentification Problem

U.S. privacy regulation is built on the belief that data anonymization—removal of personally identifying information ("PII") such as someone's name, address, social-security number, or telephone number[24]—ensures privacy.[25] U.S. federal and state laws carve out exceptions for entities that anonymize data.[26] However, recent commentators have pointed out that technology and reidentification science have progressed to the point that anonymization alone can no longer protect privacy.[27] With the advent of computers and the internet, more information is publicly available than ever before. With new reidentification techniques, seemingly-unrelated online datasets can be linked together to bring an adversary closer to identifying you and information about you.[28] An adversary[29] can now use information "nobody would classify as personally identifiable" to link data to your identity.[30]

For example, when Netflix, the movie streaming and rental company, decided to publish anonymous movie ratings of its users as part of a competition to improve its recommendation algorithm,[31] no one was too concerned about privacy. However, only two weeks after the release, researchers discovered that they could use public movie ratings on IMDB, coupled with Netflix's published data, to identify users in the anonymized Netflix database, including movie preferences these users probably did not want publicized.[32] The researchers also explained that, with only a little bit of knowledge about an individual subscriber, one could identify him or her in the database and find out all of their movie ratings.[33]

The Netflix example demonstrates that researchers can find unique fingerprints in even the most innocuous data sets, and can combine two or more sets of "anonymized" data to identify people

[24] Peppet, *supra* note 3, at 131.

[25] Ohm, *supra* note 13, at 1703–04.

[26] *Id.*

[27] *Id.* at 1704.

[28] *Id.* at 1749.

[29] *Id.* at 1707–08 ("A person, known in the scientific literature as an adversary, reidentifies anonymized data by linking anonymized records to outside information, hoping to discover the true identity of the data subjects.").

[30] *Id.*

[31] Ohm, *supra* note 13, at 1720.

[32] *Id.* at 1722.

[33] *Id.* at 1721.

with surprising precision.[34] All reidentification events, no matter how seemingly trivial, increase the linkability of data, exposing people to potential future harm.[35] With the rise of blogs and social media, "[n]ever before in human history has it been so easy to peer into the private diaries of so many people."[36] The combination of the availability of the information, the ease of reidentification,[37] and the great financial incentive to reidentify,[38] means that most techniques of data anonymization—which simply remove personally identifying information ("PII")—are doomed to fail.[39]

B. IoT Devices Pose Even Greater Risks

Sensor-based IoT devices exacerbate the issues addressed above. In general, sensors such as those in cars and on wearable devices enable continuous monitoring and collect a rich variety of data.[40] Most new cars in the U.S. have a "black box" that measures "a vehicle's speed, how far the accelerator pedal is pressed, whether the brake is applied, whether the driver is using a seat belt, crash details, and other information, including, in some cases, the driver's steering input and occupant sizes and seat positions."[41] Wearable sensors can collect even more sensitive information: steps taken, quality of sleep, skin temperature, breathing patterns, and heart rate, just to name a few.[42] And because these devices contain complex, multi-faceted measurement sensors such as gyroscopes and accelerometers,[43] even more sensitive information can be mined from the combination of the raw data outputs via sensor-fusion.[44] For example, researchers have found that emotional or mental states can be derived from such data.[45] The data may even be used to predict behavior and infer personal habits.[46]

But it is not just the sensitivity of the data or the continuous monitoring of IoT sensors that renders them particularly troubling. On

[34] *Id.* at 1723.

[35] *Id.* at 1746.

[36] *Id.* at 1725.

[37] Ohm, *supra* note 13, at 1731.

[38] *Id.* at 1730.

[39] *Id.* at 1732.

[40] Peppet, *supra* note 3, at 88, 91.

[41] *Id.* at 91.

[42] *Id.* at 100–01.

[43] *Id.* at 121.

[44] *Id.* at 120–21 ("Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the information is used separately.").

[45] *Id.* at 121.

[46] Peppet, *supra* note 3, at 122–23.

top of all this, reidentification is even easier for sensor data than for other types of data.[47] This is because "sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique."[48] A Fitbit's raw output data may, without more, reveal the user's gender, height, weight, and, of course, their unique gait.[49] The data would also tell you if that person is taking a bus or riding a bike.[50] If an adversary had all of Fitbit's raw data—anonymized but categorized by user—and knew just a small amount more about a specific individual from another source—for example that this person rode the bus at a specific time—they would be able to figure out which raw data matches that person, and would thus know all their other Fitbit information (i.e., all their other movements).[51]

With the enormous possibility for reidentification and the rich amount of data an adversary would have upon reidentification, it is crucial that users know what data their wearable sensors collect and how it is being used and sold. As discussed in more detail in Subsection C, if such data is used by employers or insurance companies to differentiate between individuals, it is also important that people have the ability to correct or dispute the data that is being collected.

Despite the sensitivity of the data and the increased possibility of reidentification, most IoT companies' privacy policies and consent procedures are inadequate. One commentator, Professor Scott Peppet, surveyed twenty popular IoT consumer devices, including Fitbit, and revealed some of these problems.[52] Generally, the IoT wearable devices surveyed had no means of displaying privacy notices.[53] Nor did any of the devices include privacy or data information in the box.[54] Evidently, consumers may have to rely on the website or phone app of the device to provide the privacy policy.[55] However, Peppet also found it difficult to locate the policies even from these sources.[56] In addition, when policies were finally located, they were generally

[47] *Id.* at 129. Note that IoT devices also have various data security issues that may result in *inadvertent* data leaks, *id.* at 132–39, but those are beyond the scope of this article.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Peppet, *supra* note 3, at 129–30.

[52] *Id.* at 140.

