Filed electronically: iot@ftc.gov

May 31, 2013

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

   RE: **FTC Request for Information on the "Internet of Things"**

The Software & Information Industry Association (SIIA) is pleased to provide the following comments in response to the Request for Information issued by the Federal Trade Commission ("FTC" or "Commission") on April 17, 2013.

SIIA is the principal trade association for the software and digital information industry, representing more than 500 member companies that publish and distribute digital information, provide software applications and related Internet-based services.

With these comments, we also request the opportunity to participate in the public workshop on this topic scheduled for November 21, 2013.

I. Introduction – The "Internet of Things" is an Enabler of Data-Driven Innovation

Today, we are at a key inflection point in the history of information technology (IT). The last several years have brought about significant advances in IT, representing an evolution for IT from a specialized tool into a pervasive influence on nearly every aspect of everyday life. This rich new environment has arisen from the convergence of several technological advancements such as the increasing use of sensors, actuators, and data communications technology, the increasing availability of pervasive analytics and the evolution towards "cloud" or remote Internet computing, where data storage and processing is available as a service on demand, provided with greater efficiency and with increased security.

In the late 19th century, electricity was initially associated with the critical function of providing light. Of course, as was soon realized, the application of electricity as a driver for a wide range of not yet conceived devices and appliances would go on to revolutionize the

world. So too is the anticipated impact of the Internet, as it develops from primarily a computer to computer communication network into a ubiquitous network linking electronic devices and everyday objects. This latter development is often referred to as the "Internet of Things." As much innovation and social, educational and economic opportunity has been presented by the Internet to date, the opportunities increase exponentially with the Internet of Things.

Early assessments of The Internet of Things focused on the use of RFID chips to tag objects in the supply chain.[1] Initial attempts to address policy issues raised by the Internet of Things looked to a single all-inclusive framework to regulate this technology is all of its implementations and uses.[2] Current understandings such as that evidenced in the FTC's notice recognize that the technology is more pervasive and more varied than initial assessments:

> "Consumers already are able to use their mobile phones to open their car doors, turn off their home lights, adjust their thermostats, and have their vital signs, such as blood pressure, EKG, and blood sugar levels, remotely monitored by their physicians. In the not too distant future, consumers approaching a grocery store might receive messages from their refrigerator reminding them that they are running out of milk."[3]

SIIA encourages the FTC to avoid the initial regulatory instinct to find a single all-inclusive policy framework that can resolve all the myriad policy issues encompassed by the convergence of multiple cutting-edge technologies.

As SIIA recently identified in a SIIA white paper on "data-driven innovation," it is this new Internet-enabled IT ecosystem that is leading to increases in the amount of data available and the ability to derive innovative outcomes that will provide tremendous economic and social value, capable of transforming the way we work, communicate, learn and live our lives.[4]

Ranging from vehicles to household appliances and beyond, there is a growing supply of data inputs, sensors and interfaces, along with a growing demand by users. Software and apps are rapidly evolving as services offered seamlessly across devices and platforms—some of these devices are mobile, and some fixed.

---

[1] OECD, Foresight Forum "Radio Frequency Identification (Rfid) Applications And Public Policy Considerations: Proceedings," October 5, 2010.
[2] European Commission, Recommendation on RFID, May 5, 2009.
[3] FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things, April 17, 2013.
[4] Software & Information Industry Association, "Data-Driven Innovation, A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data," May, 2013.

Additionally, while data analytics have been around for quite some time, what's new is the increasing capacity for enterprises and governments to analyze and use this information—from a variety of voluminous sources of structured and unstructured data, real-time and static — to innovate and achieve improve the outcomes of everyday life. Entrepreneurs, established businesses and governments are putting data to work to change the world for the better, applying their innovations to everything from roadways, to financial services, education, healthcare, consumer goods and food production.

In summary, rapid technological evolution is driving a world where exponentially more data is available for innovative use, and this data-driven innovation has already begun to transform how we communicate, learn and consume information—of course, today we are only experiencing the tip of the iceberg. Consumers, citizens and society as a whole stand to benefit greatly from innovative uses of data to improve health outcomes, streamlining and enhancing financial services, enhancing education and learning, and improving and maximizing our physical infrastructure.

