Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

May 23, 2016

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: IOT RFC 2016
Washington, DC 20230

Re: Docket No. 160331306-6306-01, RIN 0660-XC024

Dear Sir/Madam:

I am submitting comments in response to the notice and request for public comment (RFC)[1] referenced above on behalf of Consumer Federation of America (CFA), a nonprofit association of consumer organizations across the United States. CFA was established in 1968 to advance consumers' interests through research, education and advocacy. CFA appreciates the request by the U.S. Department of Commerce (DOC) for input on the benefits, challenges, and potential role of government as it seeks to foster the advancement of the Internet of Things (hereinafter referred to as the IoT).

The IoT raises a number of important consumer issues, including privacy, security, transparency, digital rights, sustainability, choice and redress. From CFA's perspective, the DOC's main focus should be on helping to develop technical standards for interoperability and security in the IoT, areas in which it has considerable expertise.

While the DOC is not a privacy or consumer protection agency, CFA believes that it can play a constructive role in other ways as well. The DOC should support legislation that would provide individuals with strong, enforceable privacy and security rights and give the Federal Trade Commission (FTC) the rulemaking authority that it needs to adequately protect consumers and provide clear rules of the road for businesses. The DOC should also use its relationship with the business community to promote policies and practices aimed at ensuring that individuals have the tools they need to use IoT products and services properly, are treated fairly in the deployment of the IoT, and have effective means of redress when they encounter problems. In these comments, we also note what other federal agencies are doing, and could do, to ensure that the IoT truly benefits consumers.

We have chosen to respond specifically to questions 1. and 15. in the RFC, but many of the points we make are relevant to other questions that the DOC poses.

[1] www.federalregister.gov/articles/2016/04/06/2016-07892/the-benefits-challenges-and-potential-roles-for-the-government-in-fostering-the-advancement-of-the.

Question 1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?

The opportunities that the IoT can provide to enhance health care, energy efficiency, safety, convenience, consumers' experiences and decision-making, and responsiveness to consumers' needs are well-described in a recent report by Consumers International (CI)[2] and were also explored in the public workshop that the FTC convened and its subsequent report on the IoT.[3] CFA's comments will focus on the challenges that the IoT poses, specifically in the business-to-consumer context. These challenges are not necessarily new or different, but they have not been adequately addressed previously, and the IoT complicates and exacerbates them, adding new urgency to address them.

Privacy

A history of information privacy law published by Daniel Solove in 2006[4] dates the principle that the home is one's castle to 1499 and describes the large role that technology has played in the emergence of privacy laws over time. More recently, much has been written, by the White House,[5] the FTC[6] and others about the benefits and risks of "big data," as advances in technology have facilitated the collection of vast amounts of information about individuals and its analysis in real time, for a wide variety of uses, often without the data subjects' knowledge or consent.

The challenge of protecting individuals' fundamental rights to privacy rises to a new level with the IoT, as sensors and software embedded into objects turn them into tracking devices. Information about people's most intimate activities – what they do in their homes, where they go and the transportation they use to get there, their health and fitness, how they entertain themselves, and more – can be compiled across platforms and devices, analyzed instantly, and used with few legal constraints.

---

[2] Consumers International, *Connection and Protection in the Digital Age*, April 2016, www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf.

[3] Federal Trade Commission, *Internet of Things, Privacy & Security in a Connected World*, January 2015, www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[4] Daniel J. Solove, *A Brief History of Privacy Law*, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

[5] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[6] Federal Trade Commission, *Big Data, a Tool for Inclusion or Exclusion?* January 2016, www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

Inferences drawn from this data may not be accurate; even if it is, its use may be unfair.[7] The expanding system of surveillance which the IoT will help to facilitate is largely invisible and outside of individuals' control.

Security

Security, a serious challenge with today's technology, is an even greater concern with in the IoT because the consequences of security failures may be greater. As CI points out in its report:

> "Hacking and disrupting services such as a telecoms provider causes distress and damage, but the prospect of a hacked vehicle or home security system could bring a whole new level of consequences – like losing control of your car or opening up your home to criminals."[8]

Consumers already struggle with updating their software; a 2012 survey showed that 42 percent of American adults failed to do so when first prompted, and a quarter of survey respondents did not know why it is important to do the upgrades.[9] With more software-embedded products, consumers will have more updates to contend with.

