TELECOMMUNICATIONS INDUSTRY ASSOCIATION
ADVANCING GLOBAL COMMUNICATIONS
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

Submitted via iot@ofcom.org.uk

October 1, 2014

Attn: Gary Clemo
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA

RE: Comments of the Telecommunications Industry Association in Response to Ofcom's Request for Input on *Promoting Investment and Innovation in the Internet of Things*

Dear Mr. Clemo:

The Telecommunications Industry Association (TIA) hereby submits input to Ofcom in response to its request for stakeholder views on the actions required to ensure that the UK takes a leading role in the emerging Internet of Things (IoT). TIA, representing the global community of information and communication technology (ICT) manufacturers, vendors, and suppliers, believes that the IoT holds incredible potential for positive innovations across segments of the economy and improvements in countless aspects of consumers' everyday lives, and we commend Ofcom for exploring ways in which it can help reach this potential.

I. INTRODUCTION AND SUMMARY

TIA is a global trade association representing approximately 400 global manufacturers, vendors, and suppliers of ICT. On behalf of its members, TIA engages in policy efforts that impact the opportunities, investments, and innovations that bring ICT services and solutions to businesses and consumers around the world. In addition, TIA serves as an accredited standards development organization for the telecommunications industry, housing efforts that address industry-consensus needs across the communications space, including machine-to-machine communications, telecommunications cabling systems, public safety and business/industrial radio communications, and others.

TIA believes that the IoT holds immense promise for investment and innovation that will translate to wide societal benefit. The IoT will be driven by the convergence of exponentially-increasing availability of connected devices in both the public and private spheres, across markets. The ICT industry is continuing to work towards realizing this continuum of connectivity, and we urge Ofcom to ensure that it takes competitive- and technology-neutral approaches to any activity that may impact the deployment of the IoT.

Further, we call on Ofcom to partner with the industry on efforts to ensure informed uses of products and services by consumers.

Ofcom should recognize the importance of, and work to further, the use of global voluntary, open, and consensus-based standards in the IoT. These standards are under development in a number of fora, including TIA, with adoption being driven by mainly competition. Through reliance on these standardization efforts, Ofcom will ensure that scientific expertise from implementers in the private and public sectors is reflected in its approach. Moreover, Ofcom is strongly encouraged to recognize the global consensus that "open" standards are market-driven and allow for the inclusion of patented technologies, which are addressed through the use of fair, reasonable, and non-discriminatory patent policies. Such open standards may be developed across a wide-ranging body of organizations.

In response to its inquiry, TIA also urges for Ofcom to employ a spectrum policy that enables the IoT. Such a policy prioritizes predictability, flexibility, efficiency, and priority for superior rights from harmful interference. Specifically, sharing efforts in the United States may serve as a helpful use case for Ofcom, as well as some approaches that are currently being developed, such as Authorized Shared Access.

Further, when addressing data security and resilience, TIA urges for Ofcom to ensure that it respects competitive differentiation as a driver of enhanced security solutions. Ofcom is also encouraged to take neutral approaches to technology design, rely upon international standards and best practices, fully leverage the public-private partnership model, and the prioritize end-user awareness and education.

Finally, TIA recognizes the ICT industry's priority for addressing data privacy, and recommends that Ofcom ensure that its activities do no impose barriers that would discourage the use of existing and developing voluntary solutions that typically emerge from standardization and best practice development fora, as well as public-private partnerships. Ofcom should proceed cautiously in this area to ensure that are technically feasible and are not overly-burdensome.

II. TIA's GENERAL VIEWS ON THE INTERNET OF THINGS

The "Internet of things" is a broad label for the idea of an increasingly connected future where regular, everyday items will be fitted with sensors and actuators and the ability to connect to networks and transmit and receive data. Machine-to-machine (M2M) communications is a networking term that describes the technology that enables devices to communicate with each other. M2M is the key to the IoT because it encompasses the technologies that are necessary to enable a successful IoT environment. In the new M2M-driven world, there will be a continuous exchange of information between sensors attached to connected, everyday items or infrastructure, computers, the networks, and people. For the future, to work as envisioned, the IoT must be designed to handle the transmission, receipt, and processing of exponential amounts of data.