[53] *Id.*

[54] *Id.*

[55] *Id.* at 141.

[56] *Id.* at 141–42.

vague or ambiguous.[57] What constitutes personal information, what data is sold and in what form, ownership of the data, and breach notification policies were generally poorly explained.[58] Peppet also discovered that it was not usually possible to export raw data from the sensors, nor was it clear if users have modification or deletion rights, or what data is transmitted to and stored on company servers.[59] Thus, although these devices collect extremely sensitive data, which poses a greater risk of reidentification, users are often denied even the most basic explanation of what data is collected and how it is used.

C. Privacy Regulation of IoT Devices

Given the aforementioned risks with data collection by IoT devices, it is troubling to think that these devices are out of reach of most current federal privacy regulations.[60] First, U.S. privacy regulation generally focuses on whether PII is collected and disclosed by an entity.[61] Thus, an IoT device company does not have to worry about reidentification problems under current privacy laws—simply removing fields such as the name and address from their data provides them a safe harbor to sell the data to third parties.

In addition, most notice-and-consent requirements for companies rely on self-regulation, and have had only limited success due to the lack of government enforcement.[62] The Federal Trade Commission (FTC) has been getting complaints of inadequate self-regulation for some time.[63] However, the FTC cannot typically enforce proper privacy notices unless they are deceptive or the company otherwise injured consumers in ways that violate public policy.[64]

Furthermore, consumer fitness devices are not considered "medical devices," and are thus not regulated by the FDA.[65] The

[57] Peppet, *supra* note 3, at 142.

[58] *Id.* at 143–44.

[59] *Id.* at 144–45.

[60] *See, e.g.*, Ohm, *supra* note 13, at 1704.

[61] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

[62] *See* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 295 (2012) (discussing general failure of "industry disclosure schemes").

[63] *See* FTC STAFF, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, FTC STAFF REP. 24 n.104 (Jan. 2015), http://bit.do/FTCIoT2015 [hereinafter 2015 FTC REPORT] (quoting one participant as saying "That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body…."); 2012 FTC REPORT, *supra* note 12, at 27.

[64] Peppet, *supra* note 3, at 136 (discussing the jurisdictional limitations of the FTC).

[65] Heather Patterson, Contextual Expectations of Privacy in Self-Generated Health

Health Insurance Portability and Accountability Act (HIPAA) also does not apply to devices such as Fitbit because the data is not collected by "covered entities," such as health care providers.[66] Nor do these devices collect "health information" created by a health provider.[67] In addition, even if HIPAA were to somehow apply, HHS regulations provide an exemption if data is anonymized through removal of identifiers such as the name and address.[68] With the problem of reidentification addressed above, this exemption provides little consolation to users.

The Fair Credit Reporting Act (FCRA) also provides only limited protection. If IoT device manufacturers provide data to credit companies, insurance agencies, or potential employers, they would be regulated by the FCRA.[69] In this case, the device company would be classified as a "consumer reporting agency," and consumers would have the right to dispute the accuracy or completeness of any such report.[70] The FCRA still leaves a gap, however. As one commentator explains, "a lender, insurer, or employer doing its own analysis of sensor data would not trigger the FCRA's CRA-related requirements."[71] Thus, if your current or potential employer simply asked for your Fitbit data, no privacy regulation would protect your rights.[72] This is not an unrealistic hypothetical. Large employers seem to have developed a habit of collecting very sensitive data from employees, sometimes even charging fines to those who do not comply.[73] In particular, certain employers have recently started distributing Fitbits to employees, providing financial incentives for those who wear them and meet certain fitness goals.[74]

Users' inability to know what data is being collected or to challenge its accuracy has taken on even greater importance with the advent of IoT devices. At the same time, privacy regulation lags

Information Flows 20 (June 6, 2013) (unpublished manuscript, N.Y.U. MEDIA, CULTURE, & COMM. INFO. L. INST.) http://bit.do/PattersonPrivacy.

[66] *See id.* at 17; 45 C.F.R. § 160.102.

[67] 45 C.F.R. § 160.102.

[68] *Id.* § 164.514(b)(2).

[69] 15 U.S.C. § 1681a(d)(1).

[70] *Id.* § 1681i(a)(1)(A).

[71] Peppet, *supra* note 3, at 127.

[72] *Id.*

[73] *Id.* at 118 ("In March 2013, for example, CVS Pharmacy announced that employees must submit information about their weight, body fat composition, and other personal health metrics on a monthly basis or pay a monthly fine.").

[74] Parmy Olson, *Fitbit On Track To Sell Thousands More Devices Through Barclays, GoDaddy And Other Employers*, FORBES (Oct. 20, 2015), http://bit.do/ForbesFitbitSellThousands.

behind, focusing on outdated definitions of PII, relying on company self-regulation, and leaving consumers to fend for themselves with employers. Current copyright law only further muddies the waters.

II. DMCA AND IOT

A. DMCA Anti-Circumvention Provisions

Congress passed the Digital Millennium Copyright Act (DMCA)[75] in 1998 to implement the WIPO Copyright Treaty.[76] Section 1201 of the DMCA prohibits circumvention of "a technological measure that effectively controls access to a work protected under this title."[77] The Act defines circumvention as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[78] Since IoT devices often use technological measures[79] such as passwords and encryption to protect copyrightable works—the underlying software and data outputs,[80] for instance—the DMCA has direct implications for users attempting to hack their own devices.

From the plain reading of the anti-circumvention provision, it is clear that circumvention of a technological measure alone is an actionable offense, even if that circumvention does not involve copyright infringement.[81] What is less clear is whether circumventing a technological protection measure needs to have *some* relationship to copyright infringement.[82] This question is important because it determines what a plaintiff needs to show to bring a DMCA claim,[83] and the extent that device manufacturers can use copyright protections to completely control the use, repair, and alteration of their devices.[84]

[75] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[76] Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 521 (1999).

