Submitted Statement for the Record of
Public Knowledge

Before the
Subcommittee on Courts, Intellectual Property, and the Internet
of the
Committee on the Judiciary
U.S. House of Representatives

Hearing on
The Internet of Things

July 29, 2015

SUMMARY

The Internet of Things presents exciting opportunities for a technologically driven society, but it also presents challenges to the rights and interests of consumers in that same society. We urge the Subcommittee to account for the wide range of such challenges as it considers law and policy for the Internet of Things in the coming years.

Patents on consumer technologies. Reforming the patent system is already a key issue for Congress now, and the Internet of Things will bring new challenges to this law of innovation. In particular, the Internet of Things is often described as numerous devices connecting to each other, and a particularly problematic form of patent is that which merely covers obvious combinations of devices connected to each other. Patent quality and fairness in patent assertion will be key factors in the success of the Internet of Things.

Ownership of devices. A particular and discomfiting trend is toward leveraging intellectual property rights and end-user license agreements that prevent consumers from full enjoyment of the very products those consumers buy. Through technological measures like DRM and contractual provisions that purport to merely license rather than sell device-embedded software, manufacturers declare that consumers do not in fact own their own devices. This already-present problem will only be exacerbated by the world of the Internet of Things.

Freedom to tinker and innovate. Attendant to the undermining of ownership rights in devices is the loss of consumers' ability to repair, improve, and innovate upon their personal property for their personal interests. Laws like § 1201 of the Digital Millennium Copyright Act (DMCA) prevent such user-driven creativity and invention, and as such contradict the basic purpose of intellectual property to "promote the progress of science and the useful arts." Legal policy should embrace, not entangle, efforts toward consumer-level progress, especially as the Internet of Things places more devices and thus more opportunities in the hands of consumers.

Communications privacy. While the future of the Internet of Things is not yet formed, one thing is certain: there will be numerous devices using communications networks to transmit information, much of which will divulge potentially private information about those devices' users. In such a world, privacy of the platforms of communication becomes orders of magnitude more important. Communications statutes give the Federal Communications Commission authority to ensure privacy and data security on such communications systems, and such authority must be maintained, strengthened, and adapted to ensure that consumer expectations are met in the Internet of Things.

Spectrum management. Critical to the Internet of Things is connectivity, and the primary vector for Internet of Things interconnection is "open" or "license exempt" spectrum. The vast majority of wireless Internet of Things devices will rely on open spectrum technologies like Wi-Fi and Bluetooth. Success of the emerging Internet of Things thus requires expanding our increasingly strained supply of open spectrum on the same terms and conditions available today. Additionally, as economic incentives among some actors grow to block or degrade Wi-Fi and other protocols that support the Internet of Things, we must ensure that the robust and highly competitive ecosystem of open spectrum critical to the emerging Internet of Things remains intact.

TABLE OF CONTENTS

THE INTERNET OF THINGS

STATEMENT OF PUBLIC KNOWLEDGE

Chairman Issa, Ranking Member Nadler, and Members of the Subcommittee:

Thank you for providing us with the opportunity to submit the following testimony for the record of this hearing on the Internet of Things.

Public Knowledge is a non-profit organization dedicated to preserving the openness of the Internet and the public's access to knowledge, promoting creativity through balanced intellectual property rights, and upholding and protecting the rights of consumers to use innovative technology lawfully. As part of this mission, Public Knowledge advocates on behalf of the public interest for a balanced intellectual property system, particularly with respect to new and emerging technologies, and for communications policy that fosters such emerging technologies.

While much have been said about privacy and security concerns surrounding the Internet of Things, Public Knowledge wishes to bring to light many other important issues that would affect technology-using consumers as these new developments move forward. In particular, we recommend that the Subcommittee include the following considerations in its deliberations over the Internet of Things.

I. The Proper Balance of Patent Law May Make or Break the Internet of Things

This Subcommittee is no doubt aware of the ongoing issues with the patent system and efforts to reform that system. Concern over so-called patent trolls using patents in abusive ways to attack small, innovative businesses abound in the news,[1] in the Adminis-

[1] *See, e.g.,* Fabio Marino & Teri Nguyen, *Are Patent Trolls Now Zeroed In on Start-Ups?*, Forbes (Jan. 17, 2013), http://www.forbes.com/sites/ciocentral/2013/01/17/are-patent-trolls-now-zeroed-in-on-start-ups/; Charles Duan, *Taking a Page from the Patent Troll Playbook*, Slate: Future Tense (Dec. 17, 2014), http://www.slate.com/articles/technology/future_tense/2014/12/ben_edelman_used_patent_troll_tactics_in_going_after_a_chinese_restaurant.html; Joe Mullin, *Patent Trolls Want $1,000—for Using Scanners*, Ars Technica (Jan. 2, 2013), http://arstechnica.com/tech-policy/2013/01/patent-trolls-want-1000-for-using-scanners/.

tration,[2] and even in the opinions of the Supreme Court.[3] Congress has made significant progress on two major bills to reform patent litigation.[4]

The Internet of Things shines a bright light on the patent system and its effects. Obviously, patents are a strong incentive for inventing new technologies, and as such are a key part of driving the Internet of Things forward. But a system full of overbroad patents and abusive patent litigation will drive innovation backwards instead, hampering the very innovators who would create those new technologies by threatening them with protracted litigation over patents on the most basic ideas.

In particular, the Internet of Things is all about connecting multiple consumer devices: the alarm clock tells the coffee machine to turn on; the refrigerator tells the smart phone what food to buy at the grocery store, and so on.[5] These are simple, obvious ideas—any imaginative person could devise them—and the value for consumers is not in the idea itself but in the implementation and standardization among companies that bring these ideas to market.

---

[2] *See, e.g.,* Executive Office of the President, Patent Assertion and U.S. Innovation 6 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/patent_report.pdf (describing PAEs as "pursuing legal action in a way that does not increase incentives for innovation"); Fed. Trade Comm'n, The Evolving IP Marketplace: Aligning Patent Notice and Remedies with Competition 67–68 (2011), *available at* http://www.ftc.gov/os/2011/03/110307patentreport.pdf (suggesting that increased PAE activity "can be detrimental to innovation"); *U.S. Patent and Trademark Office: The America Invents Act and Beyond, Domestic and International Policy Goals: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 13 (2014), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg88922/pdf/CHRG-113hhrg88922.pdf (statement of Michelle K. Lee, Deputy Under Secretary of Commerce for Intellectual Property) ("[T]he USPTO believes that additional legislative changes to build upon the AIA are needed to further enhance patent quality and to lessen litigation abuses in the system.").

