June 2, 2016

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

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

The views expressed herein are presented on behalf of the Section of Science & Technology Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the Association.

EXECUTIVE SUMMARY

The Section of Science & Technology Law (SciTech) of the American Bar Association has long engaged with government policymakers on matters of importance to U.S. economic and national security interests. SciTech demonstrated its leadership in IoT legal and policy issues by hosting the first National Institute on the Internet of Things in March 2016, in Washington, D.C., an event featuring many of the nation's leading IoT legal, technical, and policy experts.

The National Telecommunications and Information Administration has issued a Request for Public Comment[1] (RFC) on a number of issues relating to the Internet of Things. In these comments, SciTech discusses:

---

1 81 *Fed. Reg*. 19956 (April 6, 2016).

(1) the underappreciated importance of scope and scale in IoT technologies and vulnerabilities and the need to accord them greater significance in developing IoT norms and standards;

(2) the lack of adequate coordination among current efforts to establish norms and standards;

(3) the improvements in workplace efficiency and productivity already attributable to the IoT;

(4) the challenges in integrating the Internet of Medical Things with electronic health records, including privacy and security;

(5) the cybersecurity challenges arising from the complexity of IoT devices and networks;

(6) the potential role of NTIA in coordinating IoT privacy and data security policy efforts across the federal government; and

(7) the desirability of handling consumer protection issues arising from the IoT at the agencies having jurisdiction over similar products that are not interconnected.

GENERAL COMMENTS

FROM THE GENERAL SECTION

SciTech members are actively involved in legal and policy issues pertaining to the Internet of Things, advising clients on IoT matters and, as demonstrated by its convening of the first National Institute on the Internet of Things in March 2016, taking a leadership role in policy matters.

SciTech has a long history of working with government policymakers on matters of importance to U.S. economic and national security interests. In the past, SciTech's efforts on PKI, encryption, cloud computing, identity management, and privacy (among other issues) have been recognized as authoritative foundational works in both the legal and larger information technology communities. We hope our comments on IoT also will be viewed as a valuable product of careful and informed deliberation.

For convenience, SciTech will restate the particular questions that it is addressing, followed by its comments.

NTIA 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?

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

From a technological perspective, the most novel and high-impact policy challenge of IoT may derive less from any specific embedded technologies supporting the implementation of devices, tools or software than from two very well-understood and fundamental realities of the explosive nature of IoT deployment: the twin issues of (1) scope and (2) scale. Recent discussions and specific exercises addressing IoT norms and standards have significantly overlooked the massive scale and broad scope of the IoT.

The history of commercial information technology development and deployment is characterized by sector identification, device adaptation, and software adaptation, so that even "general purpose computing" becomes subdivided in practice and nomenclature into such categories as "personal desktop financial computing," "small business financial computing" or "enterprise financial computing." The IoT extends this pervasive presence of system elements across every segment of global economic and social activity; products are often described as "specifically developed for" specific applied environments and functions. These distinctions and market segmentations, however, are very often without meaningful substantive differences.

Nevertheless, they persist, and their existence both exaggerates and clouds the reality of "breadth of scope" for IoT. Certainly, for example, at the operating system level, the limitation of mobile operating systems (iOS, Android) or dominant desktop operating systems (Windows, Mac, Linux/Unix) is far better understood than the concentration (and risk thus inherent in) basic input/output system (BIOS) development and its associated security. Yet a BIOS is required in every modern computing operating architecture; and the copyrights and licensing for most BIOS in use on business and personal desktops and linked devices are held by a single entity, the Phoenix Co., which reports 125 million NEW Phoenix-technology dependent devices deployed each year, with an estimated 5 billion devices in service globally.[2]

[2] See http://www.phoenix.com/pages/phoenix.

The scope of application across many specific sectors — financial institutions, medical services delivery, transportation, manufacturing, and education — may thus seem diverse. But on close inspection, common technologies (and their attendant common risks) exist across billions of users.

Such breadth of scope has consequences for practical security at the maintenance level (i.e., assuring the appropriate capacity for all reliant systems and devices to be updated and secured against evolving threats) and at the attack level, where vulnerabilities leveled at the BIOS level could impact the entire fabric of the networked technology at every level—handheld specialty devices, mobile computing and smart phones, desktops, and even connected proprietary architectures.