Manufacturers' failures to identify and remedy vulnerabilities is also a serious concern. A 2014 Hewlett Packard study[10] revealed that 70 percent of the most commonly used IoT devices contained vulnerabilities that threatened their security.

Given the interconnected nature of the IoT, the consequences of such vulnerabilities can be far-reaching. Infiltration of a connected home network, for instance, could open the doors, literally and figuratively, to its contents, including personal data, and also result in physical damage to devices and other property. While the focus of our comments is on IoT products and services for consumers, it is easy to imagine the havoc that could be caused if IoT systems at power companies, financial institutions, health care providers, government agencies and other organizations are vulnerable to security threats.

Transparency

The lack of transparency and clarity about how products and services work is another "pre-existing issue" that is exacerbated by the IoT. Providing consumers with clear, complete and accurate information about products and services, at the appropriate time and in an easy-to-understand form has always been a challenge. As products and services become more complicated, however, it is even harder

---

[7] See *Civil Rights Principles for Big Data*, 2014, www.civilrights.org/press/2014/civil-rights-principles-big-data.html; Executive Office of the President, *Big Data and Differential Pricing*, February 2015, https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf; Robinson + Yu, *Civil Rights, Big Data and our Algorithmic Future*, September 2014, https://bigdata.fairness.io/wp-content/uploads/2014/11/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_v1.1.pdf; Bob Gellman and Pam Dixon, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future,* April 2014, https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

[8] Page 31, www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf.

[9] http://blogs.skype.com/2012/07/23/intl-tech-upgrade-week/.

[10] http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VytW0iGAtQI.

for consumers to understand how they work. This problem is compounded by the use of technical jargon and legalese that is incomprehensible to the average person. Furthermore, disclosures may lack information that is particularly important in the context of the IoT, such as the length of time that technical support will be provided, the privacy policy, and the consequences of malfunctions, power failures, product or service terminations, or consumers' decisions not to agree to certain terms or to use certain features.

For instance, CFA recently heard from a California consumer who purchased a forced-air gas heater for his home, which came with a thermostat connected to the Internet. After the system was installed, he was asked to create an online portal for the thermostat and give the installer access to it so that any operational problems could be quickly detected and fixed. This would also give the installer access to all of the information about the system, however, including the homeowner's settings, when the settings are changed, when the system is running and in what mode. His concern was that if he set the thermostat to vacation mode, the installer would be able to see that and determine that the family was probably away - making the home a target for theft. The installer told him that if his refusal would negate the warranty. Had he known that, he would not have purchased the system.

This example illustrates another question: who is responsible for making the disclosures? This is unclear, given the multiple parties that can be involved in IoT-related products and services: manufacturers, retailers, software developers, installers, Internet service providers, utilities, affiliates, third party business partners, payment services, data brokers, analytics companies and others, some of which may not be directly consumer-facing.

Digital Rights

The increasing array of digital products and services have already raised questions about who actually owns them, who controls them, and what measures should appropriately be taken to enforce the intellectual property rights that pertain to them. Can consumers resell e-books? Can they use digital music they have purchased on multiple devices? Are geographic limits on the functioning of DVDs fair?[11] As embedded software makes more and more products "smart," including products such as televisions and refrigerators which will were not digital previously, and connectivity gives them new functionalities, consumers will confront digital rights issues that they might not expect and that limit ability to use the products as they wish, to have them repaired by whomever they choose, and to transfer them to others.

CI's report also raises other issues. One is that software licensing can limit interoperability and "lock people into a vendor's ecosystem of products and systems."[12] Consumers who want to take advantage of add-ons or other innovations in the marketplace may find it difficult to do so because the IoT platform that they are using will not allow it. Another is that legal and technical frameworks can limit the ability of consumers to port their data between providers. Consumers who have generated data with devices about their energy use or fitness and want to or move that data to another device or

[11] This issue gained some notoriety when DVDs from the U.S. that President Obama presented as a gift to UK Prime Minister Brown could not be played because of regional restrictions, see www.telegraph.co.uk/news/newstopics/mandrake/5011941/Gordon-Brown-is-frustrated-by-Psycho-in-No-10.html

[12] Page 37, www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf.

combine it with other data, for instance, may be legally and/or technically prevented from doing so. Again, these issues are not unique to the IoT, but IoT users will certainly encounter them.

