Before the National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	Docket No. 160331306-6306-01

COMMENTS OF PUBLIC KNOWLEDGE

PUBLIC KNOWLEDGE
1818 N St. NW, Suite 410
Washington, DC 20036

June 2, 2016

Introduction

Public Knowledge appreciates the opportunity to submit comments in connection with NTIA's request: The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things. The Internet of Things ("IoT") means more software embedded in everyday consumer devices, and an increasing amount of varying types of data travelling among networked devices. Accordingly, IoT poses unique policy challenges impacting competition, innovation, consumer ownership and autonomy, consumer protection, privacy, social and economic equity, and access to limited spectrum resources. As IoT products and services continue to develop, Public Knowledge urges NTIA and the Department of Commerce to consider the wide range of potential effects on the rights and interests of consumers.

These comments touch on many of the different questions published in NTIA's request for comments. However, for organizational purposes, the following responses are specifically addressed to Questions 6 and 15, and 17–19.

Responses to Question 6

Question 6 asks commenters to address technological issues that may hinder the development of IoT, and what the government can do to help mitigate these issues.

In order for IoT to succeed, devices must be able to connect seamlessly and cheaply to the Internet and to each other. In practice, this will largely depend upon wireless communications, which in turn depends upon radio spectrum.

While some IoT devices and services can and do use licensed spectrum, the dominant source of connectivity for IoT is unlicensed spectrum, through technologies

such as Wi-Fi and Bluetooth.[1] Much of the traffic from IoT devices is relatively low-bandwidth and tolerant of the environment of license-exempt spectrum. A great deal involves local area networks and other communications across short distances, where devices can communicate with one another without routing through the internet. The nature of this traffic is well suited to networks using unlicensed spectrum, as opposed to costly mobile broadband networks operating on licensed spectrum. Indeed, it is possible that many IoT applications would never develop at all without a ubiquity of cheap, unlicensed spectrum.

While the availability of license-exempt spectrum has driven recent expansion and deployment of IoT, two major threats loom on the horizon. First is the potential exhaustion of unlicensed capacity available for IoT, creating a "spectrum crisis" for open spectrum similar to the "spectrum crisis" for exclusive use spectrum that has driven spectrum policy for the last 5 years. Second is the emergence of actors with the technical capacity and incentive to either block or degrade Wi-Fi and unlicensed spectrum generally. Federal policy must address both of these concerns to assure a robust and healthy future for IoT.

While the FCC has commenced several proceedings in recent years to expand the availability and utility of unlicensed spectrum, they will likely not be sufficient to meet

[1] *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- nal-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%20anki.pdf.

the long-term demand generated by IoT and other applications.[2] Wireless carriers have turned to unlicensed spectrum to meet their increasing need for capacity through "Wi-Fi offload." As a result, some experts predict that Wi-Fi networks will carry as much as 60% of all traffic originating on smartphones by 2019.[3] Just as the FCC proposed developing a "spectrum pipeline" for licensed spectrum in 2010, the government should supplement this with a spectrum pipeline for unlicensed spectrum. In addition, Public Knowledge recommends the following:

- The FCC should move expeditiously to complete its proceedings to expand shared access of 5GHz band. Auto manufacturers should be required to 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.[4]
- Congress should amend Section 922 of the Telecommunications Act to require the Administrator of 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, and even in the absence of

[2] *See* Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, 2015–2020 (February 3, 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf.

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

[4] 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. 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.

Congressional action, NTIA and the FCC should take such action to the extent allowed by their current authority.

- Congress should direct the Congressional Budget Office to develop and implement a dynamic scoring methodology to reflect the macroeconomic benefits of existing license-exempt access to spectrum and of expanding license-exempt access to spectrum. Congress should further require CBO and the Office of Management and Budget (OMB) to use this methodology when assessing all proposals for allocation of spectrum.

Additionally, several pending bills in Congress could increase the availability of unlicensed spectrum, deserving serious consideration. In particular, the MOBILE NOW Act,[5] if enacted, would identify 255 mHz of spectrum to be made available for broadband, specifying that a minimum of 100 mHz should be for unlicensed use. And the DIGIT Act[6] would direct the FCC and NTIA to evaluate spectrum needs for IoT and what actions are required to ensure sufficient capacity.

