Comments of Access Now
Docket No. 160331306-6306-01

TO: the National Telecommunications and Information Administration, U.S. Department of Commerce (iotrfc2016@ntia.doc.gov)
FROM: Access Now
RE: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things [Docket No. 160331306-6306-01], RIN 0660-XC024
DATE: June 2, 2016

By notice published April 6, 2016, the National Telecommunications and Information Administration ("NTIA") has requested comment "on the potential benefits and challenges of [Internet of Things (IoT)] technologies and what role, if any, the U.S. Government should play in this area."[1] Access Now submits these comments and recommendations to respond to select questions posed in NTIA's request.

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now's policy team works at the intersection of human rights and technology, furthering Access Now's mission by developing and promoting rights-respecting practices and policies. With staff placed strategically around the world, we seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society.

As the internet of things grows and expands, it will become more important to have strong legal standards for data protection and data security. It is also important to reform surveillance laws to provide adequate protections for the information that internet things will collect, including the information of those who are non-U.S. Persons. Finally, the internet of things raises the need for more transparency on internet shutdowns, including wireless network shutdowns, which are regulated under overly-opaque processes.

I. The Internet of Things

The internet of things is not a new concept. As NTIA recognizes, the term has been around since the late 1990s. Today, the internet of things is defined by many to include personal activity monitors, household appliances, children's toys, medical devices, and the power grid. The internet of things has resulted in a near-exponential growth of sensors collecting information about individuals and their daily lives. While this data collection may come with new benefits,

[1] The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19,956 (Apr. 6, 2016), *available at* https://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf.

both President Roosevelt and Ben Parker would caution that it brings with it the need for great responsibility.[2]

In defining the internet of things, it is important to do so broadly and in a way that is not limited by current technology. If the past few decades have taught us anything, it is that technology is not static. Technology, including the internet of things, is evolving and being deployed at a rate at which it is just not rational to believe that law or regulation can keep pace. A broad, technology-neutral definition will assure that policies that protect the rights of users will not be outdated before they can even be implemented.

Further classifications may be helpful in some cases to provide additional protection. These classifications should also be technology-neutral, and should instead focus on their impact on the user. For example, "things" that are inserted into the body may require special safety and security considerations. Similarly, "things" that direct or run utilities may require special emergency operations procedures that preference running the utility over powering additional sensors.

Privacy of Things

The internet of things has already greatly expanded both the types and the amount of personal information collected, stored, and analyzed. What has already been labelled 'big data' continues to get bigger as we adopt devices to monitor our rate of activity (as well as the type of activity in which we engage), our consumption, our biological functions, our water use, and more. As Access Now stated in comments on the White House's Big Data Study in 2014:

> "There has been an exponential increase in the amount of data collected and stored by private companies in recent years. Facebook announced in 2012 that its data center had grown 2500x since 2008. By 2012, Facebook was collecting about 180 petabytes of data per year. For reference, one petabyte is the equivalent of 20 million 4-drawer filing cabinets filled with text. Retailers, whether focused at online markets or off, also track customers. It is estimated that in one hour Wal-Mart processes about 1 million customer transactions containing 2.5 petabytes of data."[3]

The internet of things increases this growth in data and raises the profile of what has increasingly become an undeniable fact: the United States needs to join the rest of the world in passing baseline privacy legislation. The President's Consumer Privacy Bill of Rights (CPBoR)

[2] Wikipedia, *Uncle Ben: "With great power comes great responsibility"*, *available at* https://en.wikipedia.org/wiki/Uncle_Ben#.22With_great_power_comes_great_responsibility.22 (last visited June 1, 2016)

[3] Letter from Access Now to Nicole Wong, the White House (Apr. 2, 2014), *available at* https://www.accessnow.org/access-tells-white-house-to-promote-data-security/ (internal citations omitted).

provided a widely-accepted framework for this legislation. Elements of the CPBoR, such as focused collection and respect for context, are even more important in the internet of things world, where many companies may have little experience collecting or storing personal data. As the internet of things encompasses more devices used by more people, it becomes more important to have an across-the-board standard for protecting the users to whom that data belongs.