The penetration of Internet adoption, faster mobile connections, and the availability of advanced computing capability in the form of cheaper, smaller devices with significant processing power has facilitated the growth of the IoT. The key element driving this market is the ability to install inexpensive sensors in machines and devices due to advances in sensor technology that have dramatically reduced the cost, and may rely on geo-location technology, RFID, and many other technologies. The increased availability of low-cost sensors will expand the potential market for M2M, as cost issues in installing sensors in devices are not expected to be significant. These sensors collect real-time data and transmit it via the Internet or wireless networks to computers, other machines, or to people. At the receiving end, application software converts data to useful information. This ability to collect and analyze significant amounts of data is the aspect of the IoT that will be truly transformative. With low-cost sensors allowing virtually any device to become M2M-capable, this new data-centric information, consumers and businesses can make decisions that are more efficient, allowing them to maximize time and cost.

In 2012, an estimated 8.7 billion things were connected worldwide and projections show that with the new technological capabilities this could grow to 50 billion by the year 2020,[1] generating global revenues $8.9 trillion by 2020.[2] TIA projects the IoT will provide significant impacts across service sectors, representing an emerging market that is both unique and enormous. As Ofcom notes, IoT will have a transformative impact in sectors such as healthcare, transportation, and energy; TIA notes that the IoT also holds great potential for other important sectors, such as:

- ***Healthcare:*** the IoT's use of innovative enterprise and consumer health applications will make patient monitoring, diagnostics and treatment more personalized, timely and convenient, while also lowering costs for the healthcare provider. Studies already demonstrate that patients who log their thoughts and behaviors via mobile apps or sensors , so that doctors can monitor them between visits, resulting in better care overall. Examples include how remote monitoring is utilized in home settings for the most chronically ill: monitoring of intravenous infusions, measuring of blood glucose levels, tracking blood pressure, heart rate, and medical grade weight scale readings from the non-

[1] Cisco, The Internet of Things at http://share.cisco.com/internet-of-things.html (last accessed Sept. 29, 2014).

[2] IDC, *The Internet of Things Is Poised to Change Everything, Says IDC* (Oct. 3, 2013), available at http://www.idc.com/getdoc.jsp?containerId=prUS24366813.

hospital setting to health care workers, among many others. These and other critical information datasets can be automatically sent to medical professionals who can analyze trends and alert physicians or care providers, to identify the onset of problems quickly. Systems can also determine the location of ambulances and deploy them efficiently to reduce the time it takes to respond. All of the described benefits are effects that directly correlate with the inclusion of patient-generated health data, particularly via mobile medical applications, in health care systems.