Because devices using license-exempt spectrum are not entitled to interference protection, there is considerable concern that actors with the incentive to degrade operation of competing services using license exempt spectrum will either deliberately choose to do so or will deploy technologies indifferent to their overall impact on the unlicensed ecosystem. 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

[5] The Making Opportunities for Broadband Investment and Limiting Excessive and Needless Obstacles to Wireless Act, S. 2555, 114th Cong. (Feb. 11, 2016).
[6] Developing Innovation and Growing the Internet of Things Act, S. 2607, 114th Cong. (Mar. 1, 2016).

spectrum.[7] Although proponents insist that LTEU/License Assisted Access ("LAA") will not degrade Wi-Fi, other stakeholders note that LTEU/LAA protocols have the capacity to do so, and that wireless carriers could benefit from such degradation by inhibiting competing mobile service offered by wireline broadband providers over Wi-Fi. Additionally, Qualcomm–the primary chip vendor for LTEU/LAA – may have an incentive to shift the standard development process away from Wi-Fi standards bodies, which have adopted policies that limit Qualcomm's ability to deny rival chipmakers licenses on fair, reasonable and nondiscriminatory terms.[8]

The FCC's authority should be clarified to allow it to sanction actors who either degrade traffic over unlicensed spectrum deliberately or who deploy technologies with callous indifference to their detrimental impact. Arguably the Communications Act already provides mechanisms for the FCC to do this,[9] but the full Commission has never determined this definitively.

Responses to Question 15

Question 15 asks commenters to address the "main policy issues that affect or are affected by the IoT," and how the government should address those issues. IoT presents exciting new opportunities for innovation, competition, and technological development, but it also presents policy challenges that broadly implicate the rights and interests of consumers. Specific policy issues that affect or are affected by the Internet of Things

[7] *See* Reply Comments of Open Technology Institute at New America, Public Knowledge, Free Press, and Common Cause 24–26, in *Office of Engineering and Technology and Wireless Telecommunications Bureau Seek Information on Current Trends in LTE-U and LAA,* ET Docket No. 15-105 (Federal Communications Commission June 26, 2015) ("LTE –U Comments") *available at* http://apps.fcc.gov/ecfs/document/view?id=60001105564.

[8] *See id.*

[9] *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).

include: patent quality and fairness in patent assertion, ownership rights in electronic devices, the freedom to tinker and to innovate, consumer protection, communications privacy, consumer protection, social and economic equity, and spectrum management.

A. Improving patent quality and preventing abuses in patent assertion

Patent quality and fairness in patent assertion will be central to the successful development and commercialization of IoT products and services. Concern over so-called patent trolls using the economics of litigation to attack small, innovative businesses abound in the news, in the Administration, in Congress, and even in the opinions of the Supreme Court. The problems in the patent system that give rise to these concerns may also threaten IoT innovation. While patents can provide a strong incentive for the development of new technologies, a system rife with overbroad patents and abusive litigation will drive innovation backwards, hampering innovators' efforts and resources and deterring successful commercialization.

IoT is often about connecting multiple physical 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. 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. 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.[10]

[10] 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.

- U.S. Patent No. 6,199,048: Connecting a barcode scanner to a networked computer database.[11]
- U.S. Patent No. 7,324,833: Connecting an iPod to a car.[12]
- U.S. Patent No. 7,343,165: Connecting a GPS to user directory information.[13]
- U.S. Patent No. 7,016,512: Connecting a hearing aid to an electrical plug.[14]

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. Current efforts on patent litigation reform may mitigate this risk, as well as encouraging and facilitating the U.S. Patent and Trademark Office's efforts toward improving patent quality.[15]

B. Discouraging private attempts to undermine consumers' full ownership of their devices

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. It is now embodied in copyright's first sale doctrine and patent law's doctrine of exhaustion. But the right of

[11] 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.
[12] 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.
[13] 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/.
[14] 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.").
[15] See 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), h p://www.uspto.gov/sites/ default/ les/documents/2015quality_a_e _06may2015.pdf.

owners to be free of easements on their things has been attacked in a number of ways using intellectual property law, with particular relevance to IoT.