II. Data-Driven Innovation is a Driver of Economic Growth

A range of previously unimaginable applications of data-driven innovation are already being produced—or will be in the near future. These innovations are making people's lives better and safer and more prosperous, while also improving energy efficiency and saving money. In turn, data-driven innovation has already begun to spur substantial economic and job growth in the U.S. and around the world.

It is difficult to quantify the full economic impact of data-driven innovation because it is taking place across various different sectors of the economy. However, recent research has begun to accomplish this from various different methods.

In research around "big data" or "data collected and analyzed from every imaginable source," Gartner projects that such data analytics and related capabilities will drive $34 billion of IT spending in 2013.[5] Further, the firm concludes that these technologies are becoming an engine of job creation as businesses discover ways to turn data into revenue. By 2015, the firm expects data to lead to the creation of 4.4 million IT jobs globally, of which 1.9 million will be in the U.S. Further, applying an economic multiplier to those jobs, Gartner expects that each "big data" IT job added to the economy will create employment for three more people outside the tech industry in the U.S., adding six million jobs to the economy.[6]

---

[5] "Gartner Says Big Data Will Drive $28 Billion of IT Spending in 2012." News | Business Wire. Business Wire, October 17, 2012.
[6] Thibodeau, Patrick. "Gartner: Big Data to Create 1.9M IT Jobs in U.S. by 2015." InfoWorld. October 22, 2012.

Gartner's conclusions closely track recent research by the Centre for Economics and Business Research (Cebr). In an independent economic study conducted in 2012, Cebr investigated how organizations in the United Kingdom could harness the economic value of data through the adoption of data analytics. Cebr established a measure of the aggregate economic benefits that could be gained for organizations in the private and public sectors in the UK, terming the economic value of data as "data equity." In identifying six mechanisms, including customer intelligence, supply chain intelligence, performance, quality and risk management and fraud detection, Cebr estimates that data equity was worth £25.1 billion to UK private and public sector businesses in 2011. Further, Cebr notes that increasing adoption of big data analytics technologies will result in bigger gains, and we expect these to reach £40.7 billion on an annual basis by 2017.[7]

III. Policy Recommendations

The FTC has identified privacy and security as relevant challenges to unleashing the opportunities of the Internet of Things. Indeed, privacy risks need to be weighed against potential societal benefits. And in many cases, The Internet of Things and data-driven innovation can thrive on the use of de-identified data.

One of SIIA's core policy principles is that polices must not be developed today which are based on a snapshot of current technology. Today's dynamically evolving ICT ecosystem is certain to be very different tomorrow. Policies should be made today that allow for the long-term evolution of the industry in ways that cannot yet be predicted. This calls for policymakers to take a holistic approach and remain technology neutral, to be cognizant of the rapid evolution of ICT, and support flexible, open-ended rules rather than specific mandates.

Additionally, SIIA urges policymakers to proceed cautiously if formulating any new data policies, as these are likely to steer the future of DDI and the scope of what is possible for American innovation for decades to come. Policies that seek to curb the use of data could stifle this nascent technological and economic revolution before it can truly take hold. **A second core policy principle of SIIA is that policymakers should avoid creating broad policies that curb data collection and analysis.**

Accordingly, as the FTC considers policies regarding The Internet of Things, particularly focused on privacy and data security, SIIA offers the following specific policy recommendations that comprise a reasonable reassessment of the privacy landscape:

---

[7]Centre for Economics and Business Research Ltd. "Data Equity: Unlocking the Value of Big Data." SAS: The Power to Know. SAS, April. 2012.

1. Policymakers should continue to promote technology neutrality and avoid technology mandates.

Technology neutrality has long been a widely recognized guiding principle for technology policies, particularly Internet-based ICT. This was first recognized within the U.S. government in 1997, with the Framework for Global Electronic Commerce, a framework that has stood the test of time in establishing broad principles for regulating ICT, that "rules should be technology neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future)." By contrast, Government-mandated technology standards, can freeze the development of new technologies, or disadvantage entire categories of market players.