- ***Energy:*** The IoT is transforming the generation, transmission, distribution and consumption of electricity to provide greater automation, increased reliability, improved efficiency and reduced energy consumption through smart grid technologies. The integration of bidirectional communication through an increasing number of sensors and controls to modernize the electric grid, commercial buildings, and residential homes is revolutionizing our energy infrastructure, which until now has seen relatively modest technology advances since the early 1900's. While smart meters have become the face of the IoT for the electric grid, the benefits of the seamless integration between ICT and electric utility infrastructure provided by the smart grid run much deeper. When applied to the electric grid, the IoT has not only the potential to reduce energy consumption and carbon emissions through empowering customers with usage and pricing data enabling better end-use energy efficiency and conservation through real-time feedback, 365 days a year. The IoT also enables time of use pricing to reduce peak demand on the electric grid through demand response programs. Electric utilities are able to use sensors and controls to significantly reduce line-loss in the transmission and distribution of electricity. The IoT also facilitates the integration of more energy efficient consumer uses such as electric vehicles and smart appliances as well as more environmentally friendly energy sources such as the intermittent energy generated by solar and wind. Application of the IoT to the energy sector is providing unprecedented opportunities for both electric utilities and consumers.
- ***Intelligent Transportation Systems:*** Transportation is one of the sectors that is most primed to engage in and utilize the IoT. IoT presents great potential for all modes of transportation but vehicular transport, in particular, using M2M connections is seeing the most significant developments for connected, intelligent transportations systems (ITS). The vehicular ITS market covers the spectrum of applications from infotainment (e.g. gaming entertainment, weather) to connected vehicle technologies to autonomous vehicles. IoT in the transportation space can help to improve driver safety and optimize driving time with information about the location of nearby vehicles and traffic status as well as enhance vehicle performance with predictive maintenance. There are also security features like emergency calling, unlocking a vehicle remotely, and stolen vehicle tracking. These services can be offered as an application in smartphones, integrated into current motor vehicle designs, or as a separate device. Autonomous vehicles, for example, are able to serve as a self-contained source of safety solutions (does not require adoption of the technology by other vehicles or infrastructure upgrades) or it can be complemented by connected vehicle (V2X) offerings. Additionally, the growth of vehicular ITS points to opportunities in not just the consumer market but the commercial and public sector as well.

The IoT will utilize the gamut of network approaches and architectures, and given the wide range of services and solutions envisioned by the IoT, no particular network configuration can serve as the "best" solution. The IoT of the future will exist on an ever-advancing infrastructure so IoT will need to utilize

technology that is wireline and wireless technology, legacy and cutting edge. TIA represents the global community of manufacturers, suppliers, and vendors that create and build all the myriad physical components of broadband infrastructure from routers and servers to amplifiers and fiber nodes which will enable the IoT to grow.

The IoT is clearly in its nascent stages, and holds great potential. As ICT manufacturers and vendors work to meet the needs of their customers, competition will ultimately determine which products and services will succeed and fail in the market, driving ICT manufacturers and vendors to further innovate. As businesses increasingly make investments in the IoT, an utmost concern for Ofcom should be to take a competitive- and technology-neutral approach to respect the need for specific sectors to utilize creative solutions, and for innovators to address the needs of market segments.

Ofcom should also ensure that it avoids any role that would have a government actor be in a position to determine the future design and development of technology. To do otherwise would set a precedent of interfering with the core innovation engine of the ICT sector, negatively impacting the interoperability and standards that are needed for IoT proliferation. Should a well-developed public policy case based on the consensus of stakeholders find that regulatory activity by Ofcom is needed, we strongly encourage Ofcom to promote the competitive dynamic by adopting regulations that are outcome-based, allowing for innovation to thrive while still achieving the regulatory requirement.

The ICT industry recognizes that the emerging IoT marketplace is a great opportunity for growth. This cannot be achieved without both business and consumer buy-in and adoption of these new services: across the ICT manufacturer community, companies are already conducting outreach today to inform increasingly shorter product cycles as they compete in the global ICT market. In addition, since the penetration rate for mobile, wireless devices has grown, consumers are increasingly more aware of the enormous benefits and possible risks. To ensure awareness, industry is committed to continuing to conduct outreach to consumers and use transparent policies that enable informed use. This is an area where government can contribute by conducting outreach and awareness campaigns and providing tips to the public through consumer agencies.

III. TIA VIEWS ON SPECIFIC ISSUES AND AREAS RAISED BY OFCOM TOWARDS PROMOTING INVESTMENT AND INNOVATION IN THE INTERNET OF THINGS

The global ICT manufacturer, vendor, and supplier community is committed to the success of the IoT. Building on the above, in order to encourage the investment and innovation that will speed the realization of the IoT's benefits, TIA has found consensus around a number of principles, which we expand on below.

a. Encouraging and Leveraging Voluntary, Open, and Consensus-Based Standards is Key to the Success of the Internet of Things

i. The Role of Standards in the Success of the IoT

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards that will pave the way for devices to connect to the network. In response to industry consensus, standards that enable the success of the IoT will cut across market segments, and will range from overarching guidelines to specific technical criteria, ensuring increasing interoperability as well as backwards-compatibility. Importantly, these standards are able to dynamically adapt to needed changes based on the expertise across stakeholders. These standards also reduce costs because manufacturers and software developers can produce for multiple applications and multiple end uses allowing for the benefits of economies of scale.