[3] *See, e.g., Commil USA, LLC v. Cisco Sys., Inc.*, 135 S. Ct. 1920, 1930 (2015) (quoting *eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 396 (2006) (Kennedy, J., concurring)); *id.* at 1932 (Scalia, J., dissenting); *Bilski v. Kappos*, 130 S. Ct. 3218, 3257 (2010) (Stevens, J., concurring) ("[P]atent holders may be able to use [patents] to threaten litigation and to bully competitors . . . . That can take a particular toll on small and upstart businesses." (footnote omitted)); *Atl. Works v. Brady*, 107 U.S. 192, 200 (1883) (expressing concern over "speculative schemers who make it their business to watch the advancing wave of improvement, and gather its foam in the form of patented monopolies, which enable them to lay a heavy tax upon the industry of the country, without contributing anything to the real advancement of the arts").

[4] *See* Innovation Act, H.R. 9, 114th Cong. (Feb. 5, 2015); Protecting American Talent and Entrepreneurship (PATENT) Act, S. 1137, 114th Cong. (Apr. 29, 2015).

[5] *See* discussion *infra* p. 13 (describing various Internet of Things devices that may be connected with each other).

But it is disappointingly common to see patents on these basic ideas of connecting one known technology to another. Consider the following examples:

- U.S. Patent No. 6,975,958: Connecting a thermostat to the Internet.[6]
- U.S. Patent No. 6,199,048: Connecting a barcode scanner to a networked computer database.[7]
- U.S. Patent No. 7,324,833: Connecting an iPod to a car.[8]
- U.S. Patent No. 7,343,165: Connecting a GPS to user directory information.[9]
- U.S. Patent No. 7,016,512: Connecting a hearing aid to an electrical plug.[10]

Such patents could easily stifle the development of new Internet of Things devices, and they could unexpectedly and undesirably deem every consumer of such devices an infringer and breaker of the law merely for connecting those devices to each other.

The Subcommittee should thus keep patents at the forefront of its thinking on the Internet of Things. Current efforts on patent litigation reform are an important step, as is encouraging and facilitating the U.S. Patent and Trademark Office's efforts toward improving patent quality,[11] to hopefully avoid such patents as those described above.

---

[6]U.S. Patent No. 6,975,958 (filed Apr. 30, 2003); *see* Mike Masnick, *Honeywell's Lawsuit Against Nest: The Perfect Example of Legacy Players Using Patents to Stifle Innovation*, Techdirt Innovation (May 8, 2012), https://www.techdirt.com/blog/innovation/articles/20120508/03354418823/honeywells-lawsuit-against-nest-perfect-example-legacy-players-using-patents-to-stifle-innovation.shtml.

[7]U.S. Patent No. 6,199,048 (filed Jan. 15, 1999); *see* Michael Barclay, *U.S. Patent Office Rejects All Ninety-Five NeoMedia Patent Claims*, Electronic Frontier Found. (July 18, 2008), https://www.eff.org/deeplinks/2008/07/u-s-patent-office-rejects-all-ninety-five-neomedia.

[8]U.S. Patent No. 7,324,833 (filed Sept. 23, 2004); *see* Samuel Howard, *Affinity Labs Hits Car Stereo Cos. With Patent Suit*, Law360 (Sept. 2, 2008), http://www.law360.com/articles/67992/affinity-labs-hits-car-stereo-cos-with-patent-suit.

[9]U.S. Patent No. 7,343,165 (filed Apr. 11, 2001); *see* Jeff John Roberts, *Patent Troll Says It Owns GPS, Sues Foursquare*, Gigaom (July 26, 2012), https://gigaom.com/2012/07/26/patent-troll-says-it-owns-gps-sues-foursquare/.

[10]U.S. Patent No. 7,016,512 (filed Aug. 29, 2003); *see K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1367 (Fed. Cir. 2014) (Dyk, J., dissenting) ("This should be an easy case, reversing the quite odd decision of the United States Patent and Trademark Office . . . that it could not consider whether multi-pronged electrical connections were well known in the prior art.").

[11]Charles Duan et al., Comments of the Electronic Frontier Foundation, Engine Advocacy, and Public Knowledge, *Enhancing Patent Quality*, 80 Fed. Reg. 6475 (USPTO May 6, 2015), http://www.uspto.gov/sites/default/files/documents/2015quality_a_eff_06may2015.pdf.

II. Lack of Ownership Rights over Electronic Devices Will Cause Substantial Problems for the Internet of Things

It's a basic feature of our laws that consumers have a lot of rights over their own physical and personal property. You can sell your car to whomever you like, repair it, modify it up to (and well beyond) the bounds of taste or sanity, lend it to anyone, and even rent it out or sell it to others. The same is true of pretty much anything else you have in your possession—your umbrella, your coat, and your desk. The right of ownership is the right to use and the right to dispose of physical property.[12]

Yet when it comes to equally physical, equally tangible electronic devices, those basic ownership rights have been diminished and even at times eliminated, often through use of intellectual property law.[13] Such efforts are troubling to the consumer interest and will only worsen as the Internet of Things places more electronics—and thus more opportunities to erode ownership rights—into everyday household products.

Are You Allowed to Turn Your Devices On? Every computing device, and thus every Internet of Things device, necessarily performs acts of copying of embedded software whenever it is turned on and operated. This means that, absent some sort of appropriate legal exception, it would be an act of copyright infringement merely to turn on your computer, smartphone, or FitBit. Unsurprisingly, the Copyright Act does contain such an exception: 17 U.S.C. § 117 "it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy" where the copy is made "as an essential step in the utilization of the computer program."[14]

It would seem that § 117 would resolve the issue, except that manufacturers have sought to circumvent—and successfully circumvented—this provision by declaring that a purchaser of a device with embedded software is not "the owner of a copy" of that software.

---

[12] *See* Denise R. Johnson, *Reflections on the Bundle of Rights*, 32 Vt. L. Rev. 247, 253 (2007) (enumerating eleven rights attendant to property ownership).

[13] *See* Christina M. Mulligan, *Personal Property Servitudes on the Internet of Things*, 49 Ga. L. Rev. (forthcoming 2015) (manuscript at 4–5), *available at* http://ssrn.com/abstract=2465651.

