Privacy and Security Implications of the Internet of Things

Response to the US Federal Trade Commission Request for Comments

Alexander Ilic (Auto-ID Labs, ETH/HSG Switzerland)
Mark Harrison (Auto-ID Labs, Cambridge, UK)
Rahul Bhattacharyya (Auto-ID Labs, MIT, USA)
Elizabeth Board (GS1 Global Office)
Massimiliano Minisci GS1 Global Office)
Rebecca Humora (GS1 US)
Bernie Hogan (GS1 US)

12th March 2014

Auto-ID Labs White Paper WP-BIZAPP-067

WP-BIZAPP-067

Executive Summary

This White Paper is a response to the Request for Comments of the US Federal Trade Commission on Privacy and Security Implications of the Internet of Things. The White Paper represents the position of the Auto-ID Labs in alignment with GS1.

As the development of the Internet demonstrated, these technologies transcend political boundaries and will only deliver their true potential if policymakers are able to engage with all relevant stakeholders to identify a global framework of principles that can address societal expectations. International cooperation efforts offer convincing examples of how such principles could be developed. In the Internet space, the World Summit on Information Society organised by the UN in 2003 and 2005 and the ensuing Internet Governance Forum have not only significantly contributed to a better understanding of the opportunities and challenges of such a transformative technology but, perhaps even more significantly, have contributed to shaping innovating policy-making approaches. Recognising the complexity and interplay of the societal and economic effect of the Internet technologies, governments along with a wide variety of stakeholders have constructively engaged in dialogue both at regional and global level to identify innovative answers to emerging technical, economic and cultural issues.

On a more general policy level, established international platforms for regulatory cooperation would provide an ideal means to develop a truly global approach to the IoT. The US-FTC through the Trans-Atlantic Economic Council, the OECD, APEC, and the International Telecommunication Union, could lead international co-ordination where new standards are needed (e.g. in areas of privacy, confidentiality and usage of data etc.) as well as explore innovative approaches to new radio spectrum allocation.

We would like to express our appreciation for the thoughtful work of the Federal Trade Commission and for allowing us to participate in this dialogue. We look forward to continuing to work with other stakeholders in the important work of protecting privacy, fostering innovation and enhancing global commerce. We hope that the global perspective we bring will help lead to the global policy interoperability that both we and the Commission are seeking.

1. What do we mean by the Internet of Things

The term 'Internet of Things' (IoT) refers to a collection of technologies that enable existing Internet technologies and applications (including the World Wide Web) to interface more seamlessly with physical objects, locations, and processes happening in the real world, so that interactions in the physical world can be exchanged and used to remotely monitor operations and make them more efficient. Kevin Ashton coined the term, while director of the Auto-ID Center[1].

The Internet of Things is closely related to new technology paradigms such as pervasive computing and ubiquitous computing. A number of technologies contribute to enabling the vision of the Internet of Things. These include hardware technologies such as sensors and actuators, bar codes, radio-frequency identification (RFID) tags and readers, geolocation technologies such as GPS, as well as software technologies such as complex event processing, machine learning, machine vision technologies, data analysis, etc.

We live in a global society in which citizens and products can easily move anywhere within the world within hours. Products and electronic devices are manufactured for the global marketplace. Individual citizens, typically carrying a number of electronic devices when traveling, can reasonably expect connectivity to the Internet of Things wherever they go. This results in a strong need for global standardization to reduce region-specific barriers to adoption. These measures also aid in avoiding mistakes made in numerous other areas including lack of harmonization on radio spectrum (frequency bands and protocols) for mobile phone traffic, the lack of global standards for mains power sockets and plugs, and region-coding of DVDs. This type of regional divergence increases cost and complexity for end-users.

We must encourage open discussion and global cooperation on the standardization required for successful implementation and usage of the Internet of Things. Significant progress has been made over the last 10 years through the efforts of the global GS1 community[2] to develop freely available open standards for networked RFID, unique identification and supply chain information exchange. These standards have been supported by commercial hardware and software implementations and open source initiatives such as the Fosstrak[3] project.