TIA expects the development of IoT to be driven by a global – not regional – approach that is based on the development of open, voluntary, and consensus-driven standards. Numerous standardization efforts already in existence, as well as future efforts, to address industry-consensus needs, will define and contribute to the development of an interoperable IoT. TIA broadly supports the "multiple path" approach to the development of international standards, where healthy competition amongst these efforts will result in market-driven solutions. For example, TIA's Engineering Committee TR-50 M2M (Smart Device Communications) is responsible for the development and maintenance of access agnostic interface standards for the monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications or networks. These standards development efforts pertain to but are not limited to the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.[3]

As a founding member of oneM2M, TIA is continuing to make positive advances in standards development internationally. oneM2M is a global organization creating a scalable and interoperable standard for communications of devices and services used in M2M applications and the Internet of Things. Formed in 2012 by seven of the world's preeminent standards development organizations, oneM2M membership today consists of thought leaders from a broad range of industries, including industrial manufacturers and suppliers, consumer device manufacturers, component suppliers, and telecommunications service providers. oneM2M Partner standards development organizations are: ARIB

[3] *See* http://www.tiaonline.org/all-standards/committees/tr-50.

(Japan), ATIS (U.S.), CCSA (China), ETSI (Europe), TIA (U.S.), TTA (Korea), and TTC (Japan). Additional partners contributing to the oneM2M work include: the BBF (Broadband Forum), Continua, HGI (Home Gateway Initiative), the New Generation M2M Consortium - Japan, and OMA (Open Mobile Alliance). oneM2M specifications provide a framework to support applications and services such as the smart grid, connected car, home automation, public safety, and health. oneM2M actively encourages industry associations and forums with specific application requirements to participate in oneM2M, in order to ensure that the solutions developed support their specific needs.[4]

Because standardization is a form of economic self-regulation, it can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways. TIA urges Ofcom to defer to these standards as they are developed and come to define the IoT. By taking this approach, Ofcom can use these standards as valuable sources of scientific and technical information developed with the assistance of private sector experts, allowing for agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area. Such standardization efforts include, but are not limited to: TIA's TR-50 (Smart Device Communications);[5] oneM2M;[6] the Internet Engineering Task Force, (IETF);[7] and the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.[8]

ii. Open Standards and the IoT

While TIA believes that Ofcom appreciates the role of standards in the growth of the IoT, TIA has concerns with Ofcom's reference to "open versus proprietary" standards in its discussion of how IoT services could be deployed. Recently, there have been some attempts to re-define "open standards" that may disrupt the development of standards and the related balance of interests. For some, the concept of "open" is being equated with patented technology that is "free" (without payment) or "free to use freely" (without payment and without any restrictions). These proposed re-definitions are being used to advocate policy changes that would undermine the rights of those who have invested in the development of the standardized technology.

While the notion of patents being "free to use freely" is superficially attractive, like most "free" things, it comes at a cost. Technological capabilities and innovations most often result from substantial investments in R&D. Such investments typically drive the growth of the investor's patent portfolio. If patent holders in standards-setting activities are expected to give away or waive their patent rights, there are likely to be significant adverse results including that technology leaders will reduce or cease participation in (or technical contributions to) voluntary standards-related activities; or individuals and organizations will not invest (or will invest less) in the development of innovative and next-generation technology in the technical

---

4 *See* http://onem2m.org/.

5 *See* http://www.tiaonline.org/all-standards/committees/tr-50.

6 *See* http://www.onem2m.org/.