[14] 17 U.S.C. § 117(a) (2012).

For example, many product manufacturers write End User License Agreements (EULAs) that claim that the embedded software is never owned by the user. This allows them to assert that users can be found liable for copyright infringement for violations of the EULA despite § 117.

Courts have looked askance at such a strategy, expressing concerns that it "would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners,"[15] but have overall upheld the idea that purchasers of software may be denied status as "owners" of such software by virtue of such EULAs.[16] This Subcommittee should look equally askance at this denial of basic ownership rights by contracts of adhesion, considering the negative effects that will only multiply with the device multiplicity of the Internet of Things.

Chattel Servitudes Via Intellectual Property. The principle that physical, personal property may not be encumbered by post-sale restrictions set by a seller of that property—that chattels may not be subject to servitudes—dates back to Lord Coke's common law treatise of 1628.[17] It is now embodied in copyright's first sale doctrine[18] and patent law's doctrine of exhaustion.[19] But that right of owners to be free of easements on their things has been attacked in a number of ways using intellectual property law.

Section 1201 of the Digital Millennium Copyright Act (DMCA)[20] has been used to restrict electronic device owners' ownership rights. Although courts have at times stated that § 1201 does not "allow any company to attempt to leverage its sales into aftermarket monopolies,"[21] authorities such as the Library of Congress (who oversees administration

[15] *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 941 (9th Cir. 2010).

[16] *See, e.g., Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1111–12 (9th Cir. 2010); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 n.5 (9th Cir. 1993); *MDY Indus.*, 629 F.3d at 938.

[17] 1 Edward Coke, Institutes of the Lawes of England § 360, at 223 (1628).

[18] *See* § 109(a).

[19] *See Quanta Computer, Inc. v. LG Elecs., Inc.*, 553 U.S. 617, 625 (2008).

[20] 17 U.S.C. § 1201 (2012).

[21] *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1201 (Fed. Cir. 2004).

of portions of § 1201) have permitted such restrictions, for example by denying consumers the right to unlock their cell phones to use them with alternate mobile phone networks.[22]

Similarly, the Court of Appeals for the Federal Circuit has approved of using patent law to enforce manufacturer-imposed restrictions on consumers' ability to resell lawfully purchased goods.[23] This decision is currently being reconsidered as having potentially been overruled by later Supreme Court precedent.[24]

These efforts to erode the basic ownership right of alienation, termed "first sale" in copyright law and "exhaustion" in patent, have not gone unnoticed. As one commentator explains, "the similarities between unprotected goods and intellectual-property-embedded goods suggest that the exceptions to the first sale doctrine for conditionally-sold patented goods and software-embedded goods ought to be met with skepticism."[25] This Subcommittee should take an equally skeptical eye toward such developments in the law, in view of the Internet of Things.

Lack of Ownership Rights Harms Consumers. Such efforts to eviscerate ownership rights in their owned products directly harm consumers, who highly value freedom to use their purchase products and who despise such post-sale restrictions.

Several months ago, the coffeemaker manufacturer Keurig implemented lock-down technology into the Keurig 2.0 machine, preventing the machine from being used with single-serve coffee cups other than those authorized by Keurig. Consumers were outraged, going so far as to say, "I will never buy another Keurig product. This borders on the unethical forcing people to buy only the K-cups you make."[26]

---

[22] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 65260, 65255–66 (Library of Cong. Oct. 26, 2012) (to be codified at 37 C.F.R. § 201.40 (2014)), *repealed*, Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144, 128 Stat. 1751 (2014).

[23] *See Mallinckrodt, Inc. v. Medipart, Inc.*, 976 F.2d 700, 708 (Fed. Cir. 1992).

[24] *See Lexmark Int'l, Inc. v. Impression Prods., Inc.*, 785 F.3d 565 (Fed. Cir. 2015) (sua sponte order for rehearing en banc) (considering whether *Mallinckrodt* has been overruled by *Quanta*).

[25] Mulligan, *supra* note 13, at 30.

[26] Fred Barbash, *Keurig's K-Cup Screw-up and How It K-pitulated to Angry Consumers*, Wash. Post (May 7, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/05/07/keurigs-k-cup-screw-up-

Consumers also have objected to vehicle-implemented technological protection measures that prevent repairs, as those protection measures amount to post-sale restrictions. "Vehicle owners expect to have the freedom to repair and tinker with their vehicles, as they have done for decades," argued one organization seeking to obtain rights for consumers to overcome such technological locks.[27] And an agricultural advocacy group wrote: "We stand with a community of farmers . . . whose right to access, understand, and fully utilize their tools should be defended."[28] These civil society groups vocalized the expectations of consumers in having full, unhindered ownership rights.

Full ownership rights confer numerous societal and economic benefits. They avoid unnecessary administrative costs of tracing the trail of restrictions on any given product.[29] They open the door to secondary markets like eBay.[30] They allow consumers to repair their cars and other possessions.[31]

All of these rights are necessary today, and they will only become even more necessary with the developing Internet of Things, where electronic devices will abound. This Subcommittee must ensure that in the shuffle to bring new products and services to the market, consumers' ownership rights are not lost.

A Step Forward: The You Own Devices Act Fortunately, there are simple and straightforward solutions to protecting this consumer interest in ownership rights. The

---

and-how-it-k-pitulated-wednesday-to-angry-consumers/; *see also* Mat Smith, *Surprise! People Don't Like Keurig's DRM-Protected Coffeemakers*, Engadget (Feb. 6, 2015), http://www.engadget.com/2015/02/06/unsurprisingly-people-didn-t-like-keurigs-drm-protected-coffee/ (noting "consumers complaining everywhere online" about Keurig's plan).

[27] Comments of Electronic Frontier Foundation 16, *Exemption to Prohibition on Circumvention of Copyright Protection Systems*, 79 Fed. Reg. 73856 (Copyright Office Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class21.pdf.

[28] Comments of Farm Hack, *Exemption to Prohibition on Circumvention of Copyright Protection Systems*, 79 Fed. Reg. 73856 (Copyright Office Feb. 4, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_FarmHack_class21.pdf.

[29] *See, e.g., Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013); Mulligan, *supra* note 13, at 32 ("As software is incorporated more frequently into personal property, the information costs associated with using and transferring personal property will increase.").

[30] *See* Zachariah Chafee, *The Music Goes Round and Round: Equitable Servitudes and Chattels*, 69 Harv. L. Rev. 1250, 1261 (1956) (describing "policy in favor of mobility" long embraced by personal property law).