Manufacturers have frequently attempted to establish that a purchaser of a device with embedded software is not "the owner of a copy" of that software, but merely a licensee. For example, many product manufacturers write End User License Agreements (EULAs) claiming that embedded software is never owned by the user. Under this approach, a rightsholder may condition a license to that software on a user forfeiting certain rights that would otherwise flow from his or her ownership of the physical device. This theory, if successful, could expose a user who violates such contractual restrictions to liability for copyright infringement, notwithstanding the exception contained in 17 U.S.C. § 117(a).[16] Despite concerns that this practice "would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners,"[17] courts have overall upheld the idea that software purchasers may be denied statute as "owners" by virtue of EULAs.[18]

Furthermore, while some courts have stated that §1201 of the Digital Millennium Copyright Act does not "allow any company to attempt to leverage its sales into aftermarket monopolies,"[19] the Library of Congress has, in the past, permitted such

[16] Owners of copies of software are permitted to make whatever new copies of software that are "an essential step in the utilization of the computer program in conjunction with a machine." 17 U.S.C. 117(a)(1). See generally Comments of Public Knowledge and New America's Open Technology Institute, in Software-Enabled Consumer Products Study, Docket No. 2015-6 (Copyright Office February 16, 2016), available at https://www.regulations.gov/#!documentDetail;D=COLC-2015-0011-0012
[17] *MDY Indus., LLC v. Blizzard Entm't, INc.,* 629 F. 3d 928, 941 (9th Cir. 2010).
[18] *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.
[19] *Chamberlain Group, Inc. V. Skylink Techs., INc.,* 381 F.3d 1178, 1201 (2004).

restrictions, for example, by denying consumers the right to unlock their cellphones to use them with multiple mobile phone networks.[20]

These efforts to restrict ownership directly harm consumers, who typically value the freedom to use their purchase products without post-sale restrictions. Full ownership rights for purchased devices confer numerous societal and economic benefits. For example, they avoid unnecessary administrative costs of tracing the trail of restrictions on any given product. They open the door to secondary markets like eBay. And they protect against the anti-competitive harms from post-sale lock-in with exclusive platforms and suppliers.

One legislative approach to protecting consumers' ownership interests is the You Own Your Own Devices (YODA), which provides that a consumer is allowed to sell a device containing operating software regardless of any contractual provisions on the right to resell such software.[21]

C. Supporting consumer freedom to tinker and to innovate

Ownership rights in Internet of Things devices are the essential prerequisite to the "freedom to tinker": the ability of consumers to use, inspect, repair, modify, and improve upon their devices, in ways not contemplated by or even contrary to the interests of the original manufacturers. The freedom to tinker is important because it is often a well-spring of productive innovation. As one survey found, "millions of citizens innovate to create and modify consumer products to better fit their needs."[22] The resulting user-

[20] *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), *repealed*, Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144, 128 Stt. 1751 (2014).
[21] You Own Devices Act, H.R. 862, 114th Cong. (Feb. 11, 2015).
[22] 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/20-13/08/smr-art-as-pub.pdf.

driven innovations become an "unexpected 'front end' of free innovation designed to serve as an important feedstock to commercial innovation processes in a wide variety of fields."[23] Freedom to tinker therefore does not only benefit the tinkerers, but often manufacturers and the public as a whole. However, many manufacturers seek to curtail such rights.

In addition to the attacks on ownership rights discussed above, the anti-circumvention provisions of the Digital Millennium Copyright Act provide another avenue for extinguishing the freedom to tinker. By placing technological protection measures on consumer products and using 17 U.S.C. § 1201 to prevent consumers from circumventing those measures, manufacturers may also dictate what consumers can and cannot 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,[24] and a garage door opener manufacturer disallowing its customers from using aftermarket clicker transmitters.[25] These attempts at control have not lessened over the past decade, as filings and testimony at last 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. [26]

NTIA should consider the potential impact of § 1201 on IoT devices, including various proposals to limit its misapplication. These include legislation such as the

[23] *Id.* at 29.
[24] *See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).
[25] *See Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).
[26] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Notice of Proposed Rulemaking, 79 Fed. Reg. 73856 (noting receipt of forty-four petitions for exemptions), http://www.copyright.gov/fedreg/2014/79fr73856.pdf.