7 *See* http://www.ietf.org/.

8 *See* http://standards.ieee.org/innovate/iot/.

areas subject to standardization, thereby creating innovation "dead zones" in those areas. These adverse results would cause (a) the standardization system; (b) its open, voluntary and consensus-based process; and (c) ultimately the resulting open standards, to be less effective or successful than they are today. Moreover, TIA believes that these results would have a negative impact on global respect for intellectual property that helps stimulate innovation and develops local economies around the world.

True "open standards" are market-driven, and promote competition and innovation. The ITU, for one, has well-established views on what constitutes an open standard,[9] which TIA supports and urges the United Kingdom to align with. Such standards are developed or ratified through a voluntary, open and consensus-based process. This process is defined by flexible policies that balance incentives to participate in and contribute to the formulation of standards. This process benefits users and consumers by the broad implementation of the resulting standards. One element of a voluntary, open and consensus-based process addresses the inclusion of patented technologies. The patent policies of standards organizations typically find a balance among differing interests. For example, implementers need to access and use patented technology included in the standard. Patent holders need to preserve their rights in a way that encourages them to contribute their innovative solutions to the standardization effort. Fair, reasonable, and non-discriminatory (FRAND) patent policies seek to provide this type of balance by helping to make that patented technology available to all on "reasonable and non-discriminatory" (*i.e.*, FRAND) terms and conditions.

Further, TIA supports the following principles of an "open standard":

- The standard is developed and/or approved, and maintained by a collaborative consensus-based process;
- Such process is transparent;
- Materially affected and interested parties are not excluded from such process;
- The standard is subject to FRAND Intellectual Property Right (IPR) policies which do not mandate, but may permit, at the option of the IPR holder, licensing essential intellectual property without compensation; and
- The standard is published and made available to the general public under reasonable terms (including for reasonable fee or for free).

[9] *See* http://www.itu.int/en/ITU-T/ipr/Pages/open.aspx.

b. A Spectrum Policy that Enables the Internet of Things

The Internet of Things will rely significantly upon maximizing *continuity of connectivity*. With the world rapidly becoming wireless, establishing an appropriate spectrum policy is therefore essential to ensure that the IoT will be successful.

Radio spectrum has never before been more important. In commercial communications networks, mobile data use is exploding as consumers embrace smartphones, tablets and other devices. Wireless connectivity is becoming the way in which consumers access the Internet from technologies such as LTE, Wi-Fi and satellite. Governments worldwide also have a significant dependency on spectrum for both communications and non-communications purposes.

Meanwhile, radio technologies themselves are changing, placing new demands on spectrum allocations, and raising new operational and regulatory challenges. As a result of these dynamic changes, spectrum allocations and uses that may have sufficed during the 20th century are increasingly under stress.

Unfortunately, policymakers are no longer writing spectrum policy on a blank sheet of paper, and virtually all spectrum suitable for mobile service has been allocated. For that reason, TIA believes that any national spectrum policy must reflect the following principles to allow the use of radio spectrum to evolve to meet changing demand and promote innovation:

- *Predictability.* Spectrum allocations need to be predictable. Identifying demand and changes in demand, understanding the pace of radio technology development by platform, and long term planning are all essential parts of a spectrum policy that can provide predictability for both commercial and government users.

- *Flexibility.* For commercial allocations, flexible use policies consistent with baseline technical rules that are technology-neutral have proven to be the best approach. Any government allocations of spectrum should be managed to ensure better usage of scarce spectrum resources for all users.

- *Efficiency.* Policies should encourage more efficient use of spectrum where technically and economically feasible. In particular, policies should prioritize *global harmonization* and coordination or spectrum allocations;[10] protection from harmful interference for licensed uses; adjacency to similar services; and allocations of wide, contiguous blocks of spectrum. Cleared, exclusively licensed spectrum allows for the most efficient and dependable use of spectrum for commercial mobile broadband deployment.