[1] Auto-ID Center, an academic research program and global business initiative started at MIT in 1999. The Auto-ID Center focused its work on simple RFID tags to enhance supply chain efficiency in the fast moving consumer goods industry. The Auto-ID Center ended its work in 2003, licensing its research results to the then newly born EPCglobal (now fully integrated into GS1) for commercialization and standardization. Ongoing research was transitioned to the Auto ID Labs.

[2] GS1 is a neutral, not-for-profit, international organisation that develops global standards and solutions to improve the efficiency and visibility of supply chains across industries. It engages a global community of trading partners, industry organizations and technology providers to understand their business needs and develops global standards in response to those needs. GS1 is driven by close to two million user companies, which execute more than six billion transactions daily in 150 countries using GS1 standards. GS1 has local Member Organisations in over 110 countries. More information at www.gs1.org

[3] https://code.google.com/p/fosstrak/

Internet of Things technologies enable a much more granular view into operations in the real world. Each individual product instance can be tracked separately throughout the supply chain, allowing for access to information about its provenance, ‘from farm to fork’ for food products, from raw ingredients and components to finished product and beyond.

The essential characteristics of IoT data is that it can contain very granular, real-time, geo-located signals about activity in the real world. This highly specific information provides for the opportunity to more efficiently balance supply and demand, whether in retail (replenishment in store and also across supply chains) or better use of transport resources (demand-responsive transport, on-demand car-pooling), energy consumption within the home or workplace (e.g. through the use of smart meters). Fine-grained IoT traceability data can be used to make our supply chains more secure and to more effectively detect and eliminate counterfeit goods. IoT technology also includes network-connected sensors and remote processing of the data. This results in applications in healthcare and assisted living for the elderly, through the use of body sensors to remotely monitor vital signs, as well as intelligent medicine cabinets and other tools which ensure that patients take the correct dosage of medication at the prescribed times and conditions.

2. How can the Internet of Things be useful to society?

We live on a planet with an ever-increasing human population but with essentially finite or constrained resources, in terms of available energy, land mass for agriculture, and fresh water for drinking. IoT technology helps us to make much more intelligent use of such resources, reducing waste and environmental degradation by understanding what we could be doing better. The IoT provides not only the required information but also the ability to focus on how our own actions as individual citizens aggregate together to have a significant impact on the future well being of all life on Earth. The business rationale of the IoT can be subsumed under the term High Resolution Management (HRM). This refers to a management paradigm that consequently leverages the power of granular data analytics to increase visibility and leverage it for business excellence and consumer empowerment. The following examples illustrate the value of IoT for our society, which follow high resolution management thinking.

The IoT will help businesses to not only increase their operational efficiency (e.g. by reducing waste in supply chains due to smarter cool chain monitoring), but also to ensure that the products we consume are safe, particularly in areas such as food and pharmaceuticals. IoT technologies help in the fight against counterfeiting and adulteration of products with automated collection and checking of traceability data which can be used to detect gaps and inconsistencies in the entire lifecycle of products. This allows for quickly detecting potential counterfeit products at the point of introduction into supply chains and preventing them from distribution further downstream and reaching consumers. Another example includes the use of IoT technology for sustainability through monitoring our environment and to automatically taking effective corrective action in order to reduce risks to our health. For example, sensors can be used to monitor air quality and be linked to traffic control systems that restrict or divert traffic flows if air pollution levels exceed a safe level.

The mega trend of the IoT of continuously merging physical and digital world also affects consumers and their behavior. Smart phones are ubiquitously available and act as the medium for consumers to connect physical and digital world. This brings the IoT into a personal context and empowers the consumer to leverage its benefits. What results is a shift from traditional "big data" thinking where companies own all the data to "consumer big data" where the consumer is able to establish and drive a dialogue with his peers, social network, brands and retailers. The IoT will help consumers live healthier lives, enjoying smarter and faster decision-making to discover healthy and sustainable food product alternatives more easily, increase the standard of living by adjusting our home environment automatically to our preferences, saving energy thanks to consumption feedback of smart meters and devices, and managing our lives better with automated tracking of spending in various dimensions (e.g. CO2 footprint, spending, low calories, etc.) thanks to automated feedback and digital receipts.

