

Resolution on Internet of Things

Introduction:

In the early 1990s, the public phase of the Internet rapidly evolved the technology to connect millions of computers and thousands of computer networks. Today, anyone with Internet access can view and create web content or provide services to multiple communication terminals. The next evolution of the Internet will support generalised connectivity of objects, also known as the Internet of Things (IoT). This next phase of the Internet envisions billions of interconnected devices embedded or attached to objects that consumers use daily. The IoT can include any consumer product: electrical appliances, packaging information on food products, smart meters and clothes tags.

The IoT will have benefits for consumers, but there are also concerns in terms of privacy and data protection, information security and physical safety.¹ The IoT will reveal much more about consumers' habits, from the books they read and the medications they take to the types of transportation they use. Implementation of privacy by design will be important for the enforcement of consumer and privacy rights. In addition, the data protection principles (data collection limitations; lawful and fair collection; proportionality; finality; accuracy; transparency; right of access and rectification; confidentiality and security of processing) should be respected and implemented in the technology. Health and safety concerns must also be addressed. It is important to carefully assess the possible human and environmental impact of the IoT and to conduct research in this field.

Recommendations:

In considering the use of IoT-enabled products and services, consumers will need clear, easy to understand information about how they work; choice to decide whether and when to use them and from which providers; and strong rights to protect their privacy, security and health. The TACD is carefully assessing both the benefits of the IoT and the consumer concerns related to it and remains committed to bringing forward concrete recommendations. The TACD has already adopted several resolutions that are applicable to the IoT.

The recommendations in these resolutions should be considered by the EU and US governments and by the relevant businesses as the IoT is developed:

1. Resolution on Privacy and Security Related to Smart Meters²
2. Resolution on Internet Security³
3. Resolution on Radio-Frequency Identification⁴
4. Charter of Consumer Rights in a Digital World⁵

¹ EPIC IPv6 Comments, National Institute of Standards and Technology,

www.epic.org/privacy/internet/IPv6_comments.pdf

² http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=40

³ http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=56&Itemid=40

⁴ http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=77&Itemid=40

⁵ http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=43&Itemid=40

Background:

The Internet of Things (IoT) can be described as things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate with social, environmental and user contexts⁶.” It is no longer a futurist scenario; the IoT is already being deployed today. RFID tags used in the retail sector and wireless communication systems such as those found in home area networks, smart telecommunication devices, electronic books or smart meters are an important component of the IoT. Smart meters are being deployed by energy operators providing real time information to consumers regarding their energy consumption. Other types of advanced sensors are used in logistics to track the progress of shipment across the world and support large scale inventory management to reduce loss or theft of products in the manufacturing, transport and retail environments. Scan bar codes are widely used by the pharmaceutical industry to verify each product and can be easily replaced by RFID technology. The lower cost and miniaturisation of RFID technology is making it a very attractive option for manufacturers and retailers to manage inventories. IoT applications are being tested and others are already operational in retailing, transport logistics, tracking of cargo and security related applications⁷.

The IoT infrastructure is pervasive because it will rely on the existing wireless Internet communication technology and established consumer products. Given that objects will communicate with each other in the background without the consumer’s knowledge, the risks to privacy and protection of personal data increase significantly. The term “Internet of Things” may therefore be misleading, as it will not only link objects but also people. The IoT will not be limited to a one-to-one tracking of items and a person, but the environments where items and people exist inside as well as outside of structures.

However, the impact of the IoT on consumers and citizens may be wider than just privacy – as it will have an impact on human relationship – how people interact with one another – through objects for instance - and an impact on the perception of society, the trend being a move towards a universal surveillance society. In addition, many components in an IoT system will be used in close proximity to each other and radio devices may share frequency bands, raising concerns about the health effects of electromagnetic fields EMF exposure.

⁶ Internet of Things in 2020 Roadmap for the future, http://www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/270808_IoT_in_2020_Workshop_Report_V1-1.pdf

⁷ Communication of the European Commission on Internet of Things — An action plan for Europe COM(2009) 278 final http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf