KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Statement of **Justin Brookman**
Director, Consumer Privacy
Center for Democracy & Technology

Before the Senate Committee on Commerce, Science, and Transportation

The Connected World: Examining the Internet of Things

February 11, 2015

The Center for Democracy & Technology (CDT) is pleased to submit testimony to the Senate Committee on Commerce, Science, and Transportation for today's hearing on the privacy and security implications of the Internet of Things (IoT).

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. I currently serve as the Director of CDT's Consumer Privacy Project. Our project focuses on issues surrounding consumer data, and I have previously testified before Congress on issues such as data breach notification legislation, commercial privacy, and cybersecurity.

The Internet of Things presents amazing opportunities for enriching citizens' lives. As consumer advocates, CDT is extremely enthusiastic about the potential advances to public health, the environment, education, and quality of life that will be brought about by the coming wave of IoT devices. However, in order to achieve this enormous potential for improving the lives of Americans, these sensor- and internet-enabled devices must be purposefully designed with consumer privacy and empowerment in mind. My testimony today will address four key policy areas that must be addressed for the Internet of Things to be fully realized: weak data security practices, unexpected and unwanted secondary data collection and use, diminishing user control over their own devices, and the potential for law enforcement and intelligence abuse. Companies must respond to these challenges, or user adoption of these valuable and even life-saving technologies will be dramatically stunted.

I. The transformative potential of the Internet of Things

We read about new *smart* technologies seemingly every day: keyless cars that you start with a cell phone, refrigerators that automatically order eggs when you've run out, dog collars equipped with GPS trackers, and even baby booties that monitor a child's heart rate and oxygen levels. This is a remarkable time for innovation and growth. According to recent reports, 26 to 30 *billion* devices will be connected to wireless internet by 2020. This means in just five years, the

number of connected gadgets could grow to over 30 times its size in 2009.[1]

In addition to their *cool factor*, smart devices enhance healthcare, education, finance, agriculture, and a number of other fields. Connected cities are also starting to leverage these technologies regularly: Philadelphia has saved over $1 million by placing smart garbage cans around the city that alert sanitation workers when pick-up is necessary; New York City plans to convert outdated public pay phones into free open WiFi hotspots.[2]

In many ways, consumers have already embraced many smart Internet of Things devices. Over 70% of Americans now own a smartphone, giving each of us access to the wealth of the world's information at our fingertips as we go about everyday life.[3] Many of us have smart TVs or smart DVD players, meaning we have access not just to what's on TV or in our video library, but we can connect to Netflix, Amazon, or YouTube to watch virtually anything, or use Skype or Hangouts to call a loved one. In the near future, smart car technologies have the potential to dramatically reduce accidents, improve traffic flows, and reduce greenhouse gas emissions.

Without question, IoT has real revolutionary potential. However efforts to make all of our things smarter raise unique consumer protection concerns. Reports of major electronics companies planning to connect *all* of its consumer devices to the internet in the next five years[4] suggests the question: do consumers want *everything* to be smart? Is there a meaningful use case for a *smart toaster*? Even if there are incremental advantages to some connected devices, might the downsides in some cases outweigh the benefits? Unfortunately, some poor design decisions today are compromising the revolutionary potential of the Internet of Things, with the potential result that many if not most consumers will reject many of these innovations.

Smart technologies often involve the mass collection, storing and sharing individuals' data. While much of this is necessary and unobjectionable —the very nature of some devices (such as health wearables) is to track a user's data for that user's benefit — certain data practices seriously threaten individuals' security and right to privacy.

Internet of Things devices collect extremely sensitive personal information about

---

[1] Press Release, Gartner, Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 (Dec. 12, 2013), http://www.gartner.com/newsroom/id/2636073.

[2] Sarah Ashley O'Brien, *The Tech Behind Smart Cities*, CNN MONEY (Nov. 11, 2014), http://money.cnn.com/gallery/technology/2014/11/11/innovative-city-tech/index.html.

[3] *Asymco: Smartphone penetration reaches 70% in the U.S.*, GSMARENA (Jul. 9, 2014), http://www.gsmarena.com/asymco_pricing_doesnt_affect_smartphone_adoption_in_the_us-news-8982.php.