Unlocking Technology Act[27] and the Breaking Down Barriers to Innovation Act, [28] as well as legislative and administrative changes that would make it easier to obtain an exemption from anti-circumvention prohibitions, to keep that exemption over time, and to seek the assistance of technical experts in carrying out the exempted activity. Furthermore, the government should encourage efforts to limit the impact of anti-circumvention prohibitions on security research.

Responses to Question 17

Question 17 asks how the government should "address or respond to privacy concerns about the IoT."

IoT raises numerous privacy and data security concerns based on the quantity and granularity of data communicated by software-enabled devices. Even when anonymized by stripping out personally identifying information, data can nevertheless reveal the identity of individuals through an analytic process called "deanonymization."[29] A 2012 investigation revealed that the big-box chain Target, through aggregation of personal data, was able to determine whether young women were pregnant — at times even before they or their parents knew.[30] And the potential for revealing data only increases as IoT

[27] Unlocking Technology Act of 2015, H.R. 1587, 114th Cong. (Mar. 24, 2015).
[28] Breaking Down Barriers to Innovation Act of 2015, S. 990, 114th Cong. (Apr. 16, 2015), and H.R. 1883, 114th Cong. (Apr. 16, 2015).
[29] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716–22 (2010), http://www.uclalawreview.org/pdf/57-6-3.pdf (describing several examples of anonymized datasets where individual records were reidentified with individuals); Petition for Declaratory Ruling at 6–8, In re Petition of Pub. Knowledge et al. for Declaratory Ruling Stating that the Sale of Non- Aggregate Call Records by Telecomms. Providers without Customers Consent Violates Section 222 of the Commc'ns Act, WC Docket No. 13-306 (FCC Dec. 11, 2013).
[30] *See* Charles Duhigg, *How Companies Learn Your Secrets,* N.Y. Times Mag. (Feb. 16, 2012), h p://www.nytimes.com/2012/02/19/magazine/shopping-habits.html ("As [Target's researcher Andrew] Pole's computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a 'pregnancy prediction' score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very speci c stages of her pregnancy.").

devices become more prevalent. Such devices install within a person's household numerous small computers in thermostats, refrigerators, door locks, and other devices. Many of these small computers communicate on the Internet, oftentimes without knowledge or consent of their owners, and these communications may not be encrypted.[31]

IoT devices thus provide broadband internet access service (BIAS) providers a new opportunity to collect a valuable category of data. These providers are in a position not only to learn what devices the subscriber owns but potentially much of the information they transmit. Because the online activities of these devices are not always fully understood by their owners, a BIAS provider could easily know more information about subscribers than the subscribers ever believed they had revealed. Accordingly, the volume of information passed from a subscriber through a BIAS provider provides an enormous opportunity for the collection of private information. No wonder, then, that a leading scholar described such providers as being "the single greatest point of control and surveillance."[32] These possibilities should raise significant concerns and highlight the need for close attention to how to oversee BIAS providers' use of subscriber information.

Sections 201 and 222 of the Communications Act protect so-called "customer proprietary network information," or "CPNI."[33] In its current privacy proceeding, the FCC is considering whether to require customer consent before traffic data may be sold

---

[31] *See Nick Feamster, Who Will Secure the Internet of Things?,* Freedom to Tinker (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of- things/ (noting several Internet of Things devices transmitting video, ZIP codes, and other sensitive data without encryption); Lorenzo Franceschi-Bicchierai*, Nest thermostat Leaked Zip Codes Over the Internet*, Vice: Motherboard (Jan. 20, 2016), http://motherboard.vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet ("Some smart devices have such li le computing power that they couldn't perform the necessary en-cryption processes even if their creators wanted them to . . . .").

[32] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1423.

[33] 47 USC §§ 201, 222 (2012).

or transferred by the ISP.[34] The FCC's authority and active enforcement in this area should be supported and encouraged.