3. What are the significant services and products that enable the IoT?

Together with GS1, the Auto-ID Labs research the next generation IoT. In order to follow the successful path of the classical Internet, its architecture would need to make sure that any object can be seamlessly identified across industries and domains, and that data can be exchanged in an interoperable, unambiguous and scalable manner. Today, these requirements are typically addressed with local, technology vendor-specific closed-loop schemes. Therefore, a critical factor in enabling the IoT will be the availability of global standards for identification, data capture and sharing for hardware, software, and application infrastructure.

On the hardware level, the key driver is the on-going need for miniaturization and availability of low-cost labels, tags and sensor networks with ever increasing computing power. These sensors represent the nerve endings of the IoT and enable things to act smarter than those that have not been tagged. Take, for instance, the problem of pervasive sensor design. In order for sensors to be pervasively deployed in an environment, they must be cost effective. Prices in microelectronics continue to drop every day but we are still not at the point where it is economically viable to monitor the temperature of every frozen carton in the cold chain with a conventional wireless sensor. Imagine the possibilities if this depth of monitoring became cost efficient.

On the software level, new methods for collecting, aggregating, storing, interpreting, visualizing, and sharing the massive data sets generated by sensors are the future. Smart analytics is the key to leveraging the power of sensor data for businesses and consumers to derive actionable insights in the right context. In order to enable IoT analytics, global standards for linked open data are required to distribute this information in a machine-readable and interoperable way through the Internet. Software application developers will be able to leverage Linked Data to combine data from multiple sources in order to add contextual information. For example, open mapping data can be combined with geospatial data in web pages and real-time observation data from GPS, RFID or scanned QR codes to build augmented reality applications. This will allow people to discover additional relevant information about their immediate surroundings, local businesses, local events, exhibitions etc.

Last but not least, interfaces and user-driven standards for empowering consumers to leverage the IoT in a powerful way are required. While the IoT in principle is able to manage complex systems semi or even fully autonomously, users need tools to be involved for decision-making and control via their smart phones or personal computers.

4. Leveraging Parallel Developments

As discussed above, pervasive sensing and embedded field intelligence empower us with an enhanced understanding of the world in which we live and promote safety, system efficiency and resource conservation. In order to enable a truly connected smart environment, we must leverage parallel developments in areas such as materials science, microelectronics, telecommunications and cloud computing.

Object identification technologies such as RFID and NFC lend themselves well to applications requiring truly low-cost, disposable sensing. For example, researchers at the Auto-ID Labs, GE Global Research, Georgia Tech and Intel Research have developed RFID tag-based sensors using passive UHF and HF RFID tags. Changes in light, temperature or other physical quantities are related to a change in the strength of the tag's reply to the reader, or to a shift in the frequency at which the tag responds to the reader. The changes to the RFID tag are effected using low-cost light or temperature sensitive smart materials. This highlights the use of parallel advancements in materials research. The concept of sensing makes use of tag signal information available at the RFID reader, which is normally not utilized. In doing so, we go 'beyond the ID in RFID and NFC' and enable sensing applications in addition to simple observation of EPCs or other globally unique identifiers. Furthermore, this sensing concept is a seamless extension of the GS1 Gen 2 air interface protocol.

Besides sensor design, the issue of data acquisition and visualization must be addressed as well. Pervasive WiFii or Wi-Max coverage in a city would, for example, enable sensors or readers to easily transmit sensed data to the cloud, from which monitoring authorities or the public could access them. In areas where WiFii coverage is not an option, advances in power harvesting devices and batteries could be utilized to boost sensor communication range. Use might also be made of 'data mules' to gather data from sensors outside the "read range." For example, a reader mounted on a janitor's cart would allow for the daily monitoring of short-range passive air quality sensors in all rooms of a building. Similarly, readers mounted underneath a railway engine could be used to periodically monitor concrete railroad ties for strain and cracks.