[4] Rachel Metz, *CES 2015: The Internet of Just About Everything,* MIT TECHNOLOGY REVIEW (Jan. 6, 2015), http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/.

us. This is especially true about IoT devices *in our homes*. In his majority opinion for *Florida v. Jardines*,[5] Justice Scalia articulated the high level of privacy an individual is entitled to in his or her home, writing "when it comes to the Fourth Amendment the home is first among equals… At the Fourth Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreason-able governmental intrusion'"[6]

The Supreme Court has repeatedly held that people have heightened privacy interests in what happens within their home — even over information[7] that is technologically observable[8] by others. We have "peeping tom" laws to protect against private observation in the home for the same reason — just because someone has the means to watch what you're doing in your home doesn't mean they should. Our homes are our most personal, private spaces and we maintain this expectation even if we bring smart devices into our home.

Internet of Things devices not tied to the home also have the potential to collect sensitive information. Certainly geolocation information — generated by several IoT devices — is extremely sensitive and revealing: unwanted disclosure can endanger one's personal safety by letting an attacker track your physical location. Otherwise, geolocation can reveal other deeply personal information, such as where you worship, where you protest, and where (and with whom) you sleep at night. Other IoT technologies often collect sensitive information on an individual that is not immediately apparent when that person is in a public space — such as his physical or mental health, emotions, and preferences.

In many cases, consumers will gladly share this information with IoT service providers in order to receive a particular service. However, in other cases, consumers won't want this information collected at all. Internet of Things devices must be designed with this fact in mind, or consumers will reject these products as not worth the risks.

II. There are currently insufficient security protections in place to regulate IoT data collection.

It is no exaggeration to say that academics have documented the security vulnerabilities of the Internet of Things for years. Central to some of these concerns is that IoT devices use *embedded* operation systems, where computing is implanted into the device itself. The computer chips that power these systems are often cheaply produced, rarely updated or patched, and highly susceptible to hacks. Users do not have the expertise to regularly patch the system or install system updates manually, nor are they typically alerted of security updates. As prominent technologist Bruce Schneier succinctly puts it, "hundreds of millions of

[5] Florida v. Jardines, 133 S. Ct. 1409 (2013).

[6] *Id.*

[7] Kyllo v. United States, 533 U.S. 27 (2001).

[8] Florida v. Jardines, 133 S. Ct. 1409 (2013).

devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years. . . . We have an incipient disaster in front of us. It's just a matter of when."[9]

While some large, complex, smart IoT systems may have WiFi connections, software updates, and multiple types of functionality and interfaces, many of the more widely deployed IoT systems will be more modest, without such capabilities. These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal. Such incentives have failed certain elements of the smart phone market, resulting in millions of vulnerable devices that will remain so for the remainder of their shelf life.[10] Eventually, we expect to see entirely new types of market events, such as product recalls, based solely on vulnerabilities in the network and computational interface that provide IoT-like communication services. Otherwise, many of these devices and systems may never be updated in their after-market environment, and home networks and IoT-capable communication platforms will have to be designed to deal with errant and outright hostile (e.g., hacked through a flaw or vulnerability) participants on the local network. Compounding this problem is the fact that home routers — the devices that link all these devices together — are also famously vulnerable to attack.[11]

Even at this early stage of IoT development, seemingly every type of connected device has already experienced these vulnerabilities: spy chips have been discovered in tea kettles and irons[12]; hackers have stolen Smart TV login credentials in order to listen in and spy on people in their homes[13]; live streams from baby monitors have been uploaded to public websites[14]; thieves can disable home alarm systems with a tool from 250 yards away[15]; and even smart toilets,

---

[9] Bruce Schneier, *Security Risks of Embedded Systems*, SCHNEIER ON SECURITY BLOG (Jan. 9, 2014), https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.

[10] Dan Goodin, *ACLU Asks Feds to Probe Wireless Carriers over Android Security Updates*, ARSTECHNICA, (April 17, 2013), http://arstechnica.com/security/2013/04/wireless-carriers-deceptive-and-unfair/.

[11] Dan Goodin, *12 million home and business routers vulnerable to critical hijacking hack*, ARSTECHNICA, (Dec. 18, 2014), http://arstechnica.com/security/2014/12/12-million-home-and-business-routers-vulnerable-to-critical-hijacking-hack/; Brian Krebs, *Lizard Stresser Runs on Hacked Home Routers*, KREBSONSECURITY, (Jan. 15, 2015), http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[12] Erik Sherman, *Hacked from China: Is Your Kettle Spying on You?*, CBS (Nov. 1, 2013), http://www.cbsnews.com/news/hacked-from-china-is-your-kettle-spying-on-you/.