Privacy legislation isn't only important for users in the United States. The overseas viability of the internet of things will rely on a lasting cross-border data transfer arrangement between the EU and the United States. Currently, the Privacy Shield is set to be approved by the Article 31 Committee, but serious questions have been raised on the arrangement's ability to withstand judicial scrutiny. A coalition of groups from the United States and Europe explained, "a lasting data transfer framework requires increased protections for personal data collected or used commercially in order to meet the standards set forth by the [Court of Justice of the European Union]. Wider data protection reforms, which must include robust and comprehensive enforcement mechanisms, are necessary to ensure that the U.S. provides a level of essentially equivalent protection to that available under the European legal framework."[4]

The ability of Privacy Shield to withstand scrutiny is also dependent on substantive U.S. surveillance reform to protect the human rights of those abroad. As the coalition explained, "The Privacy Shield should be contingent on U.S. legislative reform of surveillance laws within a reasonable time."

U.S. surveillance law and practice is likely to impact the adoption of the internet of things. The vast majority of data generated by the internet's things - metadata - enjoys the least legal protection. That is because the data falls within the third party doctrine, a legal concept that says that people do not have an expectation of privacy in information that they make available to a third party.[5] This means that the information, unlike information deemed "content," is not covered by Constitutional protections, and must rely on statutory structures to limit law enforcement access. This distinction is increasingly nonsensical. Studies demonstrate that metadata can be as revealing - if not more so - than content information.[6] Human rights standards have outright disregarded this superficial distinction.[7] However, while the Supreme Court has hinted that it may be ready to offer content-level protection for at least some types of metadata, the law in the U.S. has not yet caught up.

---

[4] Letter from Access Now, et. al to Ms. Isabelle Falque-Pierrotin Chairman, Article 29 Working Party, et. al (Mar. 16, 2016), *available at* https://www.accessnow.org/cms/assets/uploads/2016/03/Priv-Shield-Coalition-LtrMar2016.pdf.
[5] *See, e.g.,* Smith v. Maryland, 442 U.S. 735 (1979).
[6] *See, e.g.*, Jonathan Mayer and Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, Web Policy (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.
[7] International Principles on the Application of Human Rights to Communications Surveillance, the 13 Principles, https://www.necessaryandproportionate.org (last visited May 27, 2016).

The inability for U.S. law to offer adequate protections against mass surveillance is likely to hinder the adoption of the internet of things. Studies continue to demonstrate how individuals change their behavior under threat of government surveillance.[8] It is foreseeable that this same consequence will extend into the internet of things. Congress must meaningfully address the question of surveillance reform to ensure that the internet of things does not become yet another firehose of sensitive user data for the government to warrantlessly tap into.

Finally, we must ensure that data breach notification laws are adequate to handle the internet of things. Currently, the United States operates under a patchwork of notification laws, some more robust than others.[9] A federal standard, which provides minimal protection without pre-empting stronger state standards, is necessary to ensure that data collected by internet things are adequately secured. Such a standard should encompass the sensitive, non-financial data that many of these devices will collect, like biometric information which cannot simply be re-issued or replaced.[10] Industry has adopted procedures for breaches of financial information, including provision of credit monitoring and issuance of new account numbers.[11] The Department of Commerce should further study proper means of redress for all breaches, and work to develop ways to correct breaches of personal data where there isn't an established recovery mechanism.

Summary of Recommendations:

1. Support the introduction and passage of the Consumer Privacy Bill of Rights;
2. Support U.S. surveillance reform, including of section 702 of the FISA Amendments Act and to fix overbroad application of the third-party doctrine to metadata;
3. Support extraterritorial application of the rights to privacy and freedom of expression in the International Covenant on Civil and Political Rights;
4. Support a federal data breach notification law without pre-emption for stronger state standards;
5. Study how to provide redress for non-financial data breaches.

---

[8] *See*, Elizabeth Stoycheff, Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring, Journalism & Mass Communication Quarterly (2016), http://m.jmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf?ijkey=1jxrYu4cQPtA6&keytype=ref&siteid=spjmq; Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor, PEN America, *available at* https://pen.org/chilling-effects (last visited May 27, 2016).

[9] Security Breach Notification Laws, National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited May 26, 2016).

[10] *See,* Rafe Needleman, *The 2 Big Problems with Fingerprint Security*, Yahoo (Jan. 28, 2015) *available at* https://www.yahoo.com/tech/the-2-big-problems-with-fingerprint-security-109371608679.html (noting that fingerprints cannot be reissued if breached whereas new passwords can be created).