[77] 17 U.S.C. § 1201(a)(1)(A).

[78] *Id.* § 1201(a)(3)(A).

[79] *See infra* note 97.

[80] *See infra* note 100.

[81] 3-12A MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.03 (2015) ("The basic provision… is equivalent to breaking into a castle—the invasion of another's property is itself the offense…. Note that the gravamen here is not copyright infringement, but instead something that can be labeled 'paracopyright.'").

[82] Megan M. Chung, *Does Liability under the DMCA Require a Showing of Nexus to Copyright Infringement*?, 22 INTELL. PROP. LITIG. 14 (Spring 2011).

[83] *Id.*

[84] *See* Daniel C. Higgs, Lexmark International, Inc. v. Static Control Components, Inc.

Circuits have split on whether the anti-circumvention provision needs to have some connection to copyright infringement.[85] The Federal Circuit has expressed concerns that completely dissociating the DMCA from copyright infringement would have disastrous effects for users:

> Under [this regime]…, the owners of a work protected by *both* copyright *and* a technological measure that effectively controls access to that work per § 1201(a) would possess *unlimited* rights to hold circumventors liable under § 1201(a) *merely for accessing that work*, even if that access enabled *only* rights that the Copyright Act grants to the public…. In a similar vein, [this] construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products.[86]

The Sixth Circuit shares the Federal Circuit's sentiment,[87] if not its solution to the problem.[88]

The Ninth Circuit, in contrast, believes that reading an "infringement nexus"[89] into the DMCA is "contrary to the plain language of the statute" and that the Federal Circuit's policy concerns "are best directed to Congress in the first instance."[90] The Ninth Circuit explains that the DMCA § 1201(a) "creates a new anti-

& Chamberlain Group, Inc. v. Skylink Technologies, Inc.*: The DMCA and Durable Goods Aftermarkets*, 19 BERKELEY TECH. L.J. 59, 77 (2004).

[85] *Compare* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 948 (9th Cir. 2010) ("[S]ection [1201] (a) creates a new anticircumvention right distinct from copyright infringement…."), *with* United States v. Reichert, 747 F.3d 445, 458 (6th Cir. 2014) ("Accordingly, several courts, including ours, have held that circumvention technologies designed primarily for purposes other than to bypass copyright restrictions are not within the ambit of the DMCA's anti-circumvention provision."); *see also* Chamberlain Group, Inc. v. Skylink Techs., Inc. (*Chamberlain III*), 381 F.3d 1178, 1195 (Fed. Cir. 2004) ("Statutory structure and legislative history both make it clear that § 1201 applies only to circumventions reasonably related to protected rights.").

[86] *Chamberlain III*, 381 F.3d at 1200–01.

[87] *See Reichert*, 747 F.3d at 458.

[88] *See* Caryn C. Borg-Breen, *Garage Door Openers, Printer Toner Cartridges, and the New Age of the Digital Millennium Copyright Act*, 100 NW. U. L. REV. 885, 898–99 (2006).

[89] Chung, *supra* note 82 (defining "infringement nexus" as "a showing that the technological measure served the purpose of protecting an exclusive right provided by the Copyright Act"); *see also Chamberlain III*, 381 F.3d at 1193 ("The plain language of the statute therefore requires a plaintiff alleging circumvention (or trafficking) to prove that the defendant's access was unauthorized—a significant burden where, as here, the copyright laws authorize consumers to use the copy of Chamberlain's software embedded in the GDOs that they purchased."); *id.* at 1202 ("We conclude that 17 U.S.C. § 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners.").

[90] *Blizzard*, 629 F.3d at 950.

circumvention right distinct from copyright infringement."[91] The court believes that Congress intended to create a new right by pointing to the language and legislative history of the statute.[92] For example, the House Commerce Report proposed moving the new DMCA provisions entirely outside of Title 17 because "these regulatory provisions have little, if anything, to do with copyright law."[93] In addition, the fact that Congress granted the Library of Congress the power to create temporary exemptions for the anti-circumvention provisions seems to indicate that Congress was trying "balance copyright owners' new anti-circumvention right with the public's right to access the work."[94] Finally, though the Ninth Circuit did not address this, during the House Commerce Committee's Congressional hearings on the DMCA, several commentators proposed narrowing the anti-circumvention provisions to include some reference to infringement.[95] The fact that Congress chose not to act on these proposals is telling in and of itself.

Even if the DMCA does contemplate an infringement nexus for circumvention, that nexus may not be so difficult to meet. As Lawrence Lessig elegantly put it:

> Digital technology, at its core, makes copies. Copies are to digital life as breathing is to our physical life. There is no way to use any content in a digital context without that use producing a copy. When you read a book stored on your computer, you make a copy (at least in the RAM memory to page through the book). When you do anything with digital content, you technically produce a copy.[96]

Thus, if you hack a wearable device to look at its data output, you are likely infringing and violating the DMCA. Most data and software on these devices are encrypted or protected by other TPMs[97] which

[91] *Id.* at 948.

[92] *Id.* at 943–48.

[93] H.R. REP. NO. 105-551, pt. 2, at 23–24 (1998) [hereinafter HOUSE COMMERCE COMMITTEE REPORT].

[94] *Blizzard*, 629 F.3d at 945–46.

[95] *The WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before the Subcomm. on Telecomm., Trade, and Consumer Protect. of the H. Comm. on Commerce*, 105th Cong. 16, 22, 48 (1998) [hereinafter *House Commerce Hearings*].