Information from sensors can also be used for monitoring perishable goods such as fresh food products, as well as public infrastructure such as bridges, tunnels etc. to look for signals that give an early warning of degradation, spoilage or the need for maintenance or intervention. However, sensor data is much more complex than simple observation data when bar codes or RFID tags are read at different locations. Not only are there a wide variety of different properties that can be sensed (e.g. light levels, humidity, concentration of gases, vibrations), it is sometimes necessary to "smooth" the data in order to extract the most meaningful interpretations. To realize the goal of effective standards for seamless identification, capture and sharing of information about physical objects and activities in the real world in an IoT, GS1 and the Auto-ID Labs are collaborating with established organizations for the classical Internet. On topics such as capture, processing, discovery and

exchange of sensor data, GS1 and the Auto-ID Labs are collaborating with organizations such as the Sensor Web Enablement architecture from the Open Geospatial Consortium and the Semantic Sensor Network activity within W3C.

5. What are the potential unique concerns associated with the IoT?

GS1 US[4] understands firsthand the difficulties in developing and introducing new technologies. Few people remember the swirl of controversy that surrounded the introduction of the now ubiquitous bar code in retail settings. Opponents of the use of bar codes warned of dire consequences for consumers and sought to prevent the use and deployment of bar codes. Today, it is difficult to imagine a world without the benefits of bar codes such as faster checkouts and the lower prices enabled by improved supply chain management.

Controversies such as those involving the introduction of bar codes in the 1970's have helped GS1 to understand the importance of broadly inclusive processes in developing appropriate policies. As an organization devoted to the development of standards that allow for global interoperability, we are convinced of the importance of requiring interoperability in the public policy domain.

GS1 has been actively engaged in the transatlantic and global dialogue on the IoT. From 2009 to 2011, GS1 was the leader of an EU funded project (GRIFS[5]) which explored the feasibility of coordinating on a global level IoT-related standardization activities. GS1 also participated in a second project aimed at raising awareness among industry and consumers about RFID technologies. Since 2010, the policy debate in the European Union Commission has broadened its scope to address a wide set of technologies, similar to RFID, that are generally referred to as the IoT. Here too, GS1 has been an active member of the "IoT Expert Group" that supported the European Commission's work to identify emerging policy issues for the period 2010-2012[6]. On a global level, GS1 was one of the founding members in 2011 of the Internet Governance Forum Dynamic Coalition on IoT[7], a multi-stakeholder forum aimed at fostering dialogue between the public and private sector on policies to promote development of the IoT.

Our submissions to IoT public consultations in areas such as privacy, security and sustainability are based on expert advice from the Auto ID Labs, while the high-profile IoT Conference[8] organized by the Labs features a policy session to foster a better understanding between the scientific and policy-makers communities.

[4] GS1 US is one of 111 country-based Member Organizations of GS1. GS1 is a global organization dedicated to the development of standards and solutions to improve the efficiency and visibility of supply chains and demand chains, both globally and across industries. More than two million companies use GS1 standards to do business across 150 countries. GS1 and its subsidiaries and partnerships connect companies with standards based solutions that are open and consensus-based. GS1 US member companies represent more than 300,000 American businesses in more than 25 industries including consumer packaged goods, grocery, apparel, government, aerospace, retail, foodservice, healthcare, fresh and packaged foods, consumer electronics and high-tech.

[5] http://www.grifs-project.eu/

[6] http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[7] http://www.intgovforum.org/cms/component/content/article/118-dynamic-coalition-proposals/1217-dynamic-coalition-on-the-internet-of-things

[8] http://www.iot-conference.org

Promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services and is therefore of primary concern to GS1 and the Auto-ID Labs. At the same time, discussion of privacy must take place in a real-world context with a focus on protecting citizens against realistic consequences rather than focusing on hypothetical harms.

We are not entirely confident that the full implications of the Internet of Things for the traditional means of protecting privacy and security have been fully appreciated. While the Internet of Things in some minds consists of RFID and other means of object identification, the more lasting impact will come from the rise of sensor networks.