Further, the pervasive scope raises the companion policy challenge of scale. Scale challenges exist both in absolute numbers of deployed devices and in the magnitude of risk inherent in an ecosystem where the addition of 250 billion sensors on consumer appliances, or 50 billion North American sensors for highway control devices, portends a completely unprecedented volume of threats against vulnerable devices. This in turn will require a corresponding unprecedented scale of requirements for defensive measures, updates and mitigations in the event of a security compromise.

Multiply this scale globally by even the most pessimistic estimates of IoT systems and the number of devices-at-risk, and the demand for embedded security and security update can be seen as obviously similarly unprecedented, and itself the source of massive unaddressed risk. The scale of remedy required in the event of such a disabling attack at global scale could exceed the capacity of any application vendor, the largest global device manufacturers, a self-help community within an industrial sector, or even national governments to address.

Given such a debilitating security threat, the ability to account for scope, and more importantly scale, in the creation of IoT norms and standards stands as a critical “condition precedent” as these regulatory and voluntary normative efforts continue in multilateral, governmental, national and voluntary SDO communities.

NTIA Question 3. With respect to current or planned laws, regulations, and/or policies that apply to IoT:

a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

---

b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

The largest issue is the proliferation of norms and standards without coordination. In September of 2015, the Open Group, a major sponsor of voluntary standards development activities, including a number directed at the IoT environment, published a document which included a table listing more than 65 discrete normative development activities then underway under the sponsorship of more than 15 SDOs, *ad hoc* standards bodies, multilateral bodies, and national government regulatory bodies.[3]

Many of these activities address valuable concerns, such as data exchange standards and other standards essential to interconnection and interoperability of diverse system components in a heterogeneous global marketplace. Many reflect input and investment of effort by individuals of expertise and repute participating in multiple venues for the specific purpose of assuring consistency in the evolution of technical standards and norms in this explosive environment.

Indeed, some vendors have made significant investments to assure their involvement in many of these normative processes. While this is facially commendable, the history of prior technology standards "events" is dotted with episodes in which vendor participation has exercised a "heckler's veto" that undermines efforts to reach consensus on standards. The U.S. Y2K tech industry and legislative processes in the 1990s, and HHS ONC efforts to achieve interoperability standards for data exchange across electronic health records platforms (EHR), both evidence the potential for delay and even disruption as a result of vendors simply asserting their proprietary interests.

In the case of IoT, there have yet to be reports of specific dilatory behavior in the SDO environments. Nevertheless, the sheer volume of continuing activity, especially in the absence of any formal or informal processes to coordinate these diverse international efforts, makes communicating and understanding of the work of these bodies an invaluable—and presently—missing element of any success. The Open Group's publication of the catalog of pending normative efforts is a landmark effort, which should be supported and continued.

In addition, efforts such as the Industrial Internet Consortium's publication of a Reference Architecture and the "reference architecture" character of portions of the National Institute of Standards and Technology (NIST)-sponsored Public Private working group on Cyber Physical Systems both stand as efforts intended to achieve similar objectives. They do so in part by preparing the ground for

[3] See Open Group Internet of Things Global Standards Initiative (IoT GSI); https://collaboration.opengroup.org/platform3/protected/documents.php?action=show&gdid=33590.

standards development and informing communities of developers, vendors and users of the range of activities appropriate to be considered as IoT deployments proliferate.[4]

The risk of cacophony, and outright normative conflict, whether among standards regimes or between some standards and emerging regulations is present, if not inevitable. The consequences of such a situation, including disputes resulting in litigation and decisions by juries and technically under-informed jurists are not desirable, and suggest the need to address promptly the growth of uncoordinated normative activities.

To remedy this continuing situation, development of a multi-stakeholder multilateral coordination process that, at a minimum, can maintain communication regarding the charters and scopes of work of the various normative bodies should be considered for prompt deployment.

* * * * *

FROM THE ECONOMY SECTION

IoT has already begun to alter the U.S. economy by enabling the development of innovative consumer products and entirely new economic sectors, enhancing a variety of existing products and services, and facilitating new manufacturing and delivery systems. In light of this, how should we think of and assess IoT and its effects? The questions below are an effort to understand both the potential economic implications of IoT for the U.S. economy, as well as how to quantify and analyze the economic impact of IoT in the future. The Department is interested in both the likely implications of IoT on the U.S. economy and society, as well as the tools that could be used to quantify that impact.