[96] LAWRENCE LESSIG, CODE: VERSION 2.0 192–93 (2006).

[97] Advanced Medical Technology Association, *Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, COPYRIGHT OFFICE 5 (Mar. 11, 2016), http://bit.do/CommentAdvMedTechAssoc [hereinafter AdvaMed Comment] ("Typically, the TPMs used in medical devices includes data encryption that requires a key to the encryption in order to understand the data."); FITBIT, *supra* note 19; Electronic Frontier Foundation, *In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201*, COPYRIGHT OFFICE 1–2,

means you would have to overcome these measures to gain access to the data, i.e. you have to circumvent the technological measures.[98] Any manipulation of the software or data of the device will inevitably mean you are making unauthorized copies.[99] And since software and data output can be copyright-protected,[100] you may be infringing on the manufacturer's copyright.

In any case, the ambiguity in copyright law about whether the DMCA includes an infringement nexus itself serves to primarily benefit copyright owners. At best, if a nexus is required, a user who hacked their own device for privacy reasons can attempt to argue fair use, a notoriously unpredictable argument in court.[101] At worst, if the court does not require an infringement nexus, the user must hope for the court to otherwise interpret the DMCA's anti-circumvention provision in the user's favor. In the end, a pending lawsuit and the uncertainty of outcome may pressure many users into settling, licensing, or simply not even accessing the copyrighted work to avoid court costs.[102]

Litigation is likely because manufacturers of devices have enormous incentives to keep you from being freely able to manipulate your devices. Knowing the software or data output of a device can

http://bit.do/CommentExemptiontoProhibition [hereinafter *Comment Exemption to Prohibition*] (software in cars "is often encrypted"); Charlie Osborne, *Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack*, ZDNET (July 22, 2015), http://bit.do/SecurityVulnerable ("[E]very [smartwatch] device implemented encryption using SSL/TLS.").

[98] This is especially true given the broad definition of a TPM: "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). For example, the firmware (or operating system) of the device may itself prevent copying of the data output and would thus be a TPM. *See* Electronic Frontier Foundation, *In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, COPYRIGHT OFFICE (Mar. 11, 2016), http://bit.do/AccessControlTech ("For example, Apple, Inc.'s iOS operating system, which runs the iPhone, iPad, and iPod Touch, blocks all software from running on those devices unless the software is cryptographically signed by Apple").

[99] *See* LESSIG, *supra* text accompanying note 96.

[100] *See, e.g.*, Eng'g Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335, 1342 (5th Cir. 1994) ("Clearly, therefore, some output formats will contain sufficient original expression to merit protection."); Oracle Am., Inc. v. Google, Inc., 750 F.3d 1339, 1381 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887 (2015) ("For the foregoing reasons, we conclude that the declaring code and the structure, sequence, and organization of the 37 Java API packages at issue are entitled to copyright protection.").

[101] James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 889 (2007) ("fair use is too ambiguous to provide much ex ante guidance").

[102] *Id.* at 890–91 (explaining the "license, don't litigate" tendency in copyright caused by "doctrinal indeterminacy" of the fair use doctrine).

allow you to reverse-engineer the device. Thus, TPMs, by blocking access to the software and data, are used to protect the intellectual property underlying the device. TPMs also give manufacturers total control over how you use the device. They can keep you from repairing or altering it, as car manufacturers have done.[103] They can limit what applications run on it, as Apple has done with its tablets and phones.[104]

These are not just abstract hypotheticals. Ford Motors recently sued a car equipment company, Autel, under the DMCA for hacking Ford's diagnostic software and copying Ford's proprietary database of vehicle parts.[105] Autel created an independent diagnostic tool for repairing Ford vehicles that competed with Ford's built-in software.[106] Although the district court dismissed the DMCA claim because Ford "d[id] not allege that [it] owned a copyright on its data compilation at the time when the alleged circumvention of its technological security measures took place,"[107] it is clearly a claim that Ford thought it could otherwise win.

The fact that the Library of Congress has recently passed an exemption to the anti-circumvention provisions allowing users to circumvent the TPMs in their cars and medical devices only further proves that the anti-circumvention provisions may otherwise have been used by manufacturers against such acts.[108] During the comment period, car manufacturers strongly opposed this exemption, claiming that vehicle owners don't actually own but only license their vehicle's software,[109] and that circumvention would allow "for pirates, third-party software developers, and less innovative competitors to free-ride off the creativity, unique expression and ingenuity of vehicle software designed by leading vehicle manufacturers and their

[103] Jake Lingeman, *Will Copyright Law Prevent You from Working on Your Car?*, AUTOWEEK (Apr. 21, 2015), http://bit.do/CopyrightCar.

[104] *See Comment Exemption to Prohibition, supra* note 97, at 11.

[105] Jeff Sistrunk, *Ford Sues Car Equipment Co. For Hacking, Copying Database*, LAW360 (Sept. 29, 2014), http://bit.do/FordSuesforHacking.

[106] Mike Wehner, *Ford's Latest Copyright Lawsuit Could Cost You Money*, DAILY DOT (Jan. 10, 2015), http://bit.do/FordAutelLawsuit.

[107] Ford Motor Co. v. Autel US Inc., No. 14-13760, 2015 WL 5729067, at 14 (E.D. Mich. Sept. 30, 2015).

[108] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,953-55 (Oct. 28, 2015) (to be codified at 37 C.F.R pt. 201) [hereinafter 2015 Exemption].

