Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Location privacy: The challenges of mobile service devices

*Anne S.Y. Cheung**

The University of Hong Kong, Department of Law, Hong Kong, China

Keywords:
Location privacy
Mobile services
Geo-location technology
Surreptitious surveillance
ePrivacy
Smartphones

ABSTRACT

Adding to the current debate, this article focuses on the personal data and privacy challenges posed by private industry's use of smart mobile devices that provide location-based services to users and consumers. Directly relevant to personal data protection are valid concerns about the collection, retention, use and accessibility of this kind of personal data, in relation to which a key issue is whether valid consent is ever obtained from users. While it is indisputable that geo-location technologies serve important functions, their potential use for surveillance and invasion of privacy should not be overlooked. Thus, in this study we address the question of how a legal regime can ensure the proper functionality of geo-location technologies while preventing their misuse. In doing so, we examine whether information gathered from geo-location technologies is a form of personal data, how it is related to privacy and whether current legal protection mechanisms are adequate. We argue that geo-location data are indeed a type of personal data. Not only is this kind of data related to an identified or identifiable person, it can reveal also core biographical personal data. What is needed is the strengthening of the existing law that protects personal data (including location data), and a flexible legal response that can incorporate the ever-evolving and unknown advances in technology.

1. Introduction

The pervasive use of geo-location technologies poses new challenges to personal data and privacy protection, as they enable third parties to locate and track people and objects anywhere and at any time,[1] for example in cases of emergency and rescue.[2] Although geo-location technologies have been part of our daily lives for a while, they have been confined largely to short-distance tracking and situations in which the user is fully aware that such technologies are being used, such as in the collection of tolls, the use of swipe cards on public transport, entry and exit cards to gain access to buildings and the use of Radio Frequency Identification (RFID) tags in library books or merchandise in shops.[3] However, the combination of ever-advancing technologies in geographical positioning systems (GPS), wireless-fidelity (Wi-Fi) and cellular identification has produced much more powerful location-based services

* The University of Hong Kong, Department of Law, 10/F, Cheng Yu Tung Tower, Centennial Campus, The University of Hong Kong, Pokfulam Road, Hong Kong.
E-mail address: anne.cheung@hku.hk.

[1] Anne Uteck, 'Ubiquitous Computing and Spatial Privacy' in Ian Kerr, Valerie Steeves and Carole Lucock (eds), *Lessons from the Identity Trail* (OUP, 2009) 83.

[2] Anas Aloudat, Katina Michael, Xi Chen, and Mutaz Al-Debei. 'Social Acceptance of Location-Based Mobile Government Services for Emergency Management' (2013) 30 Telematics and Informatics <http://www.sciencedirect.com/science/article/pii/S0736585313000051> accessed 30 August 2013.

[3] Karl D. Stephan, Katina Michael, M.G. Michael, Laura Jacob and Emily P. Anesta, 'Social Implications of Technology: The Past, the Present, and the Future' (2012) 100 Proceedings of the IEEE 1752. For a discussion of RFID, see Marcus R. Wigan & Roger Clarke, 'Big Data's Big Unintended Consequences' (2013) 46:6 IEEE Computer 46–53.

0267-3649/$ – see front matter
http://dx.doi.org/10.1016/j.clsr.2013.11.005

(LBS) that can cover large distances. Furthermore, these technologies are often embedded in our mobile devices, which are connected invisibly and remotely to networks. Michael and Michael point out that such overarching location tracking and monitoring across all time and space has pushed us to live in a state of 'uberveillance', in which surveillance has become constant and embedded, and individuals and objects can be automatically located and identified.[4]

In other words, while we as consumers are using these technologies much more extensively, they are in turn using us as consumers. Not only do devices such as smartphones, laptops, iPads and computer tablets disclose where we are and when and what we are doing, they also enable telecommunications companies or Internet service providers to record our activities. In revealing the unique combination of the location, time and content of our activities, they allow data about us to be sent to others for analysis and for subsequent profiling.[5] The smart mobile devices that we carry with us have in fact become tools for surveillance, yet many of us have embraced them willingly, albeit unwittingly. The potential for abuse of personal data and the threats to privacy that arise from government and commercial entities using geo-location technologies are enormous. Dobson and Fisher warn about the hazards of 'geoslavery', whereby a person's physical location is coercively or surreptitiously monitored or controlled by another.[6] Litigation and academic debate have already emerged concerning the possible violation of the constitutional right to privacy that might arise from the government's use of geo-location technologies for law enforcement without a judicial warrant.[7] In 2012, the US Supreme Court condemned the use of GPS technologies to track the movements of suspects without a warrant, and deemed the practice to be in violation of the Fourth Amendment of the Constitution.[8] Another strand of the literature covers the gross breaches of personal data privacy and autonomy that arise when consumer profiling is carried out on the pretext of better service planning and more efficient advertising and marketing.[9]