Growth predictions of networked sensors anticipate billions of autonomous and semi-autonomous sensors in our environment in the foreseeable future. It is a difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors used, for example, to monitor electricity use in buildings such as hotels. The same difficulties can be seen in attempting to apply data minimization requirements to sensor networks. Also, as Paul Schwartz[9] pointed out, data minimization requirements may well be at odds with even the most ethical data analytic practices.

We believe the IoT has the potential to offer enormous benefits. To address privacy and security we need a flexible framework that can accommodate radical technological change and ever increasing complexity. The easy answer is to apply a notice-consent-access regime, yet it is difficult to imagine posting notices or providing choices in many of the use cases described above. For example, how would one provide adequate notice for every embedded sensor network? How would consent be obtained? How would one apply traditional access requirements? It may not be desirable, or even possible, to effectively implement access requirements. It is difficult to consider how data minimization or purpose specification would operate if the goal is to gather a wide range of data to analyze in an effort to find new insights for the greater good.

Rather than simply importing a notice and choice regime, perhaps there is value in going back to first principles to determine a workable privacy enhancing public policy for sensor networks. It may be that the purposes of privacy protection can be achieved by reviewing enforceable use limitations rather than simply assuming that the full range of mechanisms we have used in the past will be necessary and appropriate to each new development[10]. We believe the Internet of Things requires new thinking and flexibility to garner benefit from its capabilities while protecting personally identifiable information.

Often the tendency exists to treat all threats as if they were equally likely or equally consequential. The greater emphasis should be placed on identifying those threats that are

[9] http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf

[10] For example, Is it not sufficient to provide notice to explain which kind of sensor data is being collected, along with information about whether that data is being correlated with their individual identity or whether the data is being decoupled from their identity and aggregated with similar data before being analyzed? If we consider the temperature sensors and heating / air-conditioning controls in a hotel room, a citizen could rightly be concerned if the hotel were to publish or sell data that linked the usage data to the name, address or billing details of a specific hotel guest. However, if the hotel is simply aggregating together all of the sensor / actuator data from rooms of a particular type/size in a particular floor / wing of the hotel and is removing the data field (such as room number) from the data, so that it cannot be traced to a particular hotel guest on a particular date, there should be no privacy concern. The issue is about what information is being collected, how it could be correlated with an individual (and potentially reveal other information about the person's activities (e.g. that they stayed in a specific hotel on a specific date), how it is sanitized / de-sensitized and what is the purpose for its collection.

the most likely to occur and which are most likely to have the most damaging consequences. Resources, whether in money, or attention, are in short supply. It is no doubt necessary to be inclusive in identifying threats, but it is also important to analyze each threat's likelihood and gravity in order to employ limited resources in the best manner, thus crafting proportionate safeguards that deal with the most serious threats.

Another tendency to avoid is the potential expansion of the types of data that would fall into the category of personal data. Some have argued for a definition that would include any information that *could* be linked to an individual or an identifiable person. If the definition of personal data information is equated with any data that *could* potentially be linked, the definition would sweep in almost all data, given the technical capability that now exists. This result would dramatically increase the burden on all entities and would dilute the required focus on those threats that are most likely and the most damaging.

We believe the focus should be not only on prescriptive measures to improve compliance, but would also solicit mechanisms that provide more positive incentives for appropriate treatment of data. We already have in place strong positive incentives to treat data appropriately if we are to keep the trust and respect of customers. There are strong punitive incentives that exist with the potential for enforcement actions, but there may well be other positive incentives that would play a helpful role.

Interoperability and standards are of central importance in facilitating the development of the smart devices, objects and applications that will continue to populate the Internet of Things, and should therefore be fostered as part of the overall policy goals in support of IoT. However, adopting a regional or national perspective in addressing these issues would inevitably lead to fragmentation of the user space, stifling innovation and reducing the societal and economic benefit that may be unlocked by the IoT.

Global, voluntary and industry-driven standards are a key enabler not only for interoperability, but also for the IoT ecosystem as a whole, allowing for the growth of the IoT from various verticals to a horizontal deployment – the so-called *horizontalization*. We support open standards among IoT devices and technologies that are driven by industry experts, leveraging the effectiveness of current global standards-setting organizations that involve industry and government collaboration.