Big Brother has a big brother: the Internet of Things

By Karlin Lillington

Published on **EuroScientist**: www.euroscientist.com

Failure to regulate access to the deluge of data brought by the Internet of things could threaten citizens' privacy

What is your watch, your television, your car saying about you? Not just as brands, that is, but as eavesdroppers capable of passing along personal, even highly sensitive information, including, potentially, your conversations? That's more than a prospect; it's a reality with the fast-developing Internet of Things (IoT). Yet, according to one study, 87% of people say they don't even know what it is — even though the IoT currently sits at the top of analyst Gartner's annual Hype Cycle chart, as the most hyped current technology.

The Internet of Things is the next evolution of the internet, connecting not just traditional web-enabled devices like computers, mobiles and tablets. But rather, it is about sensors, electronics, home appliances, vehicles, cameras, factory machines, wearable technology, smart energy meters, and even tagged livestock connected to the internet.

This is typical of new waves of technology; the capabilities are outstripping our ability to fully understand their implications, much less prepare for them, particularly in terms of regulations. The numbers are already staggering. By the end of this year, up to 25 billion physical objects will be connected to the internet. Within five years, Intel estimates, this will explode to 200 billion.

EuroScience | 1, Quai Lezay-Marnésia | F-67000 Strasbourg | France
Tel +33 3 8824 1150 | Fax +33 3 8824 7556 | office@euroscience.org | **www.euroscience.org**

As might be expected, privacy advocates have strongly voiced concerns about how such massive rivers of data can be effectively protected. And no wonder, when computing giant HP says 70% of IoT devices are vulnerable, open to hacker attacks, data breaches and surveillance.

National governments have taken note, though responses vary enormously. This raises questions about governments' global readiness for the data onslaught. A recent report published on 10th March 2015 by the UK's Chief Scientific Advisor focuses on the IoT's opportunities. But it also pays scant attention to privacy, assuming UK legislation adequately covers the issue.

Meanwhile, the US Federal Trade Commission released a report in January 2015 specifically focusing on privacy, security in the context of the IoT. And it raised numerous concerns. "Many, if not most, aspects of our everyday lives will leave a digital trail," said Federal Trade Commission chairwoman, Edith Ramirez, in a keynote speech at the annual Consumer Electronics Show in Las Vegas in January 2015. "That data trove will contain a wealth of revealing information that, when patched together, will present a deeply personal and startlingly complete picture of each of us, one that includes details about our financial circumstances, our health, our religious preferences, and our family and friends."

Europe is concerned, too — rightly so, having more connected objects than either China or the US. Some 29% of all machine-to-machine connections are in Europe, compared to 27% in China and 19% in the USA.

In recommendations issued last year, the EU's Article 29 Data Protection Working Party recognised the potential of the IoT. But it also cautioned: "Data losses, infection by malware, but also unauthorised access to personal data, intrusive use of wearable devices, or unlawful surveillance are many risks that stakeholders in the IoT must address to attract prospective end-users of their products or services." These issues are also considered in a 2013 European Commission report based on an extensive public consultation process.

No one and no country can be complacent about the privacy nightmare the IoT introduces.

Voluntary industry compliance consistently has been shown to be inadequate when it comes to protecting digital privacy. Therefore, policy makers must understand that a serious economic and societal challenge looms. There is a need to create a framework that supports innovation as well as personal privacy.

To date, no legislation exists in Europe - or elsewhere - specifically addressing the IoT. This I, in part, because some policy makers argue that the challenges it poses can be managed within existing privacy, data protection, security and corporate governance laws. However, this is wildly optimistic. The EU has already recognised that pre-Internet era data and privacy safeguards are inadequate to a post-Internet world. But current legislation and proposals hardly touch the new complexities and capabilities the IoT will introduce.

Policy makers need to be considering legislating for standards for defining the billions of objects and associated forms of data the IoT will contain, and baking in permissions that determine how data may be used and stored. Privacy safeguards must take a fresh look at the implications for profiling individuals, at drawing inferences or creating behavior patterns from aggregated data.

Corporate and government governance and liability laws must factor in not just IoT data gathering but also the way the IoT allows far greater interconnectedness between systems, machines, and devices, exponentially increasing data and cyber security risk. And, with the IoT's endless opportunities to hand over data in seemingly innocuous ways, data literacy needs to be on the schools curriculum to produce citizens that can make informed choices.

Get it right, and the benefits are great. Get it wrong, and the most deeply held principles of open, democratic societies will be under attack.

Photo credit: Anna Bardocz from Shutterstock

EuroScience | 1, Quai Lezay-Marnésia | F-67000 Strasbourg | France
Tel +33 3 8824 1150 | Fax +33 3 8824 7556 | office@euroscience.org | **www.euroscience.org**