Sustainability

While no one expects products and services to last forever, given the networked nature of the IoT and the cost of some of the devices, the impact on consumers when components are no longer supported or simply cease to function can be significant. The decision by Nest, now owned by Google, to shut off its Revlov smart home hub is a cautionary tale.[13] As of May 15, 2016 this $300 item has been rendered unusable by the company, and it does not have a similar product to offer. Who decides when a product or service can no longer be used? Is there a minimum amount of time that a consumer should reasonably be expected to be able to use it? If the product or service ceases to function, what effect could that have on other products or services that that the consumer uses?

Some of these questions have arisen in the transition from copper-wire to IP-enabled telephone service. Consumers complain that when their copper-wire service needs repair, they are being forced to switch to IP-enabled service instead. There have also been problems with IP-enabled service not working with consumers' existing security alarm systems. Carriers argue that it is difficult to find the parts or technicians with the requisite expertise to fix the old lines. In the rapidly evolving IoT marketplace, products and services may become obsolete quickly.

Choice

Whether consumers can choose not to participate in the IoT is an important issue. The mandatory deployment of smart meters and time of day electricity pricing, for instance, has generated much debate.[14] Not all consumers will benefit from these types of technologies. Some may believe that there are better ways to achieve their goals or the greater societal good. Some may decide that the risks to privacy or other concerns outweigh the benefits. Some may not have Internet access. And some may simply not want to have these products or services at all. CI observes, however, that the IoT could become so pervasive, or economic and other pressures may become so great, that the use of IoT "becomes a pre-requisite for accessing essential services."[15] We have certainly seen the shift towards providing consumer assistance and services through the Internet in the last decade; the IoT is likely to propel that trend further, leaving consumers with no real choice.

Redress

The complexity of the IoT ecosystem can make consumer redress, which is already challenging, more difficult. With so many players involved, who is responsible if something goes wrong? Does it depend on the nature of the problem? What are consumers' rights? In our home heating system example, for instance, can the consumer return it to the retailer because he would not have purchased it if he knew about the terms of use of the thermostat? Or should he be able to return only the thermostat? Should the warranty cover the system even though the installer will not get automatic alerts about

[13] http://mashable.com/2016/04/04/revolv-smart-home-shutdown/#R6zi.FfIePqI.
[14] See www.aarp.org/politics-society/advocacy/info-03-2011/smart-meter-benefits-questioned-ca.html
[15] Page 38, www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf.

malfunctions through the online portal, which might result in more severe damage than would have been the case if a problem could have been detected more quickly?

CFA is also concerned about forced-arbitration clauses buried in the terms of service that seek to prevent consumers from going to court to enforce their rights. These are becoming common in many types of products and services. The use of "gag" clauses in contracts and terms of service that threaten consumers with financial penalties if they post negative reviews or complain to organizations or agencies about a company's product or service is another tactic aimed at deterring consumers from seeking redress.

Question 15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

CFA's response to question 1. outlines what we believe are the main policy issues in the business-to consumer context. We will offer some suggestions for how the government should address them. Many of these recommendations are not specific to the IoT.

Privacy

The current U.S. government approach to privacy, which relies on narrow sectoral laws and self-regulation, leaves huge gaps and does not provide individuals' with effective protection. CFA applauded the basic concepts for a consumer privacy bill of rights that were articulated in a 2012 White House paper.[16] The bill[17] that was drafted at the DOC to implement it, however, was roundly rejected by CFA[18] and other leading consumer and privacy organizations. Instead of providing individuals with clear, actionable rights concerning the collection and use of their personal information, it took the approach that businesses and organizations should determine if their data practices would pose risks of harm to individuals and, if they did, what steps to take to address those risks. It would have preempted stronger state privacy laws, made it harder for state authorities and the FTC to stop privacy abuses, and barred individuals from bringing their own lawsuits to protect their privacy. In short, the bill would have done little to change current practices and would actually weaken privacy protection in the U.S. rather than strengthen it.