- *Priority.* In cases where spectrum sharing is technically and economically possible, policies must advance good engineering practice to best support an environment that protects those with superior spectrum rights from harmful interference.

[10] Globally harmonized spectrum is essential to ensure the economies of scale that will facilitate the large-scale deployments necessary to fully utilize the promise of new technologies. Global harmonization also facilitates roaming, which is an important part of creating the "continuity of connectivity" required for the Internet of Things.

Focus on Spectrum Sharing. In recent years, increasing attention has been focused on spectrum sharing as a means to increase the efficient use of spectrum and to help alleviate challenges in spectrum scarcity. In particular, spectrum sharing techniques could eventually prove critical towards enabling the *continuity of connectivity* that is so critical for the Internet of Things. In the United States, efforts are underway in several contexts, including:

- Transitioning the AWS-3 spectrum (1755-1780 MHz), currently used by the U.S. Department of Defense and other government users, to commercial use;
- Opening the 3.5 GHz band (3550-3650 MHz) to commercial uses, potentially including a scenario whereby licensed and unlicensed users can co-exist, perhaps using new technologies such as *small cells.*
- Supporting public and private-sector research and development efforts towards new technologies that will increase spectrum utilization through sharing.[11]

Europe has achieved some promising developments related to Licensed Shared Access (LSA) approaches. LSA is a "third way" spectrum management system that combines elements of traditional "command and control" spectrum management with geolocation technology, e.g., by providing users with a "token" to use spectrum at certain times/places. LSA approaches show great promise as a means to enable sharing among disparate uses. They provide a means to ensure ongoing viability of incumbent uses by creating a policy environment that enables compatible operations with new uses. Meanwhile, these approaches also provide secondary users a means to gain access to spectrum that is already licensed to one or more primary users, but may be under-utilized or capable of supporting multiple uses.

c. Solutions for Security and Resilience in the Internet of Things

With the IoT naturally meaning an ever-increasing number of "things" being connected throughout society, new and evolving security issues will emerge as challenges. Already, ICT members consider security issues into the design of products and services, and this approach will continue to mitigate threats as the IoT develops and proliferates. The IoT represents an opportunity for greater security through the use of a network approach that is paired with proper risk management techniques, where IoT devices can be made to work together to produce comprehensive, actionable security intelligence in near real-time. These approaches and risk management techniques are by and large driven by market demands, typically manifested through industry-driven best practices and standards developed in open, voluntary, and consensus-based fora. In response to Ofcom's request for input on the steps required to enable the IoT to support high levels of security and resilience, TIA, building on the above, urges Ofcom to be guided by the following principles:

First, Ofcom is urged to respect competitive differentiation and business continuity, and to view this as a driver of solutions to security issues. As ICT manufacturers and vendors work to meet the needs of their

[11] TIA, *Spectrum Sharing Research and Development* (Oct. 20, 2013), *available at* http://www.tiaonline.org/sites/default/files/pages/SpectrumSharingR%26DPaper%3D10-20-13.pdf.

customers, less secure products that are more vulnerable to cyber attacks will naturally be less attractive in the market. This drives ICT manufacturers and vendors to strive to make their products and services less susceptible to cyber attacks. To illustrate how much this concept drives enhanced cyber defenses in ICT products and services, we note worldwide spending on total information security spending is projected to reach approximately $76.9 billion.[12] To what degree an organization's performance goals are used to ensure their ability to provide essential services while managing cybersecurity risk will be dependent upon the specific needs of their sector and organization. However, ICT manufacturers work with the range of organizations they supply to ensure that performance goals of those organizations are reflected in the ICT they purchase. The flexibility to innovate and the use of voluntary, consensus-based standards are both key enablers of this capability. We urge Ofcom to take great care to avoid altering this virtuous effect.

Ofcom should also avoid any role that would have a government actor be in a position to determine the future design and development of technology. To do otherwise would set a precedent of interfering with the core innovation engine of the ICT sector, pulling apart the innovation, interoperability, and standards that are needed to drive security and innovation into the global network. There is no "one size fits all" solution to securing the IoT. The reach of the IoT across segments of the economy that will have varied levels of risk illustrates this.