NTIA Question 14. What impact (positive or negative) might the growth of IoT have on the U.S. workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?

The IoT has already improved employee safety and productivity through the use of smart technologies and devices and these improvements will only increase over time. Offices and factories will be more comfortable with efficient

[4] Citations to IIC Reference Architecture IIC: http://www.iiconsortium.org/IIRA.htm; and NIST Public/Private Working Group on Cyber Physician Systems Draft Report. https://s3.amazonaws.com/nist-sgcps/cpspwg/pwgglobal/CPS_PWG_Draft_Framework_for_Cyber-Physical_Systems_Release_0_8_September_2015.pdf.

energy saving devices and technologies. Employees may be more efficient and comfortable, leading to improved productivity and employee satisfaction. Devices may take away some jobs and eliminate unskilled positions, but a more sophisticated workforce may emerge.

Monitors of individual behavior such as requiring "swipes" to enter designated areas or restricting logging onto particular devices can control access to sensitive areas and protect proprietary information from misappropriation. Controlling access also improves personal safety by preventing intruders for entering specific locations. At the same time, excessive monitoring of individuals' personal habits, including how often they leave their work area, their food consumption habits, and with whom they associate, could lead to an erosion of personal freedoms that are not job related.

Employer-mandated wearable devices may improve the long term health of employees and reduce health care costs for employers, but could enable discrimination against employees who are physically disabled, suffer from certain diseases or conditions, or simply do not have the time to exercise because of family or other obligations. In addition, the volume and variety of data collected from devices and through monitoring can be merged with other data from other sources for purposes that were not anticipated when the data were collected. While combining data in such a way may conceivably generate social benefits, they also could lead to discrimination and the erosion of personal freedom in the workforce. Consequently, as with all data, there is great good and potential risk related to the use of IoT data in the workforce.

What role or actions should the government take in response to workforce challenges raised by IoT, if any?

At the present time, the government should approach IoT workforce challenges with caution. Existing laws should be enforced when there is evidence of discrimination or disparate impact, or when unfair or deceptive acts or practices harm individual consumers. To date, it does not appear that the introduction of the IoT into the workplace has given rise to abuses that would require additional regulation, bearing in mind that overregulation can chill innovation in the IoT.

In addition, employers should be mindful of the ethics associated with certain of their practices and be ever vigilant in the consideration of individual rights and liberties. Regulators should pay special attention to understand the potentially invasive and discriminatory use of IoT data, especially in the employee monitoring space.

* * * * *

FROM THE POLICY SECTION

A growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.

NTIA 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?

One particularly important policy issue is the role in treatment and personalized medicine of networked medical devices, known as the Internet of Medical Things (IoMT), and their integration into electronic health records. Innovations in science and technology are developing precision medicine to treat and prevent disease on a personally individualized basis.

Research and development in precision medicine require a continuous source of individual health information and big data. The IoMT is a vast pool of that big data.[5] Patient electronic health records are an ideal source of structured information, such as diagnoses, treatments performed, laboratory results, prescription drugs administered, geographic location of patients and, whenever available, the patient's genomic information.

Can medical device data from the IoMT be integrated into electronic health records, both as an aid to providers in treating patients and a resource for precision medicine researchers? Medical device data, transmitted directly to electronic health records, could give physicians instant access to information they may need to make treatment decisions. For example, patient data from pacemakers, blood glucose monitors, insulin pumps, health, wellness and fitness apps could inform healthcare providers as they review patient histories and prepare treatment plans. Alerts from networked medical devices connected to electronic health records might notify diabetics that their blood sugar is too high or too low or that a cardiac patient's pulse is too fast and the patient should seek immediate treatment.

Beyond enabling these forms of treatment, electronic health records can be a rich source of accurate individual health information for research. Data in electronic health records is available for research when authorized by hospital Institutional Review Boards, hospital Privacy Boards or de-identified or provided to researchers in limited data sets under Data Use Agreements with researchers.