Another aspect of the bill that we found very troubling was that it would have given voluntary codes of conduct that are produced from the DOC's "multi stakeholder processes" (MSP) an presumption of adequacy that is not merited. CFA's experience with the MSPs on mobile app privacy disclosures and facial recognition were exercises in frustration and futility. CFA declined to endorse the model privacy disclosures that emerged from the mobile app MSP because we believed that they were inadequate and misleading.[19] To our knowledge, these disclosures have never been tested to determine if they accurately describe participating apps' actual data practices or if consumers correctly understand what

[16] The White House, *Consumer Data Privacy in a Networked World*, February 2012, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[17] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[18] See http://consumerfed.org/press_release/cfa-statement-on-the-administrations-consumer-privacy-bill-of-rights/.
[19] See http://consumerfed.org/press_release/cfa-on-the-ntia-short-form-notice-code-of-conduct-to-promote-transparency-in-mobile-applications/.

they mean. And after participating in the facial recognition MSP for more than a year, CFA[20] and every other consumer and privacy group[21] walked out when it became clear that no consensus could be reached on basic issues such as whether individuals' consent should be required. That process is still limping along but we doubt that it will provide meaningful protection for individuals. The DOC has just concluded an MSP concerning privacy, transparency, and accountability issues regarding commercial and private use of unmanned aircraft systems.[22] We have not evaluated the best practices that were agreed to, but we note that very few consumer or privacy groups participated in the process.

The DOC is not the right place to develop U.S. privacy policy. It is not a privacy or consumer protection agency. Its mandate is to promote business, and businesses are its core constituents. The MSPs are not balanced, with corporate interests far outnumbering nonprofit consumer and privacy advocacy groups. From CFA's perspective, what the businesses and trade groups that participated in the mobile app and facial recognition MSPs wanted was to produce codes of conduct that placed no restrictions on their current or future data practices and would provide them with legal safe harbors.

This is not to say that stakeholders cannot provide useful guidance for businesses. Indeed, CFA has convened stakeholders to develop best practices for companies that provide identity theft services[23] and provided input IoT Trust Framework[24] that was produced earlier this year through a stakeholder process organized by the Online Trust Alliance (OTA). Focused specifically on home connected devices and health wearables, the Framework makes several good recommendations on privacy, including that the data collected should be limited to what is reasonably useful for the functionality and purpose for which it was collected and that collection for other purposes should be based on consumers' opt-in consent.[25]

While efforts such as this are helpful, they are not sufficient by themselves to protect Americans' privacy. The U.S. Congress should enact a comprehensive data protection law. In a recent study[26] by the Pew Research Center, 68 percent of Internet users said that current laws are not good enough to protect people's privacy online, 64% want the government to do more to regulate advertisers, and most expect at least some limits on how long their data is retained. Of particular relevance to the IoT, only 27 percent said that it would be acceptable for a smart thermostat to collect information about people's comings and goings in return for energy savings.

A comprehensive data protection law should recognize individuals' fundamental rights to privacy, require them to be given meaningful control over their personal information, prohibit practices that take advantage of vulnerable individuals or unfairly discriminate against them, empower the Federal Trade Commission to promulgate rules, and provide for private rights of action so that individuals can

---

[20] See http://consumerfed.org/press_release/statement-by-susan-grant-on-the-decision-to-withdraw-from-the-ntia-process-to-develop-a-voluntary-code-of-conduct-for-companies-using-facial-recognition-technology/.
[21] See http://consumerfed.org/pdfs/6-16-15%20Privacy%20Advocates%20Statement%20on%20NTIA%20Facial%20Recognition%20Process_Comments.pdf.
[22] https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.
[23] Consumer Federation of America, *Best Practices for Identity Theft Services Version 2.0*, November 2015, http://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf.
[24] See https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf.
[25] *Id*, page 3, #18.
[26] See Lee Rainie, *The state of privacy in America: What we learned*, Pew Research Center, January 20, 2016, www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

enforce their rights. A federal privacy law should also allow states, which can act more nimbly and test different approaches (and some of which have already enacted privacy laws) to require stronger protections if they deem it necessary to do so. The DOC should strongly support such legislation because it will make consumers more confident about how their personal information will be handled when they interact with businesses, particularly online and in using IoT products and services.

The FCC's recent proposal[27] for broadband Internet privacy rules is another important step in providing needed protection for individuals and clear rules of the road for businesses. Internet service providers are in a unique position to capture and use information about their customers' online activities. In the context of the IoT, they may be privy to personal information that they never collected previously, such as data about customers' energy use. It is crucial for individuals to be able to control whether their Internet service providers can use the personal information that can be gleaned by virtue of their relationship can be used for any purposes other than providing them with access to the Internet. The DOC should support the FCC's proposed broadband Internet privacy rules.