[31] *See Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 497 (1961).

You Own Devices Act, introduced this February, provides that a consumer is allowed to sell a device containing operating software, regardless of any contractual provision on the right to resell such software.[32] Such a bill would be a substantial step toward restoring the rights of consumers to use and sell their personal property.

As this Subcommittee continues to look at the legal implications of the Internet of Things, it should consider solutions such as the You Own Devices Act to ensure that consumers are adequately protected in their purchases of Internet of Things devices.

III. Laws Regulating the Internet of Things Must Enhance, Not Hamper, User-Driven Innovation

The ownership interests in Internet of Things devices are particularly important because they are the prerequisite to the "freedom to tinker": the ability of consumers to use, repair, modify, and improve upon their devices, in ways not contemplated by or even contrary to the interests of the original manufacturers.

The law would never prevent a consumer from shortening the legs of a chair to better fit his table, or a driver from replacing the stock tires on her car with ones that better suited her driving conditions. Parents might disable the camera on their children's laptops to protect their privacy. The addition of networked computers into everyday devices doesn't change the impulses to modify them. Whether a homeowner wants to alter his smart thermostat to work better with his existing air conditioner, or an abuse victim who wants to alter her car's location reporting so as not to expose it to her stalker, consumers enmeshed in the Internet of Things will still want and need to make their own adjustments to their property.

Yet the presence of embedded software can change the legal status of consumers' rights to repair, adapt, and tinker with their own goods. As explained above, the mere act of turning on an Internet of Things device can be a copyright infringement based on end-user license agreements, thus opening an avenue for manufacturers to prevent consumers

[32] *See* You Own Devices Act, H.R. 862, 114th Cong. sec. 2(a) (Feb. 11, 2015).

from modifying their devices, for fear of intellectual property litigation. Such a result ought to be avoided, either through application of 17 U.S.C. § 117 as discussed above or, to the extent that a license agreement purports to divest consumers of ownership of their own property,[33] through the doctrine of fair use.[34]

The anticircumvention provisions of the DMCA[35] provide a second avenue for extinguishing the freedom to tinker. By placing digital locks on consumer products and then using § 1201 to prevent consumers from opening those locks, manufacturers can dictate what consumers are allowed to do with their property. Some of the most celebrated cases on § 1201 feature precisely the type of behavior: a printer manufacturer denying consumers the right to refill their toner cartridges,[36] and a garage door opener manufacturer disallowing its customers from using aftermarket clicker transmitters.[37] These attempts at control have not lessened over the past decade, as filings and testimony at this year's triennial proceedings have demonstrated the interest of a number of manufacturers to continue using embedded software and access controls upon it to prevent users from adapting their products.[38] The Subcommittee should take notice of the demonstrated overreach of § 1201 and make efforts to provide necessary exceptions, exemptions, and limitations to the anticircumvention provisions, so as to grant consumers their deserved freedoms.

The freedom to tinker is particularly important because it is frequently the wellspring of productive innovation. As one multinational survey found, "millions of citizens

[33]Such an assertion, which would put the ownership of the product at odds with the ownership of software necessary to grant the owner full and fair use of it, should be scrutinized for potential violations of antitrust law or as potentially unfair or deceptive trade practices.

[34]*See* 17 U.S.C. § 107 (2012). Patent law has long recognized a right to repair, *see* discussion *supra* note 31, and copyright law has recognized one as well, *see* Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. Rev. 889, 912–19 (2011) (detailing cases of rights to repair and modify under copyright law analogous to the patent doctrine). These doctrines should operate today, whether independently or through the mechanisms of fair use and first sale.

[35]17 U.S.C. § 1201 (2012).

[36]*See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).

[37]*See Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

[38]*See Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Second Round of Comments*, U.S. Copyright Off. (Mar. 27, 2015), http://copyright.gov/1201/2015/comments-032715/.

innovate to create and modify consumer products to better fit their needs."[39] The resulting user-driven innovations became an "unexpected 'front end' of free innovation designs to serve as an important feedstock to commercial innovation processes in a wide variety of fields."[40] Freedom to tinker does not merely benefit the tinkerers; it in fact benefits manufacturers and the public as a whole.

But many manufacturers prefer instead to curtail consumers' rights to tinker with goods. A manufacturer may try to prevent consumers from modifying products to better suit their lives and households, preferring instead that they go back to the manufacturer for repairs—or to buy a new suite of products entirely.

Consumers should therefore be protected against attempts to use copyright law to prevent these traditional rights in the emerging Internet of Things—in the interests of them exercising their full property rights, protecting their privacy, and even building their and their children's skills in working with technology. The value of the freedom to tinker is not only the pocketbook value of fixing and customizing one's own belongings; it also provides an educational value in showing the user how devices—and the increasingly scientific, technological, and engineered world—works.

IV. Communications Privacy Takes On an Increasingly Important Role in the Internet of Things

The Internet of Things raises numerous privacy and data security concerns due to the quantity and granularity of data opened up by software-enabled devices. The Subcommittee should carefully consider one particular such concern, namely privacy and security of communications data sent over broadband Internet and other communications networks.

[39] Eric von Hippel et al., *The Age of the Consumer-Innovator*, MIT Sloan Mgmt. Rev., Fall 2011, at 28, *available at* https://evhippel.files.wordpress.com/2013/08/smr-art-as-pub.pdf.

[40] *Id.* at 29.

A Mass of Private Information, Open to Communications Carriers. The Internet of Things puts a wealth of information into the hands of carriers such as broadband Internet providers. First, the average consumer in an Internet of Things connected home now generates more data than ever before. Second, the data produced by the Internet of Things has grown both vaster and more detailed. And third, the potential for abuse by private interests has grown exponentially.

The fundamental idea underlying the Internet of Things is one of externalization—that is, to take the tasks once managed by an individual, and delegate their coordination to a series of outside devices. A typical example may go something like this: Sarah Consumer programs her LED smart lighting system[41] to wake her at a certain time by simulating a sunrise. The program controlling the lights,[42] having identified this as the time of day when Sarah rises and goes to eat breakfast, prepares the household for the day by performing various tasks, such as adjusting the thermostat,[43] dispensing diet food for the cat,[44] brewing a pot of coffee,[45] checking to make sure there is fruit and yogurt in the fridge,[46] and compiling a grocery list if any items were missing.[47]

The amount of data that passes between devices is substantial, and extremely detailed. In the example above, at various times, connected devices are swapping information including Sarah's sleep patterns, her dietary preferences, how warm she likes her

[41]Lee Hutchinson, *In Living Color: Ars Reviews the Hacker-Approved Philips Hue LEDs*, Ars Technica (Nov. 19, 2012), http://arstechnica.com/gadgets/2012/11/in-living-color-ars-reviews-the-hacker-approved-philips-hue-leds/.