Responses to Question 18

Question 18 asks about other consumer protection issues raised by IoT. Here, the issue of product liability is worth consideration.

In the software industry, vendors typically disclaim liability for defects in their products through boilerplate language in sales contracts and licensing agreements. This has led to an anomalous situation in which software vendors may have a unique ability to exempt themselves from consumer protection laws that are otherwise universally applicable. For example, the toy company VTech has recently declared that it is not liable for defects in its software-embedded products that put the safety and privacy of children at risk.[35] The manufacturers of toy trains and blocks by contrast do not have the ability to put dangerous products into the market while shielding themselves from liability. While the legal justifications that allow for such disclaimers are suspect (that shrink-, click-, or browse-wrap contract should be enforceable, or that owners of copies of software require special permission to run the software), in the case of pure software products, there may be valid policy arguments as to why software developers should perhaps not be subject to the same levels of tort liability for defects. General-purpose software may be put to uses the developer can't predict, and may run on computers of various configurations. Holding developers to a standard of, for instance, strict liability in

[34] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 F.C.C. Rcd. 2500 (2016) (Notice of Proposed Rulemaking).
[35] Lorenzo Franceschi-Bicchierai, *Hacked Toy Company VTech's TOS Now Says It's Not Liable for Hacks*, MOTHERBOARD (Feb 9, 2016), http://motherboard.vice.com/read/hacked-toy- company-vtech-tos-now-says-its-not-liable-for-hacks.

such circumstances could chill innovation and simply deter software from being written at all.

However, to the extent that such arguments have merit when applied to software *per se*, they are inappropriate as applied to traditional product liability. A manufacturer or seller should not be able to evade what would otherwise be their responsibilities under the law merely because their products now contain software. Considering how many consumer products do or shortly will contain software, allowing vendors or manufacturers to do this would nullify decades of statutory and common law protections that were designed to protect consumers from poorly-designed or defective products and negligent commercial practices. In the context of a consumer product whether a defect is related to software should not make a difference in a liability analysis.

Responses to Question 19

Question 19 asks commenters to address the ways in which IoT could "affect and be affected by questions of economic equity."

It is difficult to predict the precise ways in which IoT will help and/or hurt disadvantaged communities, which will depend upon the continued technological development of particular applications and their associated economics. That being said, many commenters have already expressed worries that the growth of IoT will worsen the significant digital divides that already exist today, in the availability, affordability, and adoption of internet service and internet-connected technologies.[36] Public Knowledge shares this concern.

[36] Pew Research Center, *The Internet of Things Will Thrive by 2025*, at 58 (May 14, 2015), available at http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

Any IoT product or service with significant economic or social benefits has the potential to exacerbate inequities if adoption is limited by demographics, income, geography or otherwise--for example, if IoT products significantly improve the health, productivity, and ease of life of their users, but are only widely available to wealthier individuals. Similarly, if IoT applications are only available to wealthier municipalities to improve environmental quality and transportation infrastructure, the disparities in opportunity and quality of life relative to lower-income communities will only increase.

At a minimum, these concerns underscore the need for greater efforts to reduce digital divides in broadband internet access. A 2015 survey found that only 41% of households with annual incomes of less than $20,000 have broadband service at home--a decline from 46% in 2013.[37] In this same group, an additional 21% of households had mobile internet access through a smartphone.[38] But it is uncertain at best whether the most valuable consumer IoT applications will be available to users with smartphone-only internet access. And in any event, 38% of households in this group were without either a home or mobile internet subscription.[39] While there may be ways around this barrier to IoT adoption--for example, if data service is bundled with a physical device--in practice, NTIA should assume that households without dependable broadband access are very likely to be left behind in the adoption and resulting benefits of IoT, at least for consumer-facing applications. The equitable effects of IoT thus depend on the

[37] Pew Research Center, *Home Broadband 2015*, at 2 (December 21, 2015), available at http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf.
[38] *Id.*
[39] *Id.*

government's larger commitment to the principle of universal service in the internet age.[40]

[40] *See* Public Knowledge, *Universal Service in an All-IP World* (May 2015), available at https://www.publicknowledge.org/assets/uploads/blog/USF_Paper_-_Jodie_Griffin.pdf.