COMPUTER LAW & SECURITY REVIEW ■■ (2018) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR

Sandra Wachter *

Oxford Internet Institute, University of Oxford and The Alan Turing Institute, British Library, London, United Kingdom

Keywords:
Data protection
Digital Ethics
Identity
Identification
Internet of Things
Privacy
Profiling
Discrimination
GDPR
Review

A B S T R A C T

In the Internet of Things (IoT), identification and access control technologies provide essential infrastructure to link data between a user's devices with unique identities, and provide seamless and linked up services. At the same time, profiling methods based on linked records can reveal unexpected details about users' identity and private life, which can conflict with privacy rights and lead to economic, social, and other forms of discriminatory treatment. A balance must be struck between identification and access control required for the IoT to function and user rights to privacy and identity. Striking this balance is not an easy task because of weaknesses in cybersecurity and anonymisation techniques. The EU General Data Protection Regulation (GDPR), set to come into force in May 2018, may provide essential guidance to achieve a fair balance between the interests of IoT providers and users. Through a review of academic and policy literature, this paper maps the inherent tension between privacy and identifiability in the IoT. It focuses on four challenges: (1) profiling, inference, and discrimination; (2) control and context-sensitive sharing of identity; (3) consent and uncertainty; and (4) honesty, trust, and transparency. The paper will then examine the extent to which several standards defined in the GDPR will provide meaningful protection for privacy and control over identity for users of IoT. The paper concludes that in order to minimise the privacy impact of the conflicts between data protection principles and identification in the IoT, GDPR standards urgently require further specification and implementation into the design and deployment of IoT technologies.

[1] Defining the 'Internet of Things' is not straightforward. As argued by Whitemore et al. based on a 2015 literature survey, a core concept of the IoT is that "everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to achieve some useful objective" (Andrew Whitmore, Anurag Agarwal and Li Da Xu, 'The Internet of Things—A Survey of Topics and Trends' (2015) 17 Information Systems Frontiers; New York 261, 261). While seemingly any Internet-connected object can be treated as part of the IoT, narrower definitions are also available. In logistics and supply chain management, the Internet of Things can refer simply to 'objects' embedded with RFID tags, allowing for unique identification and monitoring of object movement and consumption (Whitmore, Agarwal and Da Xu; Rolf H Weber, 'Internet of Things? New Security and Privacy Challenges' (2010) 26 Computer Law & Security Review 23). The term is also often used as a synonym for ubiquitous computing or ambient intelligent, referring to "smart devices, sensors, human beings, and any other object that is aware of its context and is able to communicate with other entities" (Farzad Khodadadi, Amir Vahid Dastjerdi and Rajkumar Buyya, 'Internet of Things: An Overview' (2017) arXiv preprint arXiv:1703.06409 <https://arxiv.org/abs/1703.06409> accessed 30 June 2017). In other words, the IoT can refer to a network of sensing objects that monitor and record aspects of their environment and the behaviours of users within it. Alongside well-established RFID tags, wireless sensor networks and Bluetooth-enabled devices have emerged as IoT sensors.

* *E-mail address:* sandra.wachter@oii.ox.ac.uk.

https://doi.org/10.1016/j.clsr.2018.02.002

Please cite this article in press as: Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.02.002

1. Introduction

Usage of the 'Internet of Things' (IoT)[1] is rapidly growing. The European Union expects major investments in areas such as smart homes, personal wellness and wearables, smart energy, smart cities, and smart mobility.[2] IoT applications are emerging across myriad sectors, for example in healthcare,[3] energy consumption and utility monitoring,[4] transportation and traffic control,[5] logistics,[6] production and supply chain management,[7] agriculture,[8] public space and environmental monitoring,[9] social interactions,[10] personalised shopping and commerce,[11] domestic automation,[12] and others. These IoT devices constantly collect vast amounts of personal data such as location data and health data (e.g. Fitbit) in order to function properly or to optimise and customise their services.

The IoT is defined by connections and linked services, tailored to the specific requirements of users. Objects and services must be connected to one another and share data about a specific user to provide networked services that are informed by more than the user's direct interaction with a particular node. Without repeated and consistent identification of users, linked up, seamless services would not be possible.