In addition to providing legal certainty in the U.S., a strong framework of privacy laws and regulations here will help American companies with the challenge they face as they seek to expand their businesses abroad. The debacle of the Safe Harbor illustrates this point. This agreement between the U.S. government and the European Commission, and administered by the DOC, was designed to enable U.S. companies to process the personal data of EU citizens despite the fact that the U.S. law does not provide equivalent privacy protection. In 2015, it was invalidated as insufficient by the highest court in Europe, leaving U.S. businesses scrambling. The newly-negotiated replacement, the Privacy Shield agreement, has already come under fire before it has even been implemented and in our view will ultimately meet the same fate as the Safe Harbor.[28] The U.S. cannot successfully paper over the fact that it lags behind most of the rest of the world when it comes to privacy protection.

Security

Both privacy and security should be built in to IoT products, services and systems. The National Institute of Standards and Technology (NIST), an agency within the DOC, has been in the forefront of work on cybersecurity. In a recent speech,[29] Dr. Willie E. May, Under Secretary of Commerce for Standards and Technology and Director of NIST described how the agency is "leading the way toward a trusted IoT infrastructure through both lab-based physics, engineering and cybersecurity research." He also explained how NIST's National Cybersecurity Center of Excellence works with industry to provide standards-based solutions for cybersecurity problems. Through its laboratories, technical expertise, and collaboration with industry, NIST is trying to ensure that privacy and security are protected as connectivity expands. CFA applauds these ongoing efforts.

In addition to agencies such as NIST, stakeholder groups have developed guidelines concerning security. For instance, the OTA IoT Trust Framework[30] provides a number of recommendations about security, some of which are quite technical. Since standards must be updated as technologies evolve and new

[27] See https://www.federalregister.gov/articles/2016/04/20/2016-08458/protecting-the-privacy-of-customers-of-broadband-and-other-telecommunications-services.
[28] See Transatlantic Consumer Dialogue resolution on the Privacy Shield proposal, April 7, 2016, http://tacd.org/wp-content/uploads/2016/04/TACD-Resolution_Privacy-Shield_April163.pdf.
[29] See www.nist.gov/director/speeches/mays-iot-remarks-22516.cfm.
[30] https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf.

threats emerge, it does not make sense for Congress to set technical specifications for security. However, Congress should consider requiring businesses to meet certain general security obligations, such as conducting risk assessments, designing and implementing programs to adequately manage risk, providing security training for employees, conducting periodic vulnerability tests, and ensuring that service providers and business partners follow appropriate security practices.

It would also be helpful to give the Federal Trade Commission, which has been challenged in using its general unfair or deceptive acts or practices authority to bring security-related enforcement actions,[31] the ability to promulgate rules for security and effectively enforce them. Consumers should be able to enforce their security rights as well. As in privacy, a federal law concerning security should create a floor, not a ceiling, allowing states to require stronger protections if needed.

Transparency

The FTC enforces rules and provides guidance on advertising and marketing, including online advertising and marketing.[32] While there are no specific rules concerning advertising, marketing or sales of IoT products and services, the FTC's general authority prohibiting unfair or deceptive acts or practices applies and its ".com Disclosures"[33] provides guidance on making clear and conspicuous disclosures in digital advertising. Importantly, that guidance warns that disclosures that are necessary to prevent deception or unfairness should not be buried in the terms of service, since it is highly unlikely that consumers will read them.[34]

We wish to highlight here some of the transparency recommendations in the OTA IoT Trust Framework. One is to disclose what features will fail to function if connectivity becomes disabled or is stopped, including the potential impact to physical security.[35] Another is that consumers should be able to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase.[36] This would have certainly been helpful to the California consumer whose dilemma we described earlier in these comments. A third transparency recommendation is that whenever the opportunity is presented to decline or opt out of any policy, the consequences of doing so must be clearly and objectively explained, including any impact to product features or functionality.[37] It might be useful for the FTC to issue guidance for marketing IoT products and services, including examples of types of information that would be particularly important to disclose and who, among the many parties involved, should make the disclosures.

---

[31] See press release about FTC settlement with Wyndham Hotels and Resorts, https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment. The FTC offers many resources with advice for businesses about security at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

[32] https://www.ftc.gov/tips-advice/business-center/advertising-and-marketing/online-advertising-and-marketing.

[33] https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

[34] *Id,* page 18.

[35] See https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf, page 3, #19.

[36] *Id*, page 3, #25.

[37] *Id*, page 4, #27.