[11] Lost or Stolen Credit, ATM, and Debit Cards, Federal Trade Commission, https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards (last visited May 26, 2016).

Security of Things

With sensors in more places than ever before, ensuring that both the devices and their data links are secure is of vital importance. As prominent security researcher Katie Moussouris has pointed out, when you brick a pacemaker (render it unusable), you brick a person.[12] Vulnerabilities in internet of things devices have given unauthorized access to our nurseries and our car engines.[13] They have allowed researchers to change the aim on a rifle, or disable it entirely.[14] These are just a few of the vulnerabilities discovered and exploited in internet of things technologies.

There are two primary elements necessary to securing the internet's things. First, you must secure the thing itself to prevent the exploitation of the device. Then you must secure the data links that send and receive information from the device to prevent eavesdropping on or manipulation of data streams.

Currently, industry best practice to secure both of these elements is through encryption. Unfortunately, the U.S. Federal Bureau of Investigation (FBI) has sought to mandate vulnerable encryption for technologies. This flies in the face of a well-established and long-accepted fact: back doors or other mandates that prevent encryption from being as strong as possible put all users at risk.[15] The Administration must affirm its support for unmitigated encryption and actively promote its adoption and use in internet of things devices.[16]

There are several challenges to adequately encrypting the internet of things. First, as previously discussed, most of the information that is transmitted over the internet of things is metadata. Additional research and development is necessary to determine how to encrypt this data in an efficient and effective manner.

---

[12] Where are the Vulnerability Land Mines?, Cybersecurity for a New America (Comments by Katie Moussouris) (Mar. 9, 2016), https://www.youtube.com/watch?list=PLNoVefpaPtVMKt2C2Yc9gdarqMEwc_O3a&time_continue=2286&v=5lJHEmXIRL0.
[13] Chante Owens, *Stranger hacks family's baby monitor and talks to child at night* (May 7, 2016), http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/; Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It* (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[14] Andy Greenberg, *Hackers Can Disable a Sniper Rifle—Or Change Its Target* (July 29, 2015) https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/.
[15] Harold Abelson, et. al, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* (July 6, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.
[16] Dear President Obama, Stand Up For Strong Security No Secret Backdoors in Our Technology, https://www.savecrypto.org (last visited May 27, 2016).

Additionally, data that can be encrypted relies upon standards that are necessarily suspect. This is because the key agency in the United States for developing these standards - the National Institute for Standards and Technologies (NIST) - is required to consult with the National Security Agency (NSA) in doing so.[17] The consultation was written into law to ensure that NIST was working with the best technical experts and cryptographers in government when the standards were built. However, over time it has raised suspicion (and even outright accusation) as the NSA's surveillance mission has further and further intruded upon its separately-established Information Assurance mission.[18] This confluence has already led several organizations and experts to call for the establishment of a separate Information Assurance agency, totally separate from the NSA.[19]

To the contrary, Admiral Michael Rogers, the director of the NSA, announced a reorganization of the NSA which will instead further conflate the mission to conduct surveillance — the lock breakers - with the mission to protect networks — the lock makers.[20] This is bad for internet of things security. Potential vulnerabilities in encryption standards developed to assist the NSA in its surveillance activities also leave the door open for bad actors to gain access to our devices.

Finally, even when researchers develop and implement the strongest encryption possible, vulnerabilities will always remain. When these vulnerabilities are discovered, they need to be disclosed to the manufacturers so that they can be patched.[21] In 2014, the U.S. government re-invigorated a process, the Vulnerabilities Equities Process, to do this for vulnerabilities either discovered or made known to its agents. Unfortunately, too little is known about the process, which only became public in redacted form following a lawsuit from the Electronic Frontier Foundation.[22] For example, the FBI recently raised questions about the process by indicating that the vulnerability that it purchased to break into the iPhone that belonged to one of the shooters in the attack in San Bernadino would not be submitted to the process at all.[23] What are the circumstances when vulnerabilities are not subject to the process? What circumstances