To examine the above issues, section 2 of this article defines the meaning of location data, and highlights the problems concerning the surreptitious acquisition of location data and the equally problematic issue of uninformed consent in the seemingly voluntary disclosure of location data in consumers' increasing adoption of geo-location technologies. Section 3 identifies the legal implications in the personal data protection regimes in the European Union (EU) and the US. EU law is an obvious choice in studying this topic, as it is impossible to ignore the EU's comprehensive and elaborate legal scheme of personal data protection, especially its extraterritorial effect in requiring an adequate level of protection in countries where the data are received.[10] In contrast, the choice to study the US approach may be puzzling to some, as personal data protection has been described as 'fragmented' and often depends on the type of data and the entities in control.[11] Nevertheless, Solove and Hartzog argue that the US position is worth studying because of an emerging jurisprudence based on the large number of settlement cases and decisions from the Federal Trade Commission, which has played a pivotal role in influencing the development of personal data regulations, policies and company practices.[12] Due to the globalised nature of technology companies, it is necessary to understand the US legal landscape. After identifying the loopholes in the present legal regimes regarding the protection of location data, the legal reforms proposed by the EU and the US are examined to address this issue.[13] In reviewing the challenges posed by geo-location technologies and analysing the issues in the current legal debate, we aim to

[4] M.G. Michael and Katina Michael, 'Toward a State of Überveillance' (2010) 29(2) IEEE Technology and Society Magazine, 9.

[5] For larger implications, Katina Michael and M. G. Michael, 'The Social and Behavioural Implications of Location-Based Services' (2011) 5:3–4 Journal of Location Based Services 121.

[6] Jerome E. Dobson and Peter F. Fisher, 'Geoslavery' (2003) (Spring Issue) IEEE Technology and Society Magazine 47. William A. Herbert. 'No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery' (2006) 2:2 Journal of Law and Policy for the Information Society 409.

[7] This is discussed under protection against search and seizure of the Fourth Amendment of the US Constitution and Section 8 of the Canadian Charter of Rights and Freedom. David H. Goetz, 'Locating Location Privacy' (2011) 26 Berkeley Tech. L.J. 823. Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) 9:2 Canadian Journal of Law and Technology 193. For an overview of legal inadequacies in the US, the European Union and Australia, see Katina Michael and Roger Clarke, 'Location and Tracking of 'Mobile Devices: Überveillance Stalks the Streets' [2013] 29 Computer Law & Security Review 216.

[8] US v. Jones, 565 U.S. (2012). Peter Swire, 'A Reasonableness Approach to Searches after the *Jones* GPS Tracking Case' (2012) 64 Stanford Law Review Online 57. For a general discussion, see James M. Thurmana, 'US Courts Confront GPS Surveillance: Is *Maynard* a Harbinger of Change or an Anomaly? (2011) 5 Journal of Location Based Services 201.

[9] Roger Clarke and Marcus Wigan, 'You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies' (2011) 5 Journal of Location Based Services 135.

[10] Article 25 of the Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal L 281, 23/11/1995 P. 0031–0050 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> accessed 10 September 2013. Rolf H. Weber, *Regulatory Models for the Online World* (Kluwer Law International, 2002) 156.

[11] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 15 August 2013 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913> accessed 8 September 2013.

[12] Although the study by Solove and Hartzog focuses on the decisions of the Federal Trade Commission, companies have been looking into settlement agreements and law to guide their privacy practices and policies.

[13] For the European position, see the European Commission's 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,' 25 January 2012, <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf> accessed 17 April 2013. For the US position, see the Location Privacy Act of 2011, S. 1223, 112th Congress (2011–2012) <http://www.govtrack.us/congress/bill.xpd?bill=s112-1223> accessed 17 April 2013.