Digital Rights

The CI paper on the IoT uses an example involving John Deere tractors to how a traditionally non-digital product takes on a different character, and gives rise to digital rights issues when it becomes embedded with software. In 2015 as part of a routine review of exemptions from non-circumvention rules, the U.S. Copyright Office proposed that technological protection measures (TPMs), which block unauthorized access and modification, should be allowed to be circumvented in the case of agricultural equipment so that the owners could make changes or repairs without restrictions, such as getting the manufacturer's permission.[38] John Deere vigorously objected, stating that a "vehicle owner does not acquire copyrights for software in the vehicle and cannot properly be considered an 'owner' of the vehicle software."[39] The vehicle owner, John Deere asserted, only receives an implied license to operate the vehicle for its lifetime, subject to contractual terms – in other words, the farmer has the right to use the tractor but doesn't really own it to do with it what he or she wants. In the end, the Copyright Office granted an exemption but with some limits – it did not allow the tractor owner to circumvent TPMs for the software programs concerned with the entertainment system, for instance.

Similarly, there are often restrictions on the use and transfer of copyrighted digital content, such as music and e-books. These restrictions are set forth in one-sided user licensing agreements. Digital rights management (DRM) tools can be used to enforce these restrictions by disabling certain features, locking devices, or erasing content. CI's report notes that the Internet of Things has the potential to expand the reach and scope of DRM to more products. As an example, it cites an incident in which a woman was unable to drive her daughter to the hospital emergency room because she was delinquent on her car payments and the lender used a "starter interrupt device" embedded in her car to remotely prevent her from starting it.[40]

Interoperability and portability are also largely under the control of business interests. Consumers' ability to do things such as transfer a connected energy or security system to new owners when they sell their homes, connect competing products to IoT platforms, transfer their data to new IoT devices, and have IoT products repaired by independent services is controlled by contract terms that are not negotiable, that may be inherently unfair, and that can restrict competition.

The U.S. Copyright Office should ensure that there are reasonable exemptions from non-circumvention rules, but much more must to be done to strengthen consumers' digital rights. While we agree with the best practice in the OTA IoT Trust Framework that if and how IoT device product/service/ownership may be transferred to a new owner should be publicly disclosed,[41] notice is not enough to address this and other digital rights issues.

As far back as 2008, the Transatlantic Consumer Dialogue, a forum in which U.S. and European consumer organizations develop policy recommendations for how their governments should address

[38] See http://copyright.gov/1201/
[39] http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf, page 5.
[40] http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/
[41] *Supra*, page 3, #21.

consumer issues, issued a "Charter of Consumer Rights in the Digital World",[42] which makes a number of specific recommendations for governments and businesses.

The DOC should promote the recommendations for businesses as best practices. We note that the NIST Draft Framework for Cyber-Physical Systems[43] addresses interoperability in the IoT as well as safety and security.

The FTC and the FCC have important roles to play in strengthening consumers' digital rights. The FCC has already moved forward on a number of important issues with its reclassification of broadband services as communications services and its proposed rulemaking on set-top boxes[44] and broadband privacy. The FTC, however, lacks the ability to undertake rulemaking to better protect consumers in the digital age, a problem that Congress should remedy.

The Department of Transportation is conducting research on the IoT[45] and connected cars,[46] and has initiated a rulemaking process concerning vehicle-to-vehicle communications,[47] which addresses privacy and security, among other issues. It should expand its work to examine other consumer issues such as the use of "starter interrupt" technology.

The Food and Drug Administration has issued draft guidance concerning the security of post-market connected health devices[48] but to our knowledge has not looked at digital rights issues concerning these devices and should do so.

Sustainability

How long consumers should reasonably expect to be able to use the IoT devices and systems in which they invest and what their rights should be if their use is unilaterally curtailed is an interesting issue that should be explored, perhaps through a public workshop convened by the FTC.

Choice

Consumers should be free to decide whether to use IoT products or not, and whether to disable certain features. There may be legitimate reasons for businesses (and governments) to encourage use of certain technologies to achieve cost-savings, enhance security, or for other worthy goals. However, consumers should not be unfairly disadvantaged if they are unable or unwilling to participate in the IoT ecosystem. CI cites as an example of this the fact that it costs 50 percent more to use walk-up paper tickets to travel on the London underground than using the smart card system and that it is impossible to use cash on many busses.[49] This is unfair low-income consumers and to those who wish to pay cash in order to keep