[5] The National Institutes of Health, academic researchers at Vanderbilt University, Mayo Clinic, Cleveland Clinic, and many others are using big data analytics technologies, genomics research, bioinformatics, and molecular biology to develop individualized patient treatments for precision medicine.

There are many challenges to putting IoMT data to these uses. Information collected using wireless medical devices cannot reasonably be streamed directly into electronic health records without first addressing and resolving multiple socio-technical and legal concerns. These matters broadly include cybersecurity and patient safety, data accuracy and, as a backdrop, ownership rights in the data collected.

Data transmitted wirelessly to mobile devices through the Internet create a weak point for hackers. Interconnectivity between medical devices and systems for electronic health records leaves the medical devices vulnerable to security breaches in the same way that other networked systems are vulnerable. In 2014, SANS Institute reported that 94% of medical organizations have been the victim of a cyberattack, including attacks on medical devices and infrastructure, potentially affecting patient safety and clinical care. Cybersecurity protection is a multi-faceted problem that involves medical device users, manufacturers, licensees, technical controls, governance, regulators and standards. Healthcare organizations can start to meet the cybersecurity challenge by taking steps to understand and confront the vulnerabilities presently embedded in their networked medical devices.

The Food and Drug Administration (FDA) regulates the safety and effectiveness of medical devices through premarket and postmarket requirements, including design controls under the Quality System Regulations (QSR), 21 C.F.R. Part 820. FDA has issued a series of guidance documents to provide guidance to the device industry on cybersecurity in both the premarket and postmarket environments.[6] The FDA has also issued a guidance document on mobile applications (apps), describing when a mobile app will be regulated as a medical device and when it will not. The functionality of some mobile apps could pose a risk to a patient's safety if the mobile app does not function as intended while performing a medical device function (i.e., while used for diagnosis of a disease or other conditions or the cure, mitigation or prevention of disease).[7]

On January 22, 2016, the FDA issued for comment a Draft Guidance for Industry and FDA Staff on Postmarket Management of Cybersecurity in Medical

[6] FDA Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 29, 2014); FDA Draft Guidance: Postmarket Management of Cybersecurity in Medical Devices (January 22, 2016).

[7] A medical device manufacturer that does not make claims against third party health insurance for its products is not subject to the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that affect healthcare providers unless performing a service for or on behalf of a healthcare provider, i.e., as a business associates of a covered entity under HIPAA.

Devices.[8] The Draft Guidance states that "Cybersecurity risk management is a shared responsibility among stakeholders, including the medical device manufacturer, the user, the Information Technology (IT) system integrator, the health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA." The FDA also notes that best practices for the cybersecurity of medical devices include "collaboratively assessing cybersecurity intelligence information for risks to device functionality and clinical risk," including during the design phase prior to manufacture of the device. Although FDA guidance documents are not binding on the industry or the agency, they do set forth FDA's current thinking on approaches for compliance with FDA regulatory requirements.

Medical devices vary in their functionality and risk, and not all medical devices are interconnected. Furthermore, electronic health records are not currently subject to the same types of regulatory requirements as medical devices. Therefore, there is not one solution to approaching cybersecurity for the IoMT. Consideration should be given to the development of consensus standards that might be appropriate in this area. Appropriate security features could advance patient safety and precision medicine, while facilitating access to a stream of big data for research.

NTIA Question 16. How should the government address or respond to cybersecurity concerns about IoT?

a. What are the cybersecurity concerns raised specifically by IoT How are they different from other cybersecurity concerns?

The nature of IoT devices provides their cybersecurity risk. IoT security depends on the complex interaction of devices, networks, and clients.[9] According a recent review by the Open Web Application Security Project (OWASP, a leading consortium on internet security[10]) in order to improve cybersecurity of IoT, "a holistic approach is required" that takes into account the ways in which IoT presents multiple surfaces for attack. Such an approach will need to consider:

- The IoT device
- The cloud

[8] See http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[9] Here, we use the word "client" in the computer science sense, in which the client is a piece of computer hardware or software that accesses a server. In the IoT context, the client can include end-user clients such as a smart phone, tablet or computer where the owner of the IoT device has installed application software for the IoT device, and which the owner of the IoT device can use to manage data, settings, and activities of the IoT device.

[10] See https://www.owasp.org/index.php/Main_Page.