[13] Lorenzo Franceschi-Bicchierai, *Your Smart TV Could be Hacked to Spy on You,* MASHABLE (Aug. 2, 2013), http://mashable.com/2013/08/02/samsung-smart-tv-hack/.

[14] Loulla-Mae Eleftheriou-Smith, *Baby Monitors, CCTV Cameras and Webcams from UK Homes and Businesses Hacked and Uploaded onto Russian Website,* THE INDEPENDENT (Nov. 20, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitors-cctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto-russian-website-9871830.html.

[15] Kim Zetter, *How Thieves can Hack and Disable Your Home Alarm System,* WIRED (Jul. 23, 2014), http://www.wired.com/2014/07/hacking-home-alarms/.

refrigerators and printers have been compromised.[16] And a report released this weekend by Senator Markey raises serious questions about whether connected cars are being designed to ensure that their systems are protected from malicious hackers seeking to take physical control over the vehicles.[17]

Currently, the United States does not have a dedicated data security law requiring companies to use reasonable protections to safeguard personal information. Since 2005, the Federal Trade Commission has used its general consumer protection authority under Section 5 of the FTC Act to bring enforcement actions against companies that do not safeguard personal data.[18] The Commission has argued that the FTC Act's prohibition on "unfair" business practices extends to companies using poor data security; two years ago, it brought its first enforcement action against the manufacturer of an Internet of Things device.[19] However, ongoing legal challenges threaten to undermine the agency's efforts in this area: some defendants have argued that they are not, in fact, legally obligated to use reasonable data security practices.[20]

Increased reports of massive data breaches (including the highly publicized Sony studios and Anthem healthcare hacks) have prompted new dialogue around the need for updated data breach notification laws to respond to such incidents. Unfortunately, many of the data breach notification legislative proposals would actually *dial back* legal incentives for companies to properly secure the data they collects from consumers. For example, only requiring agency or consumer notification when a specific "harm" has been identified would discourage companies from fully investigating a breach for fear of triggering the notification requirement. Further, data breach law that omits any affirmative requirement that companies design robust security procedures for their products will ultimately do little to expand upon existing state law protections and deter or prevent future breaches. In order to encourage better security than exists under the law today, a federal breach notification bill would need to offer *new* protections not reflected in

---

[16] Lily Hay Newman, Pretty Much Every Smart Home Device You Can Think of Has Been Hacked, SLATE BLOG (Dec. 20, 2014), http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html.

[17] Report, *Tracking and Hacking: Security & Privacy Gaps Put American Drivers at Risk*, OFFICE OF SENATOR ED MARKEY, (Feb. 2015) http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[18] Press Release, Federal Trade Commission, DSW Inc. Settles FTC Charges (Dec. 1, 2005), http://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges.

[19] Press Release, Federal Trade Commission, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[20] *See* G.S. Hans, *CDT Files Brief in Wyndham Supporting FTC Regulation of Data Security* CENTER FOR DEMOCRACY & TECHNOLOGY BLOG (Nov. 13, 2014), https://cdt.org/blog/cdt-files-brief-in-wyndham-supporting-ftc-regulation-of-data-security/; *See also* Press Release, Federal Trade Commission, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

existing law, and still allow states to innovate on data sets not covered by a federal standard.[21] For more information on this topic, visit https://cdt.org/insight/cdt-issue-brief-on-federal-data-breach-notification-legislation/.

III. Sensitive personal data may be collected contrary to consumer wishes and expectations

As noted above, IoT devices have the potential to collect a tremendous amount of detailed personal information about consumers. Some of the data collected is of course expected; if I buy a fitness tracker, for example, I shouldn't be surprised that the device tracks my steps throughout the day — indeed, that's the reason I bought it. On the other hand, I might be surprised if that device were also recording all my conversations with my friends, or transmitting my geolocation to third party data brokers.