[109] Auto Alliance, *Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, COPYRIGHT OFFICE 4–5, (Mar. 11, 2016), http://bit.do/CommentAutoAlliance [hereinafter Auto Alliance Comment].

suppliers."[110] Medical device manufacturers opposed circumvention of medical devices, even if it only allowed people to access their own device's data output.[111] Both car and medical device manufacturers also pointed to other regulatory schemes that are better suited to deal with how these devices operate and collect data.[112] However, the Copyright Office, in making its exemption recommendation to the Library of Congress, pointed out that "it is inescapable that the anti-circumvention prohibition in section 1201(a)(1) plays a role in th[is] debate."[113]

B. DMCA, Privacy, and IoT Devices

As currently drafted, the DMCA does not allow for circumvention of our own, legally-purchased IoT devices for privacy reasons. The DMCA drafters considered the impact of the statute on privacy. However, as this section will explain, the DMCA's attempt to address privacy is of limited utility to users concerned about how device manufacturers are collecting and using their collected data.

The DMCA contains a savings clause that directly addressed privacy concerns:

> Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the internet.[114]

[110] John Deere Comment, *supra* note 20, at 2.

[111] AdvaMed Comment, *supra* note 97, at 2 ("We believe that patients have the inherent right to access their own medical data, however this in and of itself does not necessitate bypass of any intellectual property protections.").

[112] *Id.* at 7 ("In view of the profound risks associated with unauthorized circumvention, we strongly believe that the Copyright Office should confer with FDA and defer to its views in this matter, as FDA is the federal agency charged with assuring the safety, efficacy and security of medical devices."); Auto Alliance Comment, *supra* note 109, at 21 ("We urge the Copyright Office to give full consideration to the impacts on critical national energy and environmental goals, and on motor vehicle safety, in its decision on this proposed exemption."); John Deere Comment, *supra* note 20, at 4 ("Further, the Register is encouraged to consult with other federal government agencies, including the EPA, as part of the rulemaking process prior to deciding the outcome of Proposed Class 21.").

[113] U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SIXTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 316 (Oct. 2015), http://bit.do/RegistersRecommendation [hereinafter 2015 COPYRIGHT OFFICE RULEMAKING RECOMMENDATIONS].

[114] 17 U.S.C. § 1205.

As one commentator has pointed out, however, this vague savings provision recognizes that the DMCA may create new privacy issues but offers no solutions.[115]

The DMCA also contains a number of exemptions from its anti-circumvention provisions.[116] These exemptions are too narrowly-tailored, however, to allow for circumvention due to privacy concerns. A user circumventing a device to figure out what data is being collected is not doing "encryption research" or trying to achieve interoperability.[117] Perhaps such circumvention may be considered "security testing" because users are accessing a "computer" to investigate "a security flaw" with "the authorization of the owner."[118] But is the circumvention of software on a device the same as accessing a "computer"?[119] Also, is the user the "owner" of that software?[120]

And what if a government agency wants to figure out if a device is improperly collecting data in violation of our privacy? Although the "law enforcement" exception, § 1201(e),[121] exempts investigative activity of government agents from the anticircumvention provision, it again can only be carried out "in order to identify and address the vulnerabilities of a government computer, computer system, or computer network."[122] Just as with the "security testing" exemption, it is not clear if circumventing software of an IoT device is within the scope of this narrow language.

The DMCA exemptions also address privacy violations explicitly, noting that conduct related to these exemptions that violates privacy is prohibited.[123] This language is plainly of no assistance to users desiring to circumvent their own devices as it only further limits the permissible scope of circumvention. It appears that the DMCA drafters believed that the best security for our privacy is the protection of devices using TPMs.[124] Unfortunately, although

[115] *See, e.g., House Commerce Hearings*, *supra* note 95, at 15.

[116] *See* 17 U.S.C. § 1201(b)–(j) (exemptions for activities such as security research, law enforcement activities, and encryption research).

[117] 17 U.S.C. § 1201(f)–(g); *see also* 2015 COPYRIGHT OFFICE RULEMAKING RECOMMENDATIONS, *supra* note 113, at 307 (noting the narrow language of these exemptions).

[118] 17 U.S.C. § 1201(j)(1).

[119] *See* 2015 COPYRIGHT OFFICE RULEMAKING RECOMMENDATIONS, *supra* note 113, at 308.

[120] *See id.* at 309.

[121] 17 U.S.C. § 1201(e).

[122] *Id.*

[123] *Id.* § 1201(j)(3)(B), (g)(3)(A) (using information learned from encryption research or security testing to facilitate violation of privacy weighs against finding of exemption).

[124] S. REP. NO. 105-190, at 18 (1998) [hereinafter SENATE JUDICIARY REPORT] ("In fact,

TPMs protect our device information from being hacked by third parties, they also shield data collection and usage by device manufacturers.

The DMCA contains an explicit provision, § 1201(i), that allows for circumvention of TPMs to protect PII. Unfortunately, this provision is extremely narrow in scope. First, it only allows for circumvention when the TPM "contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected."[125] In other words, this provision is concerned with internet cookies on your browser,[126] not IoT devices. Second, circumvention is only allowed to disable the cookie, and only when the TPM does not provide "conspicuous notice" and an opt-out option for data collection.[127] This provision simply provides an incentive for cookie software manufacturers to provide notice and opt-out options to users, and is not a true "exemption" to the anti-circumvention provision.[128] In sum, the provision only addresses an outdated issue of internet cookies and uses the vestigial concept of PII, without defining the term, let alone addressing re-identification problems. The limited scope of this provision prompted one commentator to note that "[t]he most plausible explanation for the specific provisions relating to online activities is simply that interest groups brought these problems to the drafting committees' attention."[129]

In recognition that this rapidly-changing field would require regulatory flexibility, Congress provided the Library of Congress with the power to create three-year exceptions to the anti-circumvention provision.[130] Nevertheless, the most recent Library of Congress exemptions also do not allow circumvention for privacy reasons, nor do they address the privacy concerns associated with wearable

enactment of section 1201 should have a positive impact on the protection of personal privacy on the internet. The same technologies that copyright owners use to control access to and use of their works can and will be used to protect the personal privacy of internet users by, for example, encrypting e-mail communications, or requiring a password for access to personal copyrighted information on an individual's web site.").