---

[17] Amie Stepanovich, *Virtual Integrity: Three steps toward building stronger cryptographic standards*, Access Now (Sept. 18, 2014), https://www.accessnow.org/virtual-integrity-the-importance-of-building-strong-cryptographic-standards/.
[18] *Id*.
[19] Letter from Access, et. al to President Barack Obama (July 15, 2014), https://www.accessnow.org/cms/assets/uploads/archive/Veto-CISA-Coalition-Ltr.pdf.
[20] Cheryl Pellerin, *Rogers Discusses NSA Reorganization, National Security Threats* (Sept. 25, 2015), http://www.defense.gov/News-Article-View/Article/620617/rogers-discusses-nsa-reorganization-national-security-threats; Sean Lyngaas, *NSA's Information Assurance Directorate at a crossroads* (Jan. 26, 2016), https://fcw.com/articles/2016/01/26/nsa-iad-lyngaas.aspx.
[21] Technologists have also identified other security issues with the Internet of Things, like challenges to patching vulnerabilities. We encourage the Department of Commerce to do a full investigation into the wide range of security challenges raised by the Internet of Things.
[22] Redacted Vulnerabilities Equities Process, Electronic Frontier Foundation, https://www.eff.org/document/vulnerabilities-equities-process-redactions (last visited May 27, 2016).
[23] Ellen Nakashima, *Comey defends FBI's purchase of iPhone hacking tool* (May 11, 2016), Comey defends FBI's purchase of iPhone hacking tool.

have led to decisions not to disclose vulnerabilities that have gone through the process? These questions must be answered.

We also need more answers about the government's hacking operations overall. As explained, activity in furtherance of hacking (like keeping vulnerabilities secret and influencing encryption standards) undermines the security of the global internet. Both the NSA and the FBI have confirmed that they engage in hacking operations, but the extent of those operations, and any safeguards, has not been disclosed to the public.[24]

Finally, the government can and should do more to incentivize stronger cybersecurity for the internet of things. The internet of things depends on interconnectivity and weaknesses in one device or system creates greater risk across the ecosystem.[25] A positive cybersecurity agenda should support cybersecurity research and innovation, including stronger support for small companies, independent security researchers,[26] and companies taking innovating, yet rights-respectful approaches to securing information.

NIST has collaborated with industry to create a series of cybersecurity frameworks, including the Draft Framework for Cyber-Physical Systems, which is applicable to the internet of things.[27] While voluntary standards are a useful tool, particularly for smaller companies or companies newly collecting data, the frameworks' utility is limited by their generality. Instead of engaging on legislation to formalize the Framework to protect our growing digital world, Congress passed the Cybersecurity Information Sharing Act (CISA), which is of limited substantive value while insufficiently protecting the privacy of user data.[28] The risk to user privacy is particularly acute in the context of the internet of things where comprehensive and highly sensitive information is frequently collected and processed.

---

[24] Tim Starks, Stopping Mass Hacking Act gets debate started (May 20, 2016), http://www.politico.com/tipsheets/morning-cybersecurity/2016/05/stop-mass-hacking-act-gets-debate-started-prosecution-of-cyber-crimes-at-issue-bank-heists-around-the-globe-214411; *See also* Twitter, @kevinbankston (May 20, 2016), https://twitter.com/KevinBankston/status/733660493836103680.

[25] *See* FTC, *Internet of Things: Privacy & Security in a Connected World* 10-11 (2015) (staff report), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[26] *See* Dissent Doe, *FBI raids dental software researcher who discovered private patient data on public server*, The Daily Dot (May 27, 2016) (showing the arrest of an independent security researcher who discovered exposed patient data), *available at* http://www.dailydot.com/politics/justin-shafer-fbi-raid/.

[27] Greg Otto, *NIST issues draft framework for cyber-physical systems* (Sept. 21, 2015), http://fedscoop.com/nist-issues-draft-framework-for-cyber-physical-systems; *see also* Framework for Improving Critical Infrastructure Cybersecurity, National Institute for Standards and Technologies (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[28] H.R.2029 - Consolidated Appropriations Act, 2016, https://www.congress.gov/bill/114th-congress/house-bill/2029/text (last visited May 27, 2016).

In order to better protect cybersecurity of the internet of things, the CISA needs to be amended to include privacy protections as well as to include provisions that support innovative cybersecurity approaches and remove legal barriers to independent cybersecurity research.