As an example of surprising — and potentially unwanted — IoT data collection, last year, an independent researcher noticed that LG was monitoring what TV shows people watched on their smart TVs, and sending that information back to LG's corporate servers.[22] The purpose appeared to be for a future undeveloped advertising product; LG was also collecting and reporting back information about the names of files consumers accessed on computers connected to the same home network, though it's not clear why. In response to user complaints, LG initially directed people to a long, legalistic terms of service that vaguely reserved broad rights to transmit user data. The company backtracked after a host of media attention around its practice, and LG enabled an opt-out feature for users who did not want their information collected in this manner. This was a start, however, it is not clear that opt-out is sufficient to meet reasonable consumer expectations in this case. Should home appliances be monitoring consumers and reporting everything they can detect back to manufacturers *by default*? Certainly, other interconnected devices don't do this today. Your computer doesn't report back to Lenovo or HP everything that you do. Your phone doesn't report everything back to Motorola or Apple. When a consumer buys a TV, they are not typically looking for or expecting *a relationship* with LG or Samsung: they may appreciate additional smart capabilities like connecting to Skype or the web, but their TV is a platform for them to access others' content — it is not a destination in itself. A users' smart phone could have its microphone and camera transmitting 24 hours a day, seven days a week (setting aside battery and bandwidth issues) — it could collect significant amounts of interesting information in the name of "Big Data" but such data collection would go well beyond consumers' reasonable privacy expectations.

---

[21] *CDT Issue Brief on Federal Data Breach Notification Legislation*, CENTER FOR DEMOCRACY & TECHNOLOGY INSIGHTS, (Jan. 27 2015), https://cdt.org/insight/cdt-issue-brief-on-federal-data-breach-notification-legislation/.

[22] Justin Brookman, *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency,* IAPP BLOG (Nov. 27, 2013), https://privacyassociation.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/.

This precise scenario arose last week in fact, when it was revealed that Samsung's privacy policy appeared to reserve the right to collect any voice communications in proximity to its Smart TVs and send that information to an unnamed voice recognition service provider.[23] Samsung's actual practices are not easily discernable: perhaps Samsung is only collecting and transferring voice data for the limited times when a consumer is trying to use certain voice recognition commands. This might be consistent with reasonable consumer desires and expectations. Or perhaps Samsung wants to collect and process *all* dialogue in proximity to its televisions in order to refine its (or its partner's) voice recognition software. There certainly would be a benefit — to Samsung and the consumer — from that collection and processing, but query whether most consumers would find the benefit worth the persistent collection of all conversations in a living room or bedroom by an unknown third party. Ultimately, consumers must be empowered to make the determination about what data is collected and why.

We believe that the United States should enact a comprehensive privacy law regarding the collection and use of personal information. Companies should be required to offer consumers reasonable transparency and control over how their data is collected; today, the U.S. is one of the few developed nations not to have such consumer protections in place. The purpose of such a law wouldn't be to ban or prevent particular practices, but should require actionable information and an ability to express real preferences in order for a market to develop for personal information. Today, absent such requirements, too much data collection is opaque and unaccountable; consumers have a vague sense that their privacy is being violated, but don't have the information or tools available to make decisions about their personal information.

With or without a law, companies should set reasonable defaults for data collection and use based on consumer expectations. Some data may require clear opt-in because it's sensitive or the collection or use would be surprising to a user; other information may be collected automatically but consumers should have the ability to opt out of secondary data use, retention, or transfer; and some data consumers shouldn't have control over because it is fundamentally necessary for operation of the device. However, consumers must generally be empowered to make decisions about how their devices work (and what data is collected and shared with other entities). IoT should work *for* the consumer — the person who bought the product; the Internet of Things shouldn't be something that happens *to* a begrudging populace.

IV. Device connectivity and intelligence could diminish user autonomy over the devices they buy

Adding sensors and connectivity to IoT devices has the potential to make them much more useful for consumers. On the other hand, these features could also

[23] Shane Harris, *Your Samsung SmartTV is Spying on You, Basically,* THE DAILY BEAST (Feb. 5, 2015), http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

be abused to deprive consumers of continuing services, expected interoperability, or control over their own devices.

Objects included in the "Internet of Things" consist of two basic components: the physical object and the software that connects it to the network. Traditionally, when you buy something, it is yours and you are free to do with it whatever you'd like including altering, repairing, or re-selling it. However, objects within the Internet of Things do not fit into our traditional understanding of ownership. While you still take possession of the physical object, the software is typically licensed to you under an End-User License Agreement (EULA). The implications of this vary with how integral the software is to the functioning of the device — in some cases, like a washing machine that you can monitor/control from your phone, losing access to this feature wouldn't affect the core functionality and value of the machine very much. In other cases, the object itself is essentially useless without the software controlled by licensing agreements, or can quickly become obsolete without updates. For example, imagine a thermostat that only works if you can program the software. In this case, a lapse in software updates could render the physical object useless even if the physical mechanism were still in good repair.