[42]Tim Bajarin, *Amazon's Echo Is Showing Us the Future*, PCMag (July 27, 2015), http://www.pcmag.com/article2/0,2817,2488071,00.asp.

[43]Tom Simonite, *How Nest's Control Freaks Reinvented the Thermostat*, MIT Tech. Rev., Feb. 15, 2013, at 28, http://www.technologyreview.com/featuredstory/511086/how-nests-control-freaks-reinvented-the-thermostat/.

[44]Colin Jeffrey, *Bistro Cat Feeder and Health Monitor Identifies Cats Using Facial Recognition*, Gizmag (July 21, 2014), http://www.gizmag.com/facial-recognition-bistro-cat-feeder-health-monitor/33032/.

[45]Philip Palermo, *IRL: I Spent a Month Controlling My Coffeemaker over WiFi*, Engadget (Feb. 3, 2015), http://www.engadget.com/2015/02/03/irl-a-month-controlling-my-coffeemaker-over-wifi/.

[46]AJ Dellinger, *The New GE ChillHub Fridge Is So Smart, It Thinks It's a Computer*, Digital Trends (Feb. 5, 2015), http://www.digitaltrends.com/home/ge-firstbuild-chillihub-smart-fridge/.

[47]Bajarin, *supra* note 42.

apartment, her preferred brand of coffee, whether she lives alone or with others, and the fact that her cat is overweight.

Much of this data is passed over broadband providers or other communications carriers. An Internet of Things device may collect usage data and send it over the Internet to the manufacturer or third parties for various purposes, such as providing services to the consumer, collecting and aggregating data, or assessing quality of service. The Internet carrier potentially sees all of this communication, and likely can deduce from the traffic the nature of the device and potentially even usage patterns.

Others have raised privacy concerns about the capability of individual Internet of Things devices to collect and track information.[48] But communications carriers raise privacy concerns an order of magnitude larger, because they have a purview over *all devices* used by a consumer. While the manufacturer of Sarah's smart refrigerator may learn much about Sarah's eating habits, Sarah's broadband provider could potentially learn of her cat feeding preferences, coffee schedule, and daily routine as well, aggregating the many pieces of information flowing across Sarah's Internet channel.

The panoptic possibilities that the Internet of Things opens up to communications services thus demands strict oversight, if consumer privacy and data security are to be maintained.

The FCC's Communications Privacy Authority Is Critical Here. The Internet of Things highlights just how sensitive communications data can be, and thus it should come as no surprise that Congress has created specific, strong privacy protections against communications carriers misusing such data. These protections are found in Sections 201 and 222 of the Communications Act, which protect so-called "customer proprietary network information," or "CPNI."[49]

[48] *See, e.g.,* Federal Trade Commission Staff, Internet of Things: Privacy & Security in a Connected World 15 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[49] 47 U.S.C. §§ 201, 222 (2012).

Current FCC regulations put tight restrictions on the collection and use of CPNI, which is defined to include administrative network data about a user's communications, including its point of origin, destination, time, and duration.[50] Those regulations prevent communications services from utilizing CPNI for reasons other than providing "the telecommunications service from which such information is derived, or . . . services necessary to, or used in, the provision of such telecommunications service."[51] In other words, broadband providers cannot use the data gleaned from routing a customer's broadband traffic for any purpose that is not essential to providing service. This includes marketing—even when conducted by the broadband provider itself.[52]

The FCC has expressed its intent and dedication to applying these strong privacy protections to broadband Internet services in view of the agency's recent decision to reclassify broadband Internet as a telecommunications service under Title II of the Communications Act.[53] In that decision, the FCC noted that Sections 201 and 222 will apply to broadband providers,[54] because "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth."[55]

Through its CPNI authority, the FCC has proven to be a champion of consumer privacy, taking on massive data breaches by phone companies and rapidly adapting regulations to meet the needs of the times.[56] But there have been concerning efforts to strip this effective agency of this consumer-protective mandate.[57] This Subcommittee should make

[50] 47 U.S.C. § 222(h)(1)(A).

[51] 47 U.S.C. § 222(c)(1).

[52] 47 U.S.C. § 222(b).

[53] *See* Protecting and Promoting the Open Internet, 30 F.C.C. Rcd. 5601 (Fed. Commc'ns Comm'n Mar. 12, 2015) (Report and Order on Remand, Declaratory Ruling, and Order), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

[54] *Id.* ¶ 462.

[55] *Id.* ¶ 54.

[56] *See* Letter from Pub. Knowledge & 11 other organizations, to Michael C. Burgess & Jan Schakowsky, *Data Security and Breach Notification Act of 2015* 2 (Mar. 18, 2015), *available at* https://www.publicknowledge.org/assets/uploads/documents/letter-data-breach-3.pdf.

[57] *See id.* at 1.

efforts to enhance, not impair, consumer privacy in the Internet of Things by protecting the FCC's abilities in this arena.

Clear, direct protections must be applied to CPNI generated by Internet of Things devices. The Subcommittee must remain aware of these and other privacy challenges going forward, as the Internet of Things becomes more ubiquitous, and the expectations of privacy evolve.

V. A Dynamic Internet of Things Requires Spectrum Management That Favors Innovation, Not Incumbents

It is an obvious truism that any device considered part of the Internet of Things must connect "things" to the "Internet." Discussion of the Internet of Things and its evolution all too often elides over this truism without any concern for precisely how this will occur. We must not, however, take this condition for granted. If we neglect this first fundamental precondition—a way for devices to connect cheaply and seamlessly to the Internet and each other—then the Internet of Things will ultimately become stunted and strangled as it chokes on its own success.

By far, the preferred means of connecting devices to the Internet of Things has become wireless. Wireless provides mobility and limits the need for clunky physical connections. Improvement in wireless technologies has facilitated faster and more reliable connections.

A. A Brief Overview of Spectrum Policy In the United States

Access to wireless spectrum capacity (generally referred to simply as "spectrum") is managed in the United States by the Federal Communications Commission (FCC). Until the 1980s, every use of wireless spectrum required a dedicated band of frequencies for a specific purpose and no other. For example, one band for television broadcasting, one band for radio controlled cars, one band for police radios, and so forth.

Changes in technology and the rising demand for spectrum access prompted

Congress and the FCC to rethink the traditional model. By the mid-1990s, the U.S. shifted to making spectrum available primarily in 2 different ways:

- *Exclusive use "licensed" spectrum*, where the FCC auctioned off a limited number of geographic area licenses for general and exclusive use by the winner of the licenses at auction.
- *Unlicensed or "license exempt" spectrum*, where any person could operate a device that conformed to a set of fixed rules, and on the understanding that the device must (a) Not interfere with licensed services; and (b) must accept interference from any source, including other license exempt devices.[58]

The chief benefits of licensed spectrum are (a) protection from interference from other man-made transmitters (there are always sources of natural interference, such as sunspots or lightning, and networks must adjust accordingly); (b) relative high power use; and (c) exclusivity, allowing a relatively few wireless licensees to recoup the high cost of licenses and deployment by excluding other users. Licensed spectrum has become the basis for the cell phone industry. Licenses for spectrum suitable for mobile broadband cost billions of dollars,[59] and the cost of deployment of national wireless networks also runs into the billions. As a result, the United States has only 4 national wireless carriers offering mobile broadband services. Anyone seeking to use these frequencies, whether to connect with the Internet or with other local devices, must lease spectrum from one of these carriers and often must use the carrier's network—which is designed primarily for the over 300 million mobile phone customers in the country.

By contrast, unlicensed spectrum has become the home of practically all other devices using wireless access. Wi-Fi and Bluetooth have become the chief drivers of this enormous expansion of unlicensed devices, although the unlicensed spectrum supports

[58]For history, see generally Harold Feld, *From Third Class Citizen to First Among Equals: Rethinking the Place of Unlicensed Spectrum in the FCC Hierarchy*, 15 CommLaw Conspectus: J. Comm. L. & Tech. Pol'y 53 (2006), *available at* http://commlaw.cua.edu/articles/v15/feld.pdf.

[59]The most recent auction of mobile broadband wireless spectrum, Auction 97, yielded a total of approximately $45 billion in winning bids. *See* Federal Communications Commission, *Auction 97: Advanced Wireless Services (AWS-3)* (last updated Oct. 1, 2014), http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=97.

any number of proprietary or open standards for communications and support billions of non-Internet connected devices such as cordless phones, home security systems, and garage door openers.

B. Unlicensed Spectrum Continues to Be Necessary for Connectivity of the Internet of Things

Despite the advantages of interference protection offered by licensed spectrum, unlicensed spectrum has become the overwhelming source for connectivity for the Internet of Things.[60] Indeed, one may argue that the Internet of Things would be impossible without the ubiquity of cheap license exempt spectrum.

The open nature of license exempt spectrum reduces costs. Today, the number of unlicensed devices far exceeds the number of licensed devices, an inevitable result since nearly all "smart" devices operating on licensed frequencies also include Wi-Fi and Bluetooth capability.[61] This creates fantastic economies of scale, driving down the cost of standard Wi-Fi and Bluetooth chips to almost nothing per device.

The open nature of license exempt spectrum encourages innovation. Because wireless carriers invest billions in their networks, they exercise tight control over what devices may attach to the network, how much data subscribers may use, and other factors relating to the nature and type of traffic. By contrast, no one controls access to license exempt spectrum. This allows for innovation on an unprecedented scale.[62] When

[60] *See Wi-Fi Alliance "Fifteen for 2015" predictions*, Wi-Fi Alliance (Jan. 13, 2015), http://www.wi-fi.org/beacon/wi-fi-alliance/wi-fi-alliance-fifteen-for-2015-predictions ("Wi-Fi leads in smart home, industrial IoT, and connected car."); Richard Katz, Telecom Advisory Servs., LLC, Assessment of the Future Economic Value of Unlicensed Spectrum In the United States (2014), http://www.wififorward.org/wp-content/uploads/2014/01/Katz-Future-Value-Unlicensed-Spectrum-final-version-1.pdf; Richard Thanki, The Economic Significance of License Exempt Spectrum To the Future of the Internet (2012), http://download.microsoft.com/download/A/6/1/A61A8BE8-FD55-480B-A06F-F8AC65479C58/Economic%20Impact%20of%20License%20Exempt%20Spectrum%20-%20Richard%20Thanki.pdf.

[61] *See* Reply Comments of Open Technology Institute at New America, Public Knowledge, Free Press, and Common Cause 8–11, *Office of Engineering and Technology and Wireless Telecommunications Bureau Seek Information on Current Trends in LTE-U and LAA*, 80 Fed. Reg. 26561 (Fed. Commc'ns Comm'n June 26, 2015) [hereinafter LTE-U Comments], *available at* http://apps.fcc.gov/ecfs/document/view?id=60001105564.

[62] *See id.* at 8.

companies in the United States initially began to deploy "smart meters," they opted to deploy in unlicensed spectrum rather than in licensed spectrum because they could do so without either acquiring licenses or partnering with a licensed carrier. As a result, over 75% of the connections using smart meters rely on unlicensed spectrum.[63]

Internet of Things Traffic Is Better Suited to License Exempt Spectrum. Licensed networks have become highly congested with downloads of video traffic and other high-bandwidth latency-sensitive traffic. Wireless carriers have turned to unlicensed spectrum to meet their increasing need for capacity through "Wi-Fi offload" and LTE over unlicensed. As a result, experts predict that Wi-Fi networks will carry as much as 60% of all traffic originating on smartphones by 2019.[64]

Most IP traffic from Internet of Things devices is relatively low-bandwidth and tolerant of the environment of license exempt spectrum. A great deal of Internet of Things traffic involves local area networks, where devices communicate directly to one another rather than routing through a cell tower, traveling through a wireless carrier's network, and being rerouted to a device within the same building, or even the same room. The nature of this Internet traffic from devices is ideally suited to networks using unlicensed spectrum. By contrast, attempted to load this expanding Internet of Things traffic load onto licensed spectrum would result in an unmanageable spectrum crunch for everyone.