[42] http://test.tacd.org/wp-content/uploads/2013/09/TACD-INFOSOC-37-08-Consumer-Rights-in-the-Digital-World.pdf.
[43] See www.hldataprotection.com/2015/09/articles/consumer-privacy/nist-releases-draft-framework-on-the-internet-of-things/.
[44] See www.federalregister.gov/articles/2016/03/16/2016-05762/commercial-availability-of-navigation-devices.
[45] www.rita.dot.gov/publications/technology_scan/internet.
[46] www.its.dot.gov/connected_vehicle/connected_vehicle_research.htm.
[47] www.nhtsa.gov/About+NHTSA/Press+Releases/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications.
[48] www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
[49] See www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf, page 38.

information about their travel private. The DOC should promote consumer choice and reasonable alternatives as essential considerations as IoT products, services and systems are developed and deployed. This is another issue that the FTC might want to consider as a subject for a public workshop.

Redress

CFA is opposed to forced arbitration provisions in any contract or terms of service for consumer products or services. These provisions are not negotiable and unfairly require consumers to waive their ability to go to court to enforce their rights. We are pleased that the Consumer Financial Protection Bureau recently proposed rules[50] to prohibit providers of certain financial products and services from using pre-dispute arbitration agreements to block consumers from participating in class action lawsuits. Forced arbitration agreements and class action bans are already prohibited in most financial service contracts with members of the military[51] and in home loans and lines of credit.[52] The Centers for Medicare and Medical Services is considering a ban on forced arbitration in long-term care facility contracts[53] and the Department of Education has introduced proposals that would limit or ban forced arbitration.[54] In its proposed rulemaking on broadband Internet privacy, the FCC has asked questions about the appropriateness of forced arbitration.[55]

Forced arbitration provides no benefit to consumers. In our view, businesses should have good complaint resolution systems in place, which can include an option for arbitration as long as it is voluntary for consumers, free and convenient for them to use, and operates in a timely manner. There is no justification, however, for forced arbitration. Its only purpose is to protect businesses from lawsuits. Individual and class-action lawsuits not only help consumers obtain redress but can be used to change improper business practices. Congress should ban forced arbitration in all contracts and terms of service for consumer products and services.

The use of "gag" clauses in contracts and terms of service that threaten consumers with financial penalties if they post negative information about companies or their products or services or complain about them to third parties should also be prohibited by law. CFA notes that the newly-revised OECD recommendations for consumer protection in the context of ecommerce specifically state that businesses should not attempt to restrict a consumer's ability to make negative reviews, dispute charges, or consult or file complaints with government agencies and other complaint bodies.[56] The recommendations also state that subject to applicable law, the use of out-of-court redress mechanisms

[50] See press release, May 5, 2016, http://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-proposes-prohibiting-mandatory-arbitration-clauses-deny-groups-consumers-their-day-court/.
[51] 10 U.S. Code § 987, Terms of consumer credit extended to members and dependents: limitations https://www.law.cornell.edu/uscode/text/10/987.
[52] 12 CFR 1026.36, Prohibited acts or practices and certain requirements for credit secured by a dwelling https://www.law.cornell.edu/cfr/text/12/1026.36.
[53] Medicare and Medicaid Programs, Reform of Requirements for Long-Term Care Facilities, https://federalregister.gov/a/2015-17207.
[54] Negotiated Rulemaking for Higher Education 2016, Borrower Defenses, Session 3, Issue Paper 5, March 16-18, 2016, http://www2.ed.gov/policy/highered/reg/hearulemaking/2016/bd3-i5-finclresp.pdf.
[55] See https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf, pages 87-88, paragraph 274.
[56] See page 11, #12, OECD (2016), Consumer Protection in E-commerce: OECD Recommendation, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264255258-en.

such as internal complaints handling and alternative dispute resolution should not prevent consumers from pursuing other forms of dispute resolution and redress.[57]

The DOC should encourage businesses in the IoT ecosystem to make it clear to whom consumers should complain if they have problems with IoT products or services, and provide easy-to-use, effective mechanisms to resolve complaints.

Conclusion

From the consumer perspective, the IoT can add value to products and services and empower consumers, but it must be developed with privacy and security built in, with transparency about how it works, with respect for consumers' digital rights, with consumer choice, and with fair and effective means of redress for problems that consumers may encounter. The work that the DOC is doing on standards for security and interoperability is laudable, and CFA believes that legislation, rules, and guidance from agencies and pro-consumer organizations are also needed to ensure that consumers can fully benefit from the opportunities that connectivity offers.

Submitted by:

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America

[57] Id, page 16, #43.