However, the pursuit of identification and personalisation of users poses a risk to privacy. Data controllers can draw inferences from these data.[13] Users can easily perceive this insight as invasive, unexpected, and unwelcome. Discriminatory treatment can also result from inferential analytics and linkage of disparate records,[14] motivating limitations on user profiling.[15] The impossibility of anonymising data[16] and weak cybersecurity standards (often owing to the limited computational power of identifying technologies such as WiFi or RFID)[17] can exacerbate privacy risks.

Together, these risks make free and well-informed consent challenging in the IoT. Privacy policies often fail to communicate clearly the risks of data processing and linkage of user records (which requires consistent user identification).[18] The EUs General Data Protection Regulation (GDPR) might improve the situation. The regulation will come into force in May 2018, and accounts for many of these risks. The GDPR creates governing principles of data processing (Articles 5 and 25) and establishes new data protection standards relevant for IoT devices. New harmonised standards relating to informed consent, notification duties, privacy by design and privacy by default, data protection impact assessment, algorithmic transparency, automated decision-making, and profiling will apply across Europe.

These standards will be undermined by the tendency of IoT devices and services to collect, share, and store large and varied types of personal data, to operate seamlessly and covertly, and to personalise functions based on prior behaviour.

This paper analyses the inherent tension between privacy and identifiability in IoT by reviewing prior discussion in academic and policy discourse. Four topics are identified which describe the nature and effects of privacy challenges arising from identity management in the IoT: (1) profiling, inference, and discrimination; (2) control and context-sensitive sharing of identity; (3) consent and uncertainty; and (4) honesty, trust, and transparency. Key issues and potential solutions to balance privacy and identifiability are analysed in the context of new requirements and protections introduced by the GDPR. The analysis suggests that new approaches to transparency and user awareness will be crucial to balance privacy and identifiability, while accounting for potential discrimination, weaknesses in security and anonymisation, and poorly informed consent. Rather than promising that privacy can always be guaranteed in the IoT, transparency, awareness, and honesty are needed about the possible risks (e.g. via notifications, or access rights). Without open communication of the risks inherent to the IoT, informed consent and informational self-determination will be hindered.

[2] European Commission, 'Commission Staff Working Document: Advancing the Internet of Things in Europe' (European Commission 2016) SWD (2016) 110 final 31 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN> accessed 8 July 2017.

[3] Khodadadi, Dastjerdi and Buyya (n 1); F Gonçalves and others, 'Security Architecture for Mobile E-Health Applications in Medication Control', *2013 21st International Conference on Software, Telecommunications and Computer Networks – (SoftCOM 2013)* (2013); Cisco, 'Securing the Internet of Things: A Proposed Framework' (2016) <http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html> accessed 6 July 2017.

[4] S Sicari and others, 'Security, Privacy and Trust in Internet of Things: The Road Ahead' (2015) 76 Computer Networks 146; Khodadadi, Dastjerdi and Buyya (n 1).

[5] Sicari and others (n 4); Khodadadi, Dastjerdi and Buyya (n 1).

[6] Sicari and others (n 4); C Yuqiang, G Jianlan and H Xuanzi, 'The Research of Internet of Things' Supporting Technologies Which Face the Logistics Industry', *2010 International Conference on Computational Intelligence and Security* (2010).

[7] Sicari and others (n 4); L Weiss Ferreira Chaves and C Decker, 'A Survey on Organic Smart Labels for the Internet-of-Things', *2010 Seventh International Conference on Networked Sensing Systems (INSS)* (2010).

[8] Khodadadi, Dastjerdi and Buyya (n 1).

[9] Sicari and others (n 4); Khodadadi, Dastjerdi and Buyya (n 1).

[10] Khodadadi, Dastjerdi and Buyya (n 1).

[11] Sicari and others (n 4).

[12] Khodadadi, Dastjerdi and Buyya (n 1).

[13] Sarah Johanna Eskens, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to This Form of Personal Data Processing, and How Should It?' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2752010 <https://papers.ssrn.com/abstract=2752010> accessed 8 July 2017.

[14] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review.

[15] Sandra Wachter, 'Privacy: Primus Inter Pares – Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2903514 <https://papers.ssrn.com/abstract=2903514> accessed 19 February 2017.

[16] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006> accessed 28 June 2017.

[17] R Roman, P Najera and J Lopez, 'Securing the Internet of Things' (2011) 44 Computer 51.

[18] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' [2013] Nw. J. Tech. & Intell. Prop. <http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nwteintp11&section=20> accessed 2 October 2014.

Please cite this article in press as: Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.02.002