All of This Created a Virtuous Cycle that Makes Wi-Fi Ubiquitous. All these factors have combined to create a "virtuous cycle" that has expanded the availability of Wi-Fi and other technologies using shared spectrum rather than exclusively licensed spectrum. The ubiquity of Wi-Fi access points, drives down costs and encourages more innovation. This, in turn, creates more demand, driving costs down further.

---

[63]Yochai Benkler, *Open Wireless v. Licensed Spectrum: Evidence From Market Adoption*, 26 Harv. J.L. & Tech. 69 (2012), *available at* http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech69.pdf.

[64]Andrew Burger, *Juniper: Wi-Fi Offload Will Reach Nearly 60 Percent of Mobile Traffic*, Telecompetitor (June 18, 2015), http://www.telecompetitor.com/juniper-wi-fi-offload-growth-will-reach-nearly-60-percent-of-mobile-data-traffic/.

C. Threats to the Availability of Open Spectrum Threaten the Growth of the Internet of Things

While the availability of license exempt spectrum has driven the dramatic expansion and deployment of the Internet of Things, we cannot assume this happy state will continue forever. To the contrary, two major threats loom on the horizon. First, we are rapidly exhausting our supply of open spectrum available for the Internet of Things, creating a "spectrum crisis" for open spectrum similar to the "spectrum crisis" for exclusive use spectrum that has driven most spectrum policy for the last 5 years. Second, we are seeing the emergence of actors with the technical capability and financial incentive to either block or degrade Wi-Fi and unlicensed spectrum generally. Federal policy must address both these concerns to assure a robust and healthy future for the expanding Internet of Things.

We Need More License Exempt Spectrum Access. In 2010, the National Broadband Plan published by the FCC declared that the supply of available licensed spectrum could not keep pace with the increasing demand. Declaring a national "spectrum crisis" or "spectrum crunch," the FCC called for allocation of 500 MHz of wireless capacity for mobile broadband use, either from federal users or from broadcasters and other commercial users.[65] The FCC gave scarcely a nod to the need to enhance the availability of unlicensed spectrum for Internet of Things or other uses.[66]

In the 5 years since then, federal policy has gradually come to recognize the need to expand access to license exempt spectrum as well as exclusive use spectrum sold at auction. In 2012, the President's Council of Advisors for Science and Technology (PCAST) issued a report proposing that the future of federal spectrum reallocation required a mixed use "sharing model" that would permit federal users to retain adequate access to spectrum to

[65] Fed. Commc'ns Comm'n, Connecting America: The National Broadband Plan ch. 5 (2010), *available at* https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[66] *See id.*

perform vital national security and public safety functions, while providing greater opportunity for non-federal users to access spectrum on both an exclusive and non-exclusive basis.[67] Additionally, the FCC has commenced several proceedings designed to expand the availability and utility of spectrum in the 5 GHz band,[68] promote sharing with federal users as recommended in the PCAST Report,[69] and maximize the utility of license exempt operation in unassigned channels in the broadcast band—the so-called "TV white spaces"—for next generation Wi-Fi.[70]

Unfortunately, the FCC has met with considerable resistance from the automobile industry in the 5 GHz band,[71] and from wireless carriers worried that expanding license exempt access will introduce new competitors to the mobile wireless space. In addition, Qualcomm, which derives the majority of its revenues from patents in the licensed space, has consistently fought to limit expansion of license exempt and shared spectrum where its patent portfolio is weak, and where patenting policies adopted by the relevant standards bodies would prevent Qualcomm from using its patents to exclude rival chipmakers.[72]

Even if all the pending proceedings were completed, however, it would not suffice

[67]President's Council of Advisors on Sci. & Tech., Executive Office of the President, Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth (2012), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf.

[68]Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, 28 F.C.C. Rcd. 1769 (Fed. Commc'ns Comm'n Apr. 10, 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-22A1.pdf.

[69]Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550–3650 MHz Band, 27 F.C.C. Rcd. 15594 (Fed. Commc'ns Comm'n Dec. 12, 2012), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-12-148A1.pdf.

[70]Robert M. McDowell, *The FCC Should Fight for Our Right to TV White Space*, Wired (Apr. 17, 2015), http://www.wired.com/2015/04/fcc-white-spaces-database/.

[71]A portion of the Unlicensed National Information Infrastructure (U-NII) Band was assigned to the auto industry in 1999 for development of collision avoidance systems. This assignment was intended to be shared with unlicensed operations already designated for the band. *See* 28 F.C.C. Rcd. 1769, ¶¶ 92–93. Since 1999, the auto industry has failed to develop any standards or technology suitable for deployment. Since the FCC announced its intent in 2012 to expand the availability of this portion of the U-NII Band for advanced Wi-Fi capabilities, the auto industry has fiercely resisted any rule change that would facilitate deployment of Next Generation Wi-Fi.

[72]*See* LTE-U Comments, *supra* note 61, at 24–26.

to meet the expanding needs of the Internet of Things for the long term. Just as the FCC proposed developing a "spectrum pipeline" for licensed spectrum in 2010, Congress and the FCC should supplement this with a spectrum pipeline for license exempt spectrum. This will require significant rethinking by both the Office of Management and Budget (OMB) and the Congressional Budget Office (CBO) in how to assess the value of opening federal spectrum to sharing. At present, because spectrum auction provide an immediate injection of revenue, OMB and CBO do not assign a positive value to opening federal spectrum for sharing. Given the enormous value of the Internet of Things to the national economy, Public Knowledge recommends that CBO and OMB adopt "dynamic scoring" models to capture the macro-economic benefits of expanding license exempt spectrum access.

Public Knowledge therefore makes the following policy recommendations:

1. The FCC should move expeditiously to complete its proceedings to expand shared access of the 5 GHz band. Auto manufacturers should be required to either demonstrate interference with proposed use of their assigned spectrum, and to propose suitable mitigation measures that will permit enhanced shared access for the Internet of Things.[73]

2. The FCC should move expeditiously to finalize the rules for sharing the federal 3.5 GHz band consistent with the Order adopted in April 2015.[74]

3. Congress should amend Section 922 of the Telecommunications Act[75] to require the Administrator of the National Telecommunications Information Administration (NTIA) and the Chairman of the FCC to identify federal bands suitable for license exempt or otherwise shared operation with non-federal users as part of the National Spectrum Allocation Planning.

4. Congress should direct the Congressional Budget Office to develop and implement a dynamic scoring methodology to reflect the macro-economic benefits of existing

[73]Automobiles already use licensed and unlicensed spectrum as part of the Internet of Things, including anti-collision radar and rear-view cameras, without any deployment by auto manufacturers on the 5 GHz spectrum assigned to them in 1999.

