COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Enabling valid informed consent for location tracking through privacy awareness of users: A process theory

Aggeliki Tsohou [a,*], *Eleni Kosta* [b]

[a] *Department of Informatics, Ionian University, Corfu, Greece*
[b] *Tilburg Institute for Law, Technology, and Society (TILT), Tilburg Law School, Tilburg, The Netherlands*

Keywords:
Mobile applications
Privacy policies
Location tracking
Privacy awareness
User perception

A B S T R A C T

People use mobile devices for an increasing variety of purposes in order to enjoy the vast possibilities; they check the local weather, road traffic, personalised local news, their personalised favourite social network, etc. At the same time, application developers and market stores deploy mobile applications that collect vast amounts of information on mobile users, such as their age, gender, location or specific phone identifiers. Numerous studies illustrate that mobile applications collect valuable information about users and use it for profiling the users for their own purposes or sell this information for commercial interests. Therefore, the topic of consent to information processing becomes increasingly more interesting for researchers, legal experts and practitioners.

In this paper, the authors examine the issue of valid informed consent for location tracking by mobile phone users. They first analyse the legal premises for informed consent that represent requirements for mobile application developers and providers who request consent. However, the ones who actually give consent are the mobile users and therefore their understanding of consent is of paramount importance. Extensive literature is missing on empirical studies examining the topic from the users' perception perspective. For that reason, the authors conduct an empirical investigation with mobile users and present their findings in the form of a process theory. The process theory reveals how users' valid informed consent for location tracking can be obtained, starting from enhancing reading the privacy policy to stimulating privacy awareness and enabling informed consent. The paper includes a discussion section in which the authors describe the implications of the process theory for the different stakeholders and offer recommendations deriving from the empirical findings. The contribution is addressed to software and mobile application developers and providers, technology regulation researchers and policy makers, as well as security and privacy researchers.

* *Corresponding author.* Department of Informatics, Ionian University, 7 Tsirigoti Square, Corfu 49100, Greece.
Email address: atsohou@ionio.gr (A. Tsohou).

http://dx.doi.org/10.1016/j.clsr.2017.03.027
0267-3649/

Please cite this article in press as: Aggeliki Tsohou, Eleni Kosta, Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.027

1. Introduction

People use mobile devices for an increasing variety of purposes in order to enjoy the vast possibilities. Users are willing to reveal their location in order to receive information they consider important. According to the 2013 report of the Pew Research Center on Location-Based Services, approximately 74% of adult smartphone owners get directions or other information based on their current location (Pew Research Center, 2013). Moreover, recent experiences from the PokemonGo game illustrate that a significant number of users are eager to reveal their location information in order to participate in popular location based augmented reality games (Appinstitute, 2016). Application developers (hereafter app developers) successfully deploy mobile applications (hereafter mobile apps) that collect vast amounts of information on smartphone users, such as their age, gender, location or specific identifiers for the users' phone. Similarly, operating system and device manufacturers collect personal data directly from the users during registration, from the device itself during its normal use and/or through the installation and use of applications. Due to the vast amount of information that devices collect about users, they can serve also as tracking devices for operating system and device manufacturers, telecommunication providers and app developers.

Numerous studies illustrate that mobile apps running on all sorts of operating systems collect valuable information in order to profile users and further that this same information is then often also sold to online advertising companies (on the use of user data for online behavioural advertising, see Hoofnagle et al., 2012; Omer and Polonetsky, 2012; Zuiderveen Borgesius, 2014). In 2010, the Wall Street Journal (The Wall Street Journal, 2010a) analysed fifty popular mobile apps through a systematic testing methodology (The Wall Street Journal, 2010b) running on both iOS and Android operating systems and reported how they collect and share user information, demonstrating an excessive collection and transmission of data to third parties. In 2015, another report was published on what types of data mobile apps are sending to third parties. The study analysed 110 of the most popular free mobile apps from the Google Play Store and the Apple App Store and examined the apps "across 9 categories likely to handle potentially sensitive data about users including job information, medical data, and location" (Zang et al., 2015). The results of the study illustrated that many mobile apps share personal information – even sensitive information – with third parties, without prior permission of the users to access and transfer the data (Zang et al., 2015).

In particular location information, especially when accumulated over time and linked with additional information from freely available online sources, can reveal much sensitive information about users and their habits: where they live and work, their hobbies, their religion, etc. (Fritsch, 2008; Gasson et al., 2001). The collection, use and further transfer of geolocation data are of high importance for users, due to the richness of information it can reveal. In a 2012 survey that examined 3.115 smartphone users on their concerns using their devices found that 62.8% of the respondents would be "very upset" when the app would share their location with advertisers (Felt et al., 2012).

The practices followed by app developers on the collection of information about users via mobile apps, the conditions and purposes of processing as well as their further transfer to third parties are often in conflict with their legal obligations. In Europe, the legal and regulatory framework on privacy and data protection sets out specific requirements that need to be complied with for the data processing to be legitimate and contains specific rules for the processing of personal data in the electronic communications sector. These requirements create a set of obligations that need to be respected by app developers in order for their activities to be legitimate. The processing of personal data in online environments, and especially in mobile communications, is usually based on user consent. Such consent can be given via ticking a box or accepting the privacy notice of a website. In reality however, users just click on the 'Next' or 'I agree' button in order to have their transaction completed as quickly as possible, while only a small number of users actually reads privacy policies. McDonald and Cranor actually argue that the time that website visitors have to invest in reading privacy policies is in itself a form of payment, which can serve as a justification as to why people are not reading long privacy policies (McDonald and Cranor 2008).

Taking into account all the above, there is an urgent need today to study how the informed and valid consent of users of mobile devices can be construed for the processing of their personal data and especially their location data. The necessity to explore this issue becomes even more crucial, when considering that current information systems (IS) research demonstrates that modern online environments constitute a new and unknown environment for which users do not seem to be prepared. Users appear to disclose their personal information in online settings without having an understanding of the relevant privacy risks and without knowing how to evaluate those risks considering the associated contexts (e.g. the available privacy features of the online applications) (Pitkanen and Tuunainen, 2012). Existing studies highlight concerns of the individuals regarding a) knowledge or even interest about the privacy risks in the online environment (Gross and Acquisti, 2005), b) awareness of the amount of personally identifiable information that they provide and who can access them (Pitkanen and Tuunainen, 2012), c) relaxed attitude towards personal privacy and misconceived evaluation of the associated privacy risks (Acquisti and Gross, 2006), and d) awareness of the privacy features of online applications and how to use them (Acquisti and Gross, 2006).

In the particular context of mobile applications, some studies have explored mobile apps users' awareness of information disclosure and their preparedness for understanding and dealing with privacy risks. (Benenson and Reinfelder, 2013; Buchenscheit et al., 2014; Rakib and Ho, 2011). According to these studies, mobile users' may be aware of certain privacy settings in the mobile apps they are using, but they are not aware of the richness of profiling information that can be inferred from the collected data. Especially for location data, Almuhimedi et al. (2014) demonstrate that mobile app users are commonly unaware of the amount of data collected by the mobile apps.

Hence, it becomes evident that there is need for more research on how practices of location-based apps providers will enable informed consent and enable mobile users' privacy awareness. In order to address this gap, in this paper the authors

Please cite this article in press as: Aggeliki Tsohou, Eleni Kosta, Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.027