These long-held principles for resisting technological mandates and maintaining technological neutrality is especially important for a complex IT ecosystem that will comprise the Internet of Things, one which will be inherently subject to constant innovation. For example, given the range of devices that lead to the collection and utilization of data, it is impractical and ineffective to create policies based solely on a specific type of device, or an arbitrary characteristic of a device, like whether it is mobile like a smartphone or automobile sensor, or whether it is stationary, such as a computer or a refrigerator. While it might seem practical to target specific devices or platforms, this approach is likely to become dated within a matter of months or years due to the rapid evolution of IT.

Further, mandating types of encryption or approaches to de-identification might seem like good approaches for enhancing privacy and data security, but such approaches continue to prove incapable of keeping up with technological evolution. There is almost always a better way to accomplish a given purpose waiting around the corner. Policies must continue to encourage innovation to find faster, better, and less expensive ways to protect privacy and security.

For instance, while technology that designs protection in the concept and engineering phases—e.g. privacy by design—provides the most efficient way to provide for data privacy and security, government policies requiring specific technological solutions have consistently proven to be ineffective.

2. The Internet of Things requires a policy framework that provides for an evolving view of privacy rights based on risk and societal benefits.

There are a wide range of perspectives about the implications of data's growing role in everyday life. On one end of the spectrum, there is distrust of the use of data beyond limited, specifically identified purposes. This distrust heeds a call to minimize data collection and use for fear that it inhibits privacy. On the other end, there is the recognition of data as a valuable asset that is empowering innovation and economic opportunity. Data's use should be balanced to protect privacy and prevent harm to citizens and consumers. Technologists, privacy advocates and policy makers can work together to foster the societal, governmental and business opportunities provided by data-driven innovation, while also meeting the challenge of protecting privacy.

As technologies evolve, sometimes becoming more personalized and instrumental in all facets of our lives, our experience and expectations of privacy also evolve. In the past, privacy was viewed as a personal good, rather than a societal one. As such, privacy was regarded as a matter of individual choice and responsibility.

However, the Internet of Things will continue to challenge this individualist paradigm of privacy. The socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection. It is therefore critical for policies to balance principles of privacy against societal values such as public health, national security, economic growth, the environment, and more in ways that do not put the entire burden on the individual.

The possibilities created by technological changes bring about new social norms and expectations about the flow of information. Privacy expectations not only differ across societies, but they evolve over time. Policy frameworks must therefore remain sufficiently flexible to accommodate these evolutionary changes.

Policymakers should thoroughly consider the opportunities and challenges of the Internet of Things, balance the spectrum of privacy laws and potential privacy risks, being sure to recognize that socially acceptable norms of privacy are evolving along with technology.

3. The principle of data minimization should be re-interpreted to maximize opportunities presented by the Internet of Things and data-driven innovation.

Fair Information Practice Principles (FIPPs) have provided guidelines for policymakers and data stewards regarding responsible information management practices for many years. However, over time, it is critical to reexamine and reinterpret these principles in light of changing technological capabilities and shifting expectations of privacy. Data-driven

innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive.

This principle says that data should only be collected for a very specific purpose, identified and clearly limited in advance, and then should be discarded as soon as this narrow purpose is accomplished. This notion of data minimization is meant to protect individuals from privacy harms by collecting only the minimum amount of data and then destroying it as soon as possible.

While the objective is laudable and the approach very practical in certain instances, there is a tension between this method of protecting privacy and the new capabilities presented by the Internet of Things and data-driven innovation, which thrive on enormous volumes of data and the discovery of novel, unanticipated connections within them. Data-driven innovation is about maximizing data to identify new meaning and values among a wide range of seemingly unrelated data.

In this context, data minimization should not become a rigid construct formally established through legislation or regulation. Rather it must continue to remain a key element of good data stewardship, which balances risk. For instance, there is no business need to store credit card security codes after a transaction has been processed, and saving such information creates substantial fraud risks. A reinterpreted data minimization principle would dictate that such information not be retained.