[125] 17 U.S.C. § 1201(i)(1)(A).

[126] *See* NIMMER & NIMMER, *supra* note 81, § 12A.05 [B] (referring to § 1201(i) as the "anti-cookie" provision).

[127] 17 U.S.C. § 1201(i)(1)(B).

[128] *See* NIMMER & NIMMER, *supra* note 81, § 12A.05 [B][1] ("It is in this sense that the statute creates not a true exemption here, but only a conditional one in order to create an incentive for pro-social behavior that will obviate the need for the subject feature's existence.").

[129] Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 595 (2003).

[130] *See* 17 U.S.C. § 1201(a)(1)(C); *see also* NIMMER & NIMMER, *supra* note 81, § 12A.03[A][2][b].

devices.[131] Although privacy issues were raised by interested parties in comments submitted for rulemaking, the Copyright Office did not mention privacy as a primary reason for allowing circumvention,[132] and none of these concerns made it into the final regulatory text.[133]

III. PROPOSAL

Wearable IoT devices have fallen into a regulatory gap within privacy law. At the same time, manufacturers of these devices have great financial incentives to collect, use, and sell the data their devices collect. The DMCA allows manufacturers to prohibit users and government investigators from accessing the data these devices collect, without any exceptions for privacy. This seems to be a situation of foxes guarding a henhouse. How can we properly police device manufacturers? Is self-regulation really enough? Or, in the alternative, is it realistic to rely completely on regulatory agencies to find privacy violations in consumer products? All these questions indicate that some sort of amendment to the DMCA may be necessary.

A. Option 1: Add an Infringement Nexus to the Anti-Circumvention Provision

If the DMCA anti-circumvention provision is amended to require copyright infringement for liability, then perhaps users can circumvent their devices and argue that their conduct was fair use. Although this amendment would disentangle some of the privacy issues currently mixed in with copyright law by the DMCA, this type of amendment has several disadvantages. First, fair use is an uncertain standard.[134] Litigants thus have little guidance about what conduct will be deemed appropriate before they show up in court.

Second, it is not clear how anti-circumvention should be tied to infringement in the statute. Should it be tied to intent to infringe?[135]

[131] 2015 Exemption, *supra* note 108.

[132] *See, e.g.*, 2015 COPYRIGHT OFFICE RULEMAKING RECOMMENDATIONS, *supra* note 113, at 255 (discussing the fact that "discovery of software flaws and vulnerabilities … implicate privacy, security, and safety concerns"); *id.* at 272 ("In particular, proponents note that recent guidance issued by the Food and Drug Administration ('FDA') recommends that manufacturers impose TPMs to protect device security and patient privacy, such as by limiting access to data through passwords, code authentication, and encryption of wireless communications.").

[133] *See* 2015 Exemption, *supra* note 108 (the word "privacy" does not appear anywhere in the preamble or rules).

[134] *See* Gibson, *supra* note 101, at 887-92.

[135] *See House Commerce Hearings*, *supra* note 95, at 4 (opening statement for the minority by Representative Boucher).

This would involve a difficult evidentiary analysis of scienter. Or perhaps the statute should attempt to incorporate the Federal Circuit's idea "that 17 U.S.C. § 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[136] In other words, the DMCA would prohibit circumvention only where some exclusive right of the copyright owner were trespassed.[137] However, putting vague standards such as "reasonable relationship" into the statute may not help resolve ambiguities in the law. And this would again involve issues of *why* someone accessed a work, not just the fact that they did, complicating enforcement.

Lastly, this amendment is entirely too broad, further reducing the chance that Congress would ever pass it. The amendment would not only deal with privacy, but would completely revolutionize the DMCA. Congress had proposals such as the ones above in front of it when drafting the statute.[138] Yet Congress decided to instead create a new right for copyright owners, separate from copyright infringement.[139] Maybe Congress is ready to scrap the DMCA due to the technological progress that has occurred since the original bill was drafted in 1998, but there are more realistic, narrowly-tailored solutions to deal with the privacy issues addressed in this article.

B. Option 2: Repeal § 1201(i)

Repealing § 1201(i) may allow Congress to send a clearer message that the DMCA has no impact on privacy rights and that other regulatory mechanisms can ensure manufacturer compliance with disclosure, transparency, and consent without the need for circumvention. This repeal would not be a big change for the DMCA considering the limited relevance of § 1201(i) due to its narrow scope and out-of-date conceptualization.[140]

However, privacy regulation cannot be effective if the DMCA provides no clear exception to circumvention for privacy. The DMCA creates a complete lack of transparency. Only device manufacturers know what data is collected and how it is used. Government agencies are in the dark, and so are users.[141] This puts the DMCA in tension with the goals of many privacy regulations, such as those that allow

[136] *Chamberlain III,* 381 F.3d at 1202.

[137] *See id.* at 1193; Chung, *supra* note 82.

[138] *See, e.g.*, *supra* note 135.

[139] *See supra* notes 92–95 and accompanying text.

[140] *See supra* notes 125-29 and accompanying text.

[141] *See supra* Part II.B.

consumers to dispute reports provided to insurance companies and employers.[142] How can agencies tasked with protecting consumer privacy investigate these devices without the ability to circumvent them?[143] Simply repealing § 1201(i) will not resolve any of these issues.