- The mobile application
- The network interfaces
- The software
- Use of encryption
- Use of authentication
- Physical security
- USB ports

In recognition of these challenges, OWASP established the OWASP IoT Top Ten Things Project in 2014.

Since that time, numerous researchers have reached similar results. For example, Daniel Miessler, a security researcher from Hewlett Packard, briefed at the 2015 RSA conference that IoT devices failed consistently across numerous measures:

- 10/10 security systems accept "123456"
- 10/10 security systems have no lockout
- 70% of devices not using encryption
- 9/10 had no two-factor options for authentication, and
- 8/10 collected personal information.[11]

In brief, research on cybersecurity issues raised by IoT reveals three primary factors: (1) many IoT devices collect personal information; (2) a number of IoT devices fail to provide even basic security measures that are considered best practice in other information security contexts; and (3) the highly networked nature of IoT creates a large number of attack surfaces that can be exploited by an attacker to gain unauthorized access into an organization's network.

b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

Technical professionals must sew together many considerations when building an IoT infrastructure of any kind. Encryption and authentication play key roles in ensuring that cyber security threats are prevented and mitigated. This may require device-level encryption of transactions and communication and

[11] Securing the Internet of Things: Mapping Attack Surface Areas Using the OWASP IoT Top 10, Daniel Miessler, Security Research, HP Fortify on Demand, Session ASD-T10 at RSA Conference 2015.

authentication between devices to thwart data leakage and meddling on IoT content and activity by attackers.

These solutions can impose significant resource and bandwidth constraints on commercial and operational objectives. Proper risk analysis should be employed to provide the proper balance of these technologies in the big picture. The role of government should be to work with private sector entities to provide policies and guidelines to assist with adequate prioritization.

NTIA Question 17. How should the government address or respond to privacy concerns about IoT?

a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

In response to the heightened risk to consumer privacy presented by the Internet of Things, the NTIA should:

- Undertake efforts to educate the public about basic privacy and information security concerns associated with the Internet of Things; and

- Coordinate closely with the Federal Trade Commission and other appropriate government agencies to assess the privacy and security flaws in the IoT.

Pending before a stakeholder and interagency review process at the time these comments are submitted is the Draft Framework for Cyber-Physical Systems (Framework Report).[12] That document was developed in partnership with industry, academic and government experts in the Cyber Physical Systems Public Working Group (CPS PWG)[13] convened by NTIA's sister agency, the National Institute of Standards and Technology (NIST).

Members of SciTech have participated in the CPS PWG since its inception in the summer of 2014. The Framework Report under review is lengthy and

[12] Available at https://s3.amazonaws.com/nist-sgcps/cpspwg/pwgglobal/CPS_PWG_Draft_Framework_for_Cyber-Physical_Systems_Release_0_8_September_2015.pdf.

[13] *See* https://pages.nist.gov/cpspwg/.

covers a wide range of important topics. Unfortunately, its current draft is having difficulty in achieving consensus on topics of extreme importance to many stakeholder constituencies.

The Framework Report, however, has (at least until the results of NTIA's RFC are vetted and published) the unique posture of being one of the few U.S. government or government-sponsored articulations of IoT policy. Along with its extensive scope, that posture makes it natural candidate for citation, reference and reliance. With respect to privacy, the current draft of the Framework Report gives very limited treatment to privacy in the IoT or to cyber security protection of IoT devices and systems and data. Unless the limited treatment accorded privacy and security indicates that a "policy" choice has already been made, the NTIA may have a useful role in play in coordinating IoT privacy and data security issues within the federal government.

NTIA Question 18. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?

Issues of safety and product liability arise as devices associated with IoT inevitably fail or malfunction. The impact of these failures and malfunctions will range from the catastrophic to the merely inconvenient, and will be felt across a broad range of industries and consumers.

In considering how best for government to address these concerns, it is important to recognize a couple of characteristics about IoT that affect any government response. The IoT is not itself a "thing", device or product. Rather, the IoT consists of millions of devices and sensors that are interconnected to other things, sensors and/ or devices. These devices and the data and jobs they do are, or soon will be, ubiquitous. In many respects, the IoT is better thought of as the Internet of Everything.