Last year, Keurig — the popular single cup coffee maker — put software controls on its coffee maker to prevent users from using non-Keurig approved coffee pods in their machines. Though this functionality did not rely upon internet connectivity, it did take advantage of increasingly cheap and sophisticated sensors to allow the Keurig machine to detect proprietary codes on approved coffee pods. As result of this technology, consumers were prevented from brewing their preferred brand of coffee in the devices they bought and paid for. In this case, Keurig's decision appears to have backfired: featured reviews for Keurig's new line of coffee makers on Amazon prominently criticize this design feature,[24] and sales fell 12 percent last quarter.[25]

In other cases, policymakers have intervened to mitigate potential monopolistic effects of proprietary software. One example is the repair codes used by automobile manufacturers. Cars include systems that provide a specific diagnostic code that explains, for example, the cause of a "check engine" light. Originally, the guide that explains these codes was withheld from consumers and the majority of auto repair shops, forcing drivers to use specific repair shops for their vehicles. However, some states now require that the explanations for the codes be widely available.[26] In another example, the Librarian of Congress, in consultation with the Copyright Office, eliminated an exemption to laws prohibiting circumvention of digital rights management for users seeking to

---

[24] *Keurig 2.0 K350 Brewing System – Black,* AMAZON.COM, http://www.amazon.com/Keurig-2-0-K350-Brewing-System/dp/B00KYWL34Q/ref=sr_1_1?ie=UTF8&qid=1423266957&sr=8-1&keywords=keurig+2.0 (last visited Feb. 9, 2015).

[25] Josh Dzeiza, *Keurig's attempt to 'DRM' its coffee cups totally backfired* , THE VERGE (Feb. 5, 2015), http://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totally-backfired.

[26] *Mass. lawmakers approve "Right to Repair" bill*, FOXNEWS, (August 1, 2012), http://www.foxnews.com/leisure/2012/08/01/mass-lawmakers-approve-right-to-repair-bill/.

unlock their mobile phones and change wireless providers. Mobile phone unlocking had been an entirely legal and common practice for years before the Librarian eliminated the exemption. More than 114,000 Americans petitioned the White House to overturn the ban and, after both the Federal Communications Commission and the White House recommended doing so, Congress ultimately enacted legislation restoring consumers' right to unlock their own phones. Unfortunately, the exemption applies only to mobile phones and is examined *de novo* every three years.

In the Internet of Things, digital rights management affects intellectual property accessed through networked devices as much as the devices themselves. For example, users do not own the content they purchase for their e-readers (Kindle, Nook, etc.). The physical tool allows readers to buy rights to access the content of their choice, but readers do not own the book. Additionally, this access is restricted in many users may not fully understand because the relationship is so different from the physical world. For example, there are typically restrictions on *lending* the book to a friend. In this case, if the licensing agreements for that content were revoked because of a perceived or alleged violation of the license, the object itself would be useless to the average consumer who would have no way to load content.

Additionally, connectivity can allow other entities to access and control the device in ways not possible in an un-networked world. One prominent example is lenders who use technology in connected cars to punish those who are late in making payments by disabling the vehicle. In a case reported by the New York Times[27], subprime borrowers were allowed to lease vehicles provided they gave permission for the lender to remotely disable the ignition in the event of a late payment or default. Some argue this technology allows the lender to provide credit to a broader audience than would otherwise be possible; others argue that it is unethical and perilous to put people in a situation where they may have an emergency and cannot access their vehicle, as was the case for the woman in the article who needed to use her car to take an asthmatic child to the doctor. Moreover, vulnerable borrowers might be subject to egregious reconnection fees that had been disclosed only in inscrutable contracts. Regardless of what you believe, it is undeniable that this technology shifts the balance of power from the user to the company or institution that controls the software.