C. Option 3: Update and Broaden § 1201(i) and § 1201(e)

The DMCA anticircumvention provision has tangled copyright issues with privacy law in a way that needs to be addressed explicitly. Thus, the privacy exception, § 1201(i), and the law enforcement exception, § 1201(e), need to be updated and broadened to allow for proper regulation of privacy. The new exceptions need to be flexible to allow for technological change. They also need to be clearly defined to prevent abuse. Finally, the government's chief privacy agency, the FTC, needs to have a greater role in the enforcement of those provisions. The Library of Congress is utterly lacking in expertise in this space.

It may be possible to convince Congress to amend § 1201(i). Legislative history indicates that Congress had broader privacy concerns in mind when drafting the DMCA, but may have simply been unable to predict subsequent technological developments. For example, the Senate Committee on the Judiciary explained that the savings clause in the DMCA was drafted to prevent parties from relying on the DMCA's anticircumvention provision "to make it harder, rather than easier, to protect personal privacy on the internet" in a scenario where "existing or future technologies …evolve[d] in such a way that an individual would have to circumvent a technological protection measure to protect his or her privacy."[144] In proposing § 1201(i), the House Committee on Commerce noted that "in reaching to protect the rights of copyright owners, Congress need not encroach upon the privacy interests of consumers."[145] Thus, Congress may be amenable to updating § 1201(i) to protect privacy.

1. The New § 1201(i) Privacy Exception

The new § 1201(i) needs to strike a balance between incentivizing transparency for manufacturers but preventing user abuse in the name of privacy. It is not enough for § 1201(i) to allow circumvention only when device manufacturers do not provide

[142] *See* 15 U.S.C. § 1681i(a)(1)(A).

[143] *See supra* notes 121-22 and accompanying text.

[144] SENATE JUDICIARY REPORT, *supra* note 124, at 18.

[145] HOUSE COMMERCE COMMITTEE REPORT, *supra* note 93, at 27.

conspicuous notice of data collection, however. There is no proper check on the manufacturers in this case—their notice may be inaccurate, and circumvention is the only way anyone can find out about their real practices. Giving all the power to device manufacturers, when they have strong incentives not to be forthright,[146] is not a workable solution.

It is also unrealistic for the government—the FTC, for example—to monitor all device data collection and dissemination practices without third party input. Even large device manufacturers and software companies often rely on outside hackers for input about data vulnerabilities.[147] And the FTC has fewer resources and less expertise than some of these private companies do. In fact, there is evidence that the FTC already relies on private input when it comes to investigating inappropriate device collection by manufacturers.[148] Thus, some circumvention by private individuals needs to be allowed in order to properly police device manufacturers.

Section 1201(i) should be amended to allow for good-faith circumvention of a user's lawfully-purchased device to determine if data being collected is inconsistent with the context of the company's relationship or interaction with the consumer.[149] This "context of interaction" concept has been discussed by the FTC in two reports.[150] The concept addresses "the need for flexibility so that companies can tailor the[ir] choice options to specific business models and contexts."[151] In recognition of this need for flexibility, the FTC has mentioned that the timing and extent of disclosure and consent may vary depending on how the company uses the data and what type of data is collected.[152] It may be impractical and unnecessary to provide for consumer choice before every single data collection event,

[146] *Supra* notes 13-15 and accompanying text.

[147] Nicole Perlroth & Katie Benner, *Apple Policy on Bugs May Explain Why Hackers Would Help F.B.I.*, N.Y. TIMES (Mar. 22, 2016) http://bit.do/AppleBugsPolicy ("Google, Microsoft, Facebook, Twitter, Mozilla and many other tech companies all pay outside hackers who turn over bugs in their products and systems.").

[148] FTC investigations are not public. *See* Media Resources, FTC (March 2, 2016) http://bit.do/FTCMediaResources. However, in at least one recorded case, consumers tipped off the FTC about a device collecting data inconsistent with consumer expectations. *Flashlight app secretly tracked users' locations, FTC says*, CBS NEWS (Dec. 5, 2013), http://bit.do/FlashlightApp ("This particular case came to light because of the diligence of tech-savvy customers who questioned why a flashlight app would be interested in a phone's geolocation. The FTC said consumer concerns posted online helped to tip off the agency.").

[149] *See, e.g.*, 2015 FTC REPORT, *supra* note 63, at 43.

[150] *See id.*; 2012 FTC REPORT, *supra* note 63, at 48–49.

[151] 2012 FTC REPORT, *supra* note 63, at 49.

[152] *Id.* at 49-50; 2015 FTC REPORT, *supra* note 63, at 43.

especially if the collection is consistent with user expectations.[153] As detailed in the next section dealing with the law enforcement exception, the FTC can use rulemaking to define the parameters of this "context of interaction" standard and to specify new industry norms, while still leaving room for innovation.[154]

The new § 1201(i) exception could be limited in several ways to prevent abuse in the name of privacy. For instance, it would only allow circumvention of one's own device, not general trafficking in technology that would allow others to circumvent.[155] Effectively, circumvention would be open only to those users with the coding skills necessary to figure out what their own IoT device is doing (i.e., "white hat" hackers). In addition, the exception would require a "good faith" purpose for circumvention. New regulations or the revised language of § 1201(i) can further specify that the good faith purpose will only be presumed in court if the white hat hacker filed a report with the FTC about their findings. The hacker can report that he or she found no improper data collection or dissemination and would still be entitled to this rebuttable presumption.[156]

However, this presumption could be rebutted if the device manufacturer properly followed FTC disclosure and consent regulations, as detailed in the FTC's new rulemaking.[157] Thus, if the company already had a very detailed privacy policy and appeared transparent about data collection and use, there may have been less of a reason for a user to go digging into the hardware and software of the device. In sum, this exception would provide an incentive for manufacturer transparency and limit circumvention to good faith purposes by sophisticated coders.