[74]*See* Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550–3650 MHz Band, 30 F.C.C. Rcd. 3959 (Fed. Commc'ns Comm'n Apr. 21, 2015) (Report and Order and Second Further Notice of Proposed Rulemaking), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-47A1.pdf.

[75]47 U.S.C. § 922 (2012).

license exempt access to spectrum, and of expanding license exempt access to spectrum. Congress should further require CBO to use this methodology when assessing all proposals for allocation of spectrum.

We Must Protect the Ecosystem from Those with Incentive to Abuse It.

In the last year, several incidents have come to light that indicate that some actors may have particular incentives to degrade the availability of Wi-Fi or the capacity to use unlicensed spectrum. Because devices using license exempt spectrum are not entitled to any interference protection, there is considerable concern that actors with the incentive to degrade operation of competing services using license exempt spectrum will either deliberately chose to do so, or will deploy technologies indifferent to their overall impact on the ecology of the license exempt space.

Two incidents are particularly noteworthy. First, the FCC brought an enforcement action against Marriott Corporation for deliberately jamming mobile Wi-Fi "hot spots" used by guests to force these guests to pay Marriot for use of Marriott's own Wi-Fi network.[76] Marriott took the position that the FCC lacked the authority to prohibit jamming of devices and networks using license exempt networks.[77] Ultimately, in the face of customer backlash, Marriott withdrew its legal Petition, leaving the question of the FCC's authority unresolved.

More recently, a number of stakeholders (including Public Knowledge) have raised concerns over the planned deployment of LTE over unlicensed spectrum (LTEU) by wireless carriers to supplement their existing LTE deployments on licensed spectrum.[78] Although proponents of LTEU, and of a proposed standard to utilize licensed and unlicensed spectrum simultaneously ("Licensed Assisted Access" or "LAA") insist that LTEU/LAA will not degrade Wi-Fi, stakeholders note that the LTEU/LAA protocols have the capacity

[76] *See* Press Release, Federal Communications Commission, *Marriott to Pay $600,000 to Resolve WiFi-Blocking Investigation* (Oct. 3, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-329743A1.pdf.

[77] *See* Petition for a Declaratory Ruling to Interpret 47 U.S.C. § 333 or, in the Alternative, for Rulemaking, *In re Petition of Am. Hotel & Lodging Ass'n, Marriott Int'l, Inc., & Ryman Hospitality Props.*, No. RM-11737 (Aug. 25, 2014), *available at* http://apps.fcc.gov/ecfs/document/view?id=60000986872.

[78] *See* LTE-U Comments, *supra* note 61.

to degrade Wi-Fi, and that wireless carriers have the financial incentive to do so in the face of competition from cable offering mobile services on their Wi-Fi footprints. Additionally, Qualcomm—the primary chip vendor for LTEU/LAA—has the incentive to shift the standard development process away from the Wi-Fi standards bodies because the Wi-Fi standards bodies have adopted polices that would limit Qualcomm's ability to deny rival chipmakers patents on fair, reasonable and non-discriminatory terms.[79]

The Internet of Things relies on expanding access to license-exempt spectrum, particularly to ubiquitously available technologies such as Wi-Fi, and so this potential for abuse this a matter of grave concern for the future of the Internet of Things. At the same time, regulation of the "unlicensed space" may have unintended consequences with regard to the future of innovation.

Don't Regulate Technology, Police Bad Actors. A straightforward first step would be to clarify that the FCC's existing statutory authority will allow it to sanction actors who either deliberately attempt to degrade traffic using license-exempt frequencies, or who deploy technologies with callous indifference to their detrimental impact on the ecosystem as a whole. Arguably the Communications Act already provides mechanisms for the FCC to do this,[80] but the full Commission has never definitively determined whether the existing statutes provide the necessary authority to police the improper behaviors described above.

This Subcommittee should consider amending the law to clarify that no one may "willfully or maliciously" degrade or block the operation of devices using license exempt or otherwise non-exclusive/shared frequencies. Alternately, the Subcommittee should otherwise prohibit willful or malicious interference with devices operating on license exempt spectrum. In all events, the FCC should be authorized to order remedial steps where

[79] *See id.*

[80] *See* 47 U.S.C. § 333 (prohibiting anyone from "willfully or maliciously" interfering with any signal "licensed or authorized" by the FCC); § 324 (requiring all users of radio frequencies to use the minimum power necessary to complete the desired communication).

it finds that operation of a licensed or unlicensed service would constitute a threat to the unlicensed ecosystem and the Internet of Things.

It is important to understand that the "willful and malicious standard" does not include the standard "harmful interference" which all devices operating on unlicensed spectrum must accept. Nor would it in any way create superior rights of unlicensed devices to licensed devices. "Willful and malicious" are terms directed at *actors*, not at technology. "Maliciously" refers to a deliberate effort to degrade operation for personal gain, such as occurred when Marriott deliberate jammed Wi-Fi hot spots to drive traffic to its own network. "Willfully" refers to actions taken with the clear understanding that deployment creates hazards to the broader ecosystem, but where the individual nevertheless acts with callous indifference and choses to deploy the technology anyway.

Under such a standard, wireless carriers would be free to deploy LTEU/LAA, but with the understanding that deliberate efforts to degrade competing services would result in enforcement actions and sanctions. Additionally, if the deployment of LTEU created widespread interference with Wi-Fi services critical to the Internet of Things, even if carriers did not intend to cause such widespread interference, the Commission would retain the authority to order mitigation measures to protect the unlicensed ecosystem.

VI. Conclusion

As the chairman of this Subcommittee has said, Internet of Things devices "raise both opportunities and questions about regulatory policy, spectrum space, privacy and more."[81] We hope that the considerations outlined in this statement highlight the breadth of those opportunities and questions as policymakers such as the members of this Subcommittee face a fast-changing technological space. We thank the Subcommittee for offering us the opportunity to provide this statement.

Respectfully submitted,

Charles Duan
Harold Feld
Meredith Filak Rose
Sherwin Siy

On behalf of
Public Knowledge

July 29, 2015

[81] Erin Kelly, *Congress Sees Security Risk in 'Internet of Things'*, USA Today, Feb. 9, 2015, http://www.usatoday.com/story/news/politics/2015/02/09/internet-of-things-house-caucus-senate-hearing/22927075/.