So, in some respects, the devices and sensors that comprise the IoT are like the products and components of product that exist physically. Like products, the devices and sensors serve a wide variety of industries and consumers. And what many of them do is very specific to the industry and use to which they are put. IoT devices in refrigerators, for example, perform very different functions and create very different expectations than those in cars or those in a smart phone, to use just a few examples.

It may be useful to consider all the industries and area of life that are already touched by the IoT. To name just a few:

- Energy management production and distribution;
- Automobiles;
- Aircraft;
- Household appliances;

- Transportation management including the operation and maintenance of dams, bridges and roadways
- Environmental monitoring;
- Communications devices;
- Computing devices;
- Banking, financial and other consumer transactions and services;
- Marine;
- Manufacturing and workplace safety;
- Food preparation and distribution
- Wearable technology;
- Health monitoring, treatment and devices; and
- Connected home devices such as Internet connect TVs, coffee makers, refrigerators, thermostats, light bulbs.

Unlike traditional products, however, IoT devices are connected, and create and transfer data. This characteristic in turn carries with it a whole range of additional safety, privacy, and other technical concerns.

These similarities with and distinctions from traditional products make a regulatory approach, at least from a consumer product standpoint, difficult.

First, like traditional products, there is no "one size fits all." Rather, like traditional products, the regulation of the IoT must occur within those agencies that bear fundamental jurisdiction over the products affected by IoT devices and interconnections. Acceptable failure rates for automobile and aviation devices are very different from IoT devices that might be used in a child's toy. Creation of responsible and relevant standards of care for IoT devices and their use and interconnection is best left to the agencies with the expertise and background in dealing with specific industry and use concerns. Agencies as diverse as the CPSC, FAA, FDA, FTC, and FCC all have authority here.

A related problem with a broad-brush regulatory approach is that the IoT is and will continue to evolve faster than the ability for regulators to adjust. The technology changes before the ink is dry. The result is that regulation may be at best irrelevant and at worst counterproductive, especially if regulators without expertise in an industry attempt to try to paint with too broad a brush.

Instead, creation of many overall standards of care should be left to the judicial system to develop through specific cases and disputes. While that process may be cumbersome, it has proven its ability to resolve disputes and determine overall standards of care even in unique circumstances. Courts and juries have for years grappled with what is safe and unsafe, what is reasonable conduct and what is not, what is fair and unfair and deceptive, what is warranted and what is not. The same issues can be resolved in connection with the IoT.

This is not to say that the technical issues surrounding IoT devices should go unaddressed by regulators. Regulatory agencies dealing with products containing IoT devices should consider safety issues in addition to privacy and data security. And the government should recognize that many industries and uses will be overseen by more than one agency. Agencies should collaborate in connection with these issues to insure that all issues are addressed and that inconsistent regulation does not occur.

And industry groups should be encouraged by the government to provide education to consumers about IoT devices, their risks and benefits, and the potential from harm.

* * * * *

CONCLUSION

As noted above, the IoT is not itself a "thing," device or product. It is a conceptual structure consisting of tangible things (e.g., commercial and consumer goods containing sensors), real estate and fixtures (e.g., roads and buildings containing sensors), *plus* intangibles (e.g., software and data), *plus* a range of services (e.g., transmission, development, access contracts etc.). Various parts of the structure have independent significance and will be sold, leased, licensed, loaned or provided under variety of contractual or other relationships. Various parts of the structure are constitutionally protected at the federal and state levels, including but not limited to protections for intellectual property, free speech and knowledge-building information or data flows, privacy in one's home and records, and so on.

Any "thing-centric" thinking, such as automatic conceptualization or treatment of an IoT structure as a "thing," will not suffice legally or as a public policy matter. It will be difficult to discern or draw appropriate legal and policy lines because existing laws and constructs were conceptualized before the Digital Era. However, in United States, it is a certainty that any consideration of the government's role in the IoT must address legal mandates that are, above all, constitutionally acceptable.

If the history of digital privacy is any indication, legal and policy matters will vary globally and force differences, making "global" rules for IoT difficult if not impossible. Those differences will also create competition issues. Whether those differences are viewed negatively or positively, they are a fact of life that NTIA will need to consider in its deliberations. Such considerations overlay all of our comments in this document.