2. Expanded § 1201(e) Law Enforcement Exception

To complement the new privacy exception above, the law enforcement exception, § 1201(e), needs to be broadened to allow the FTC to investigate whether data collection or dissemination by an IoT device manufacturer is inconsistent with the context of the company's

[153] 2015 FTC REPORT, *supra* note 63, at 40–41, 43.

[154] *Id.* at 43.

[155] *See* 17 U.S.C. 1201(a)(2) ("No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title….").

[156] Users may need additional immunity if device manufacturers bring contract lawsuits against them for breaching the terms of service. This is beyond the scope of this article, however.

[157] *See infra* Part III.C.2.

relationship with the consumer. Since enforcement by a government agency is less open to abuse and requires more flexibility, this exception may allow FTC agents not only the right to circumvent devices but also the right to traffic in circumvention technologies. With this expanded exception, the FTC can properly respond to third party tips as it sees fit.

The recent attempt by the Department of Justice (DOJ) to force Apple to hack the San Bernadino shooter's iPhone[158] ("the Apple case") does reveal additional concerns that any new expansion of government power in this area needs to address. The suggested revision to the law enforcement exception is not intended to provide a route for government agencies to force device manufacturers to create deliberate, back-door access to their devices for investigative purposes. This type of government power may lead to reduced effectiveness of existing encryption mechanisms and hinder personal privacy. The goal of this proposal is to provide increased transparency of the use of data by device manufacturers, while minimizing any unintended effects on personal privacy.

To avoid the potential use of the All Writs Act[159] by a court of law—as the DOJ attempted to do with Apple—the law enforcement exception should mimic the limitations of the Communications Assistance for Law Enforcement Act (CALEA)[160] at issue in the Apple case. As Professor Nunziato explained in a recent article,[161] CALEA does not allow a court to invoke the All Writs Act to force Apple to create a back door to its encryption.[162] In enacting CALEA, Congress expressly stipulated that the Act "does not authorize any law enforcement agency or officer— to require any specific design of equipment … to be adopted by any provider of a wire or electronic communication service…."[163] This explicit limitation, Nunziato posits, protects manufacturers against government use of the All Writs Act because "courts cannot rely on the [All Writs] Act to issue an order that is explicitly or implicitly prohibited under a federal statute"[164] Thus, a similar limitation in the proposed law enforcement

[158] Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://bit.do/AppleFightsOrder.

[159] 28 U.S.C. § 1651.

[160] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001.

[161] Dawn Carla Nunziato, Code Free or Die: Apple's Flawed First Amendment Defense to the Government's Order Compelling Apple to Write Computer Code to Defeat iPhones' Security Features (2016) (unpublished manuscript) (on file with author).

[162] *Id.* at 7.

[163] *Id.* (quoting 47 U.S.C. § 1002(b)(1)).

[164] *Id.* at 6.

exception to the DMCA may be necessary to prevent government use of the statute for unintended purposes.

Aside from the concerns brought to light in the Apple case, the statutory exception should be broadly-worded to allow flexibility for the rapid technological changes occurring in this area. To that end, the DMCA exception needs to grant the FTC substantive rulemaking authority to define what it means for data collection and dissemination to be inconsistent with the context of the company's relationship with the consumer.[165] The FTC can use this power to develop context-specific industry standards of disclosure, consent, and user access to data that are in line with other privacy regulations already in place. The new regulations can also help steer privacy law to concepts beyond PII, for example, by developing a flexible standard that considers whether the person involved is identified or identifiable, and with the latter, the risk of re-identification.[166] In addition to rulemaking, the FTC also has expertise in providing guidance and developing data security industry standards through its enforcement actions.[167] Under this proposal, the FTC can use rulemaking and enforcement actions to align the DMCA with the goals underlying our privacy laws—providing "notice and consent, access, data integrity, enforcement, and remedies"[168]—while pushing this area of the law in the direction of much-needed updates.

CONCLUSION

Our IoT devices are constantly monitoring our every move, collecting sensitive data about us in a way that we do not fully appreciate. The companies manufacturing these devices have a huge financial incentive to collect as much data as they can, and to use and sell this data in its most identifiable form. Yet the DMCA and our current privacy regulations provide no real checks on the conduct of these companies. The DMCA anticircumvention provision prevents users and the government from ever finding out what data is collected and how it used by device manufacturers. To create some transparency in this system, Congress must amend the DMCA to

[165] *See supra* notes 149–154.

[166] *See* Schwartz & Solove, *supra* note 61, at 1877–79 (discussing a new standard for PII that takes into account re-identification potential of digital data).

[167] *See generally* Woodrow Hartzog & Daniel J. Solove, Th*e Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015) (discussing FTC authority and common law rulemaking in the privacy and data security space).

[168] Ohm, *supra* note 13, at 1734; *see also* Schwartz & Solove, *supra* note 61, at 1824–25 (discussing the listed Fair Information Practices as "the building blocks of modern information privacy law").

include a limited circumvention exception for privacy. The proposed exception attempts to incentivize above-board behavior by device manufacturers, while allowing the government's chief privacy agency, the FTC, to have the tools and resources required to investigate improper practices at its disposal. The FTC can help create binding industry standards for data collection and dissemination, aligning the DMCA with the goals in our privacy regulations and filling in the regulatory gaps our current privacy laws leave for IoT device manufacturers.