Summary of Recommendations:

1. Affirm unmitigated support for strong encryption not subject to requirements for backdoors or vulnerabilities of any kind;
2. Study the means and methods by which metadata can be efficiently and effectively encrypted;
3. Support the establishment of an independent information assurance agency for the federal government with adequate funding and resources to exist apart from the National Security Agency;
4. Support greater transparency for the treatment of vulnerabilities by the government both within the Vulnerabilities Equities Process as well as any vulnerabilities that are not introduced to the Process;
5. Support legislation that improves privacy protection in information sharing, increases funding for innovative cybersecurity approaches, and removes legal barriers stymying independent security research.

Keeping on the Things

Finally, the internet of things also elucidates the need for transparency in the issue of internet shutdowns. Internet shutdowns — intentional disruptions of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information — pose a threat to human rights around the world.

Internet shutdowns, which include wireless network shutdowns, harm everyone, including victims of emergencies, first responders, human rights defenders, businesses, journalists, demonstrators, and public services.[29] Shutdowns do not help victims, restore order, or protect rights. In 2015, officials from the United Nations declared that internet kill switches can never be justified, even during conflicts, under international law.[30]

In the internet of things, shutdowns may actually be a matter of life and death. The extent that devices will rely on the internet in order to function remains unclear.[31] Shutdowns which limit the

[29] Fighting Internet Shutdowns, Access Now, https://www.accessnow.org/internet-shutdowns/ (last visited May 27, 2016).
[30] Joint Declaration on Freedom of Expression and Responses to Conflict Situation, Article 19 (May 4, 2015), https://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation.
[31] Twitter, @beauwoods, https://twitter.com/beauwoods/status/735575104793542656 (May 26, 2016).

functionality of certain internet things, especially medical devices or those connected to infrastructure and public utilities, may have disastrous consequences.

Despite this, the U.S. government reserves the power to shutdown the internet in certain circumstances. The details of when or how the government can shut down or limit access to the internet, however, are far from transparent. U.S. law and policy accounts for wireless network shutdowns for national emergencies or public safety.[32] Standard Operating Procedure 303 contains procedures for the former.[33] Despite its approval in 2006, the document has never been released in full to the public. A highly redacted version was made available only after the Electronic Privacy Information Center instituted litigation under the Freedom of Information Act.[34] Similarly, while the Federal Communications Commission requested comments on a policy for shutdowns for the purpose of "public safety" — following an alarming incident where Bay Area Rapid Transit officials intentionally disrupted connectivity to thwart public protests — the final policy was never published.[35] In addition, by way of Executive Order in 2012 the White House granted the Department of Homeland Security authority to prioritize government communications, which could knock out connectivity for populations.[36]

More information is needed on how, when, and to what extent internet shutdowns are authorized and conducted in the United States. In addition, studies should be done on the extent that shutdowns will impact the internet of things, including risks to life caused by disruption of certain medical devices.

Summary of Recommendations:

1. Support greater transparency on the processes and use of internet shutdowns, including mobile network shutdowns, in the United States;
2. Support the development of resolutions and statements at the United Nations General Assembly, Human Rights Council, and International Telecommunication Union, declaring that shutdowns violate international human rights law and norms.

---

[32] Little is known about any formal policies on full network shutdowns in the U.S. However, the wireless network is a vital part to user connectivity. Wireless Quick Facts, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last visited May 27, 2016).
[33] National Security Telecommunications Advisory Committee, NSTAC Issue Review 2009-2010 (2010), *available at* https://www.dhs.gov/sites/default/files/publications/2009%20-%202010%20Issue%20Review%20(FINAL)_0.pdf, at 155.
[34] *See* EPIC v. DHS - SOP 303, Electronic Privacy Information Center, https://epic.org/foia/dhs/internet-kill-switch/ (last visited May 27, 2016).
[35] Commission Seeks Comment on Certain Wireless Service Interruptions, Federal Communications Commission (Mar. 1, 2012), https://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0301/DA-12-311A1.pdf.
[36] White House, Executive Order: Assignment of National Security and Emergency Preparedness Communications Functions (July 6, 2012), *available at* http://www.whitehouse.gov/the-pressoffice/2012/07/06/executive-order-assignment-national-security -and -emergency-preparedness-.

Conclusion

Thank you for your time and attention to this important issue. If you have any questions on any of the topics brought up in this comment, please contact Amie Stepanovich, U.S. Policy Manager and Global Policy Counsel, at amie@accessnow.org.

Sincerely,

Amie Stepanovich
U.S. Policy Manager and Global Policy Counsel

Drew Mitnick
Policy Counsel