Regulating IoT: enabling or disabling the capacity of the Internet of Things?

Irina Brass, **Leonie Tanczer**, **Madeline Carr** and **Jason Blackstock** consider privacy and security challenges

The Internet of Things (IoT) is the technology buzzword of the day. The number of network-connected devices has now exceeded the world population, and recent market research estimates that 8.4 billion connected 'things' will be in use in 2017 (Gartner, 2017). IoT technologies add an online identity to objects that have traditionally had only a physical identity – from fridges, to cars to power plants – enabling these objects to be virtually sensed, analysed and even actuated.

Governments around the world realize the socio-economic potential of IoT, and are eagerly exploring how their economies might harness the benefits from live data flows and customization across sectors as diverse as healthcare, manufacturing, infrastructure management and utilities (OECD, 2016). In 2015, the UK Government set its aspiration to become 'a world leader in the development and implementation of the Internet of Things' (Government Office for Science, 2014: 6). However, it also acknowledged that IoT raises unique challenges to data protection and the security of information systems and networks. These concerns are hardly unique to the UK. Connected 'things' are being manufactured and traded around the world. In most cases today, devices are built with extremely limited security specifications designed into their hardware or software, raising significant concerns about the security of rapidly expanding IoT networks.

Below we explore the regulatory approaches emerging in the EU and US in response to the security and privacy challenges of IoT. We find that the preference has, thus far at least, been for light touch regulation, though American and European approaches might soon diverge. Regardless, in order to effectively manage risks and enable societal and economic benefits, we argue governments like the UK need to develop new institutional coordination models that can enable a broad 'culture of security' for IoT across public and private sectors alike.

Responses to the privacy and security challenges of IoT

Limited security specifications in IoT devices signal a market failure that could require regulatory intervention. Manufacturers have limited economic incentives to include adequate security specifications in their IoT devices, as these can bring up costs and reduce the battery life of their products. In a recent example in 2016, IoT devices located around the world were used as launch platforms for DDoS attacks against two established Domain Name Servers – OVH and Dyn – resulting in a temporary interruption of their services. The devices were compromised by overriding easily guessable passwords set by their manufacturers (Imperva, 2016).

In the EU and the US, the response to such vulnerabilities has been to promote the principle of 'security by design' (EC, 2014) for manufacturers of IoT devices and, gradually, to extend this principle to 'security by default' (US Department of Homeland Security, 2016) and 'data protection by design and by default' (EU, 2016) for the wider management of data, information systems and networks.

There are, however, a number of challenges to implementing these principles. Firstly, they refer to a wide array of existing and emerging standards in cybersecurity and data protection, ranging from technical specifications for encryption at device level to cybersecurity risk management at the organizational level. Thus, at the moment, the landscape for privacy and security standards that apply to IoT is increasingly complex, and the market has so far indicated limited convergence towards a core set of standards to support these principles. Secondly, given the wide application of IoT, standards are being developed within, rather than across, sectoral verticals. Moreover, at the moment, these principles are non-binding in both the EU and the US, highlighting the 'light touch' regulatory approach to IoT that makes compliance with a responsible level of security and data protection difficult to ensure.

There are indications, though, that the regulatory pathways for IoT in the EU and the US might soon diverge. In the EU, the General Data Protection Regulation (2016/679), which will apply from 2018, makes 'data protection by design and by default' a mandatory requirement. Given that guidelines for applying these principles have not yet been formulated, it is not clear whether their ambit will be large enough to encompass the security by design challenges of IoT. If guidelines for data protection by design and by default are not formulated to encompass the principle of 'security by design,' then it might take longer for the EU to pass new legislation for an IoT certification scheme, as recently signalled by the European Commission (EurActiv, 2016).

In the US, there are indications that the regulatory approach to IoT will remain light touch. The Federal Trade Commission and the Department for Homeland Security have already promoted a number of non-binding guidelines and best practices for securing IoT, making reference to the framework standards designed by the National Institute of Standards and Technology (NIST). The NIST (2016) standards point towards a more systemic, end-to-end approach to securing IoT as part of the wider management of cybersecurity risk in critical infrastructure. The emphasis is currently on 'engineering trust' in cyber physical systems rather than developing separate rules for data protection and for the security of information systems and networks.

Pathways to governing IoT

The divergence of pathways for regulating IoT in the EU and US could

slow down the global adoption of core standards for data protection and security of IoT. In the interim, however, both approaches require governments to consider the wider institutional challenges for enabling IoT to develop in a secure and trustworthy manner. Security or data protection by design have such a large ambit that they cannot rely solely on top down measures for regulating IoT. Governments must search deeper in their policy toolbox to enable the institutional capacity of private and public entities to coordinate and respond in an adaptive manner to rapidly evolving security and privacy challenges.

Thus, governments must consider their wider 'orchestration' and 'mobilization' role in order to 'activate networks for public problem solving' (Salamon, 2002: 16–17). Such tools can rely on training programmes in data minimization and information and network security that do not target only providers of government contracts, but also small and medium size organizations who cannot easily cover the costs of implementing and upgrading cybersecurity measures to tackle the unique risks of IoT. In addition, governments can simplify information sharing mechanisms between private enterprises and government agencies concerned with the security of interconnected cyber and physical infrastructures. Governments can use positive incentives to promote the wider adoption of information assurance schemes in the private sector and, in turn, these measures can allow the insurance market to better assess exposure and model cybersecurity risks.

All these measures point to significant changes in the governance of risk and cultures of security currently in place across private and public sectors. The UK government has already indicated its preference for 'a flexible and proportionate model for regulation in domains affected by the Internet of Things', signalling a concern that strong IoT regulation could disable its capacity for growth (Government Office for Science, 2014: 10). Given its exit from the EU, the UK government might have a greater opportunity to consider alternative policy and regulatory designs to achieve its vision for IoT.

References

EurActive (2016) 'Commission plans cybersecurity rules for internet-connected machines.' www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/ Accessed 13 March 2017.

European Commission (2014) 'Opinion 8/2014 on the recent developments on the Internet of Things, 14/EN WP223.' Article 29 Data Protection Working Party. ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf Accessed 13 March 2017.

European Union (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. Accessed 13 March 2017.

Gartner (2017) 'Gartner Says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016.' www.gartner.com/newsroom/id/3598917 Accessed 13 March 2017.

Government Office for Science (2014) 'The Internet of Things: making the most of the second digital revolution.' www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf Accessed 13 March 2017.

Imperva (2016) 'Breaking down Mirai: an IoT DDoS botnet analysis.' www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html Accessed 13 March 2017.

NIST (2016) 'Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems.' nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf Accessed 13 March 2017.

OECD (2016) 'The Internet of Things: seizing the benefits and addressing the challenges.' www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En Accessed 13 March 2017.

Salamon, L. (2002) 'The new governance and the tools of public action', in L. Salamon (ed.), *The Tools of Government: a guide to the new governance.* Oxford: Oxford University Press.

US Department of Homeland Security (2016) Strategic principles for securing the Internet of Things.' www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf Accessed 13 March 2017.

Irina Brass and **Leonie Tanczer** are Postdoctoral Research Associates of the Standards, Policy and Governance team of the EPSRC-funded PETRAS IoT Research Hub. **Madeline Carr** and **Jason Blackstock** are Principal Investigators of the Standards, Policy and Governance team of the PETRAS IoT Research Hub.