Further, we urge Ofcom to recognize the necessity of international approaches and standards to cybersecurity. Numerous standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners & operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels. TIA urges Ofcom to ensure that its approach to the IoT reflects the priority for the development of internationally-used standards and best practices. The global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and a global supply chain can only be secured through an industry-driven adoption of best practices and global standards. ICT products are often designed and built in different locations using globally-sourced components, and to control costs and manage supply chain risk, manufacturers need flexibility to change component suppliers for a particular product at any time. Any approach taken by Ofcom should involve international cooperation and heavy engagement with the private sector, and country-specific standards should be avoided. Ofcom is discouraged from enacting cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system.

Next, we urge Ofcom to fully utilize the successful public-private partnership model. Public-private partnerships are an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face. The voluntary, public-private model is also able to evolve in response to changes in threats and the risk environment. As both the complexity and number of attacks grow, it will be critical that Ofcom and other governments leverage and augment, or create where necessary, public-private partnerships.

Lastly, TIA believes that end-user education is also a crucial aspect to improving cybersecurity in the IoT, as many cyber vulnerabilities are already known and related attacks are relatively easily preventable.

---

[12] Gartner, *Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware* (Aug 22, 2014), *available at* http://www.gartner.com/newsroom/id/2828722.

Ofcom should lead efforts to inform end users across the business and consumer communities of proper steps to take to ensure that proper cyber "hygiene" is impressed.

d. Flexibility in Addressing Data Privacy

The ICT industry recognizes privacy as a priority in the success of the IoT, and understands the wide range of related concerns held by stakeholders. The issue of data privacy in the IoT is an important issue that Ofcom appropriately includes in its request for input, and which industry actively works on today to proactively address due to existing legal requirements as well as for competitive reasons. Ofcom should ensure that its activities do not impose barriers that discourage the use of these dynamic voluntary efforts to address privacy concerns that are developed through standardization and best practice activities and public-private partnerships. TIA would urge Ofcom to focus on ensuring interoperability of differing privacy approaches to ensure unnecessary barriers are not erected to cross-border data flows between jurisdictions. The U.S.-EU Safe Harbor framework provides an important example of a framework of interoperability, which has facilitated transatlantic commercial data flows while respecting the privacy approaches in each jurisdiction .

Industry believes that any IoT services must be transparent about what data will be collected, how it will be used, and provide options for managing data access in order to allow the user to make an informed choice. We urge regulators not to adopt privacy regulations that would make it impossible for IoT systems to flourish, as data will need to be retained and used in ways not currently contemplated, even by IoT innovators themselves. Instead, industry should be allowed to adopt best practices which can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing.

Consistent with our discussion above, to incentivize the use of privacy standards and best practices, Ofcom is advised to avoid implementing privacy obligations which are ambiguous, overly burdensome, or technically infeasible. The effect of adopting such policies would be to decrease the reasons for innovative industry members to invest in IoT opportunities due to resulting regulatory uncertainty and unnecessarily higher risk. Industry members exploring IoT opportunities should have this certainty while also maintaining their ability to determine the most appropriate method to meet these requirements. TIA believes this approach would best promote the development of the IoT as it is a fluid and quickly evolving market opportunity.

Finally, Ofcom may serve an important role in ensuring IoT data privacy through public awareness efforts. Through "cyber hygiene" education efforts, many breaches that would result in a loss of data privacy can be avoided. In addition, a more informed end-user is more likely to understand the privacy implications of utilizing IoT devices and services, which will help consumers make more knowledgeable decisions.

IV. CONCLUSION

We appreciate Ofcom's request for input on ways to increase investment and innovation in the IoT, and urge consideration of the positions stated above. Please contact the undersigned with any questions.

Respectfully submitted,

October 1, 2014