V. Our government access and intelligence laws must be reformed

Finally, the default of IoT devices to phone home by reporting data to a company rather than storing it locally on the device raise concerns about government surveillance as well. Many of the same concerns that apply to in-the-home

[27] Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car,* THE NEW YORK TIMES (Sept. 24, 2014), http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/.

monitoring devices like smart grid technologies[28] apply to objects in the Internet of Things. IoT systems will, in most cases, be sensing platforms augmenting devices and objects in the home or in businesses. Light sensors can tell how often certain rooms are occupied at night or how often the refrigerator is opened. Temperature sensors may be able to tell when one bathes, exercises, or leaves the home entirely. Microphones can easily pick up the content of conversations in the home and, with enough fidelity, can identify who is speaking. In essence, the privacy and security concerns highlighted by the revelation that law enforcement has access to data stored by private companies are elevated exponentially in a future with increased connectivity and automated collection.

Government access without robust due process protection is already arguably the most significant threat posed by the collection of personal information. As the recent NSA revelations aptly demonstrate, much of the data that governments collect about us derives not from direct observation, but from access to commercial stores of data. Even in the United States and Europe, that data is often obtained without transparent process, and without a particularized showing of suspicion — let alone probable cause as determined by an independent judge. Unfortunately, there is almost nothing that consumers can do to guard against such access or in many cases even know when it occurs.

The revelation that commercial data is tied to government surveillance has the potential to fundamentally change the conversation about IoT. For the vast majority of consumers, unwanted surveillance — quite apart from practical effects of such surveillance — is the harm they're seeking to avoid. Therefore, considerations of risks associated with IoT must address harms from government surveillance as well as private sector risks.

This loss of consumer confidence has a quantifiable impact on corporate bottom lines and hence the development of these useful new technologies. For example, according to Forrester Research the losses to US technology companies from revelation of the PRISM program (detailing once facet of US surveillance practices) could result in, "a net loss for the service provider space of about $180 billion by 2016 which would be roughly a 25% decline in the overall IT services market by that final year." These costs demonstrate the market value of business practices and government policies that respect privacy.[29]

Nor is the point in sighting this figure to single out the NSA and US surveillance. As CDT has noted repeatedly, all governments are interested in data collection and have extensive legal tools to access that information. In an internet connected future it is not only the US government but also the governments around the world that may be interested in IoT and the information it reveals. For

[28] CTR. FOR DEMOCRACY & TECH. & ELEC. FRONTIER FOUND., "Proposed Smart Grid Privacy Policies and Procedures," before The Public Utilities Commission of the State of California (December 18, 2008), *available at* https://cdt.org/files/pdfs/CDT_EFF_PoliciesandProcedures_15Oct2010_OpeningComment_1.pdf.
[29] James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," FORRESTER, August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

more on legal tools that governments possess to access personal information please see: http://govaccess.cdt.info/.

Government surveillance reform is a much broader topic than the IoT and this committee's hearing today. However, the continuing access by government to commercial information highlights the need to build systems that minimize the amount of information they share and also give consumers control over what information their devices collect.

The potential benefits of the IoT are exciting and profound. It is incumbent upon manufactures of these devices and governments to make sure that those benefits are fully realized while protecting the privacy of consumers.

Conclusion

Recognition of the threats to collected personal information is particularly important because in recent years, some have argued for a new definition of privacy where there are no limits on what information companies (and governments) can collect about us or how long they retain it. Privacy is in effect redefined to only prohibit certain harmful uses of personal information. For example, President Obama's Council of Advisors on Science and Technology last year released a report on Big Data making precisely this point: because of the potentially awesome power of personal information, we shouldn't put limitations on what information is collected; instead, we should just make sure that that data is not subsequently misused.[30]

This view, however, presumes a perfect world of unbreakable security, where consumer and company expectations are fully aligned, and where due process protections fully assure there is no potential for government abuse.[31] Obviously, these conditions are not met today, and likely will never fully be realized. As such, consumers have a rational interest in exercising control over how their data is collected and retained. Without affording consumers meaningful control over their own devices, IoT adoption is seriously threatened. Today, the highly sensitive data collected by IoT devices is exposed to a variety of threats, and designers must keep these threats in mind when developing their products for market. Consumers would benefit tremendously from a full-fledged, user-centric Internet of Things. Developers must keep personal privacy and empowerment in the front of their minds in creating these products.

---

[30] EXECUTIVE OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014). http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf?utm_content=buffer06b57&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

[31] JUSTIN BROOKMAN & G.S. HANS, WHY COLLECTION MATTERS: SURVEILLANCE AS A DE FACTO PRIVACY HARM (2013), http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.