The combination of privacy by design techniques and adherence to a set of responsible data principles can create an effective framework for data minimization that balances privacy with innovation and accounting appropriately for risk.

4. Policymakers should encourage de-identification as a way to balance the needs of data-driven innovation and privacy protection, but avoid broad mandates to this end.

Some of the most important outcomes of the Internet of Things and data-driven innovation do not rely on personally identifiable information. Even if personal information is collected, it can often be immediately de-identified in a way that does not affect its value or utility for accomplishing important public and social objectives. This allows for robust privacy protection, since the data can be effectively purged of all reference to a specific individual for innovative and societally beneficial purposes.

The Internet of Things complicates the discussions surrounding the definition of "personally identifiable information," clearly casting aside the technical discussion about what is or is not personal, and focusing on which activities are desirable and socially acceptable. The caution here, however, is that if information that is not individually identifiable comes

under full remit of privacy laws based on a possibility of it being linked to an individual at some point in time through some conceivable method--no matter how unlikely-- this could not only prohibit many beneficial uses and benefits of data-driven innovation, but it could also destroy the incentive to de-identify the data.

Public policy should encourage this de-identification of personally identifiable information, where appropriate, but avoid broad mandates to this end.

5. With respect to the collection of personal information, policies should seek to focus more attention on appropriate, accountable use and harm.

Expectations surrounding the collection and processing of personal information are not purely personal. They reflect entrenched social norms of the appropriate flow and use of information.   These social norms are then embodied in legal, social, and cultural systems that differ across myriad countries and jurisdictions. Policymakers face the challenge to reconcile these different systems in a world where data easily crosses not just borders, but legal and cultural boundaries.

Policymakers should continue to consider the practicability of obtaining true and informed consent. Often the requirement to get consent acts as a barrier to socially beneficial uses of information, not because people object to the collection or use, but because the process of obtaining consent is itself too cumbersome and expensive.   Public policies should also recognize that in some cases consent should not be required at all, as many current privacy rules already recognize in the case of fraud prevention or security risk mitigation. In other cases, consent should be assumed from the context, and subject to a right of refusal. Policy makers need to be targeted and specific about which circumstances require explicit consent for the collection of personally identifiable information.

Notice and consent will remain critical components in many specific or sensitive circumstances. However, to maximize the opportunities presented by the Internet of Things and data-driven innovation, policies should take a more practical approach, shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability.

6. Open standards are critical enablers of the Internet of Things, but they must continue to evolve through industry-led standards development organizations, not governments

The ability of devices to increasingly communicate with each other, and with people, is integral to the Internet of Things, as is the ability to integrate multiple data sources to enable data-driven innovation. After all, machine-readability is the key to data analytics, and the "connectability" of data to other data. Therefore, open standards are critical

combining a wide range of data sets across myriad analytics environments and applications. Open application programming interfaces (APIs) also enhance innovative uses of data that that enable applications to interact effectively. Conversely, the advantages of the Internet of Things and data-driven innovation could be squandered where boundaries are erected unnecessarily by proprietary data standards and closed APIs.

As DDI and data centers continue to evolve, practical, cost effective new practices will continue to drive data analytics and network architectures based on open standards. Industry-led standards development organizations are well suited to determine which standards will best implement the policy goal of data interoperability.

Governments can play a key role as a facilitator and convener, applying open standards practices to their own data, and encouraging and facilitating coalescence around open standards. However, governments must resist the temptation to enact policies that impose requirements around specific technical standards or try to create new standards where they may not exist. Attempts to dictate interoperability conditions could have the undesirable consequence of reducing the marketplace to a standardized set of products and services.

IV. Conclusion

Thank you again for the opportunity to submit comments on this topic. As stated above, SIIA would like to participate in the workshop that the Commission is arranging in November. If you have questions or would like to discuss these comments in further detail, please contact David LeDuc, SIIA Senior Director for Public Policy, at dleduc@siia.net, or (202) 789-4443.

Sincerely yours,

Ken Wasch
President