Mobile Communications Privacy

D

Panagiotis Kitsos
University of Macedonia, ITLaw Team, Greece

Paraskevi Pappa
Technological Educational Institute of Epirus, Greece

INTRODUCTION

In recent years we have witnessed an unprecedented increase in the use of mobile communications as well as mobile devices such as tablets and smartphones. Consequently these developments have lead to the development of software applications, the so called "apps." The apps –offered with little cost or even for free—are used for virtually every aspect of user's life from managing the personal bank account to seeking out information, diagnosis, or even immediate treatment to health problems. However this usage might have serious implications for the privacy of their users. Besides the inherent characteristic of mobile devices as personal devices has turned them to "a spy in our pocket" (Green, N., & Sean, S. 2003). able to reveal enormous amount of personal information since a single data item can, in real time, be transmitted from the mobile device and therefore can be processed or copied between chains of third-parties such as advertisers or data analytics.

Consequently, a number of issues surrounding the ongoing regulatory and research developments on apps must be examined, such as the role and responsibilities of the different actors involved, the privacy problems arising from the emergence of apps together with the legal framework applicable to the processing of personal data in the development, distribution and usage of apps. This article will examine these issues under the light of EU data protection law as highlighted by the recent EU's Article 29 Data Protection Working Party 29 Opinion on apps on smart devices.

BACKGROUND

Mobile technology has come a long way in the last quarter of the century. In the 1980s, mobile phones could only be used for phone calls. Since then, the development of new electronic communications services led to the widespread usage of mobile phones. According to a recent survey in 2013 there were 6.8 billion total mobile subscriptions (International Telecommunications Union, 2013). A report published by ComScore highlighted that the number of smartphone users in the 5 EU countries (Spain, Germany, Italy, France and the UK) grew by 30 percent over 2012, reaching 136.2 million in the three-month average ending December 2012 (241m audience in total across all devices) (ComScore Data Mine, 2013). According to Kammala (2013) 85% of American adults own a cell phone while over half of them use their phones to access the Internet. The mobile ecosystem has changed in other ways, too. In the 1980s, the companies were just profiting from the manufacturing of mobile devices as well as the providing of cellular services.

Mobile Applications

Today mobile devices are used to access social networking sites, download and install mobile applications. It has been reported that more than 1,600 new apps are added to app stores daily (Kamala, 2013). According to ABI Research (2012) an average smartphone user downloads 37 apps. Fifty billion apps had been downloaded from App Store as of January 2013 (Statista, 2014). Apps are mobile applications for devices such as

DOI: 10.4018/978-1-4666-5888-2.ch202

smartphones, tablet computers and Internet connected televisions, available via app stores designed to "serve a wide range of purposes including web browsing, communication (e-mail, telephony and Internet messaging), entertainment (games, movies/video, music), social networking, banking and location based services" (Article 29 WP Opinion 2/2013). The complexity of apps software in addition to the fragmentation between the different parties involved in the developing of apps create a particularly privacy pervasive environment. In European Union the main legal instrument to address privacy issues with regard to apps is the Directive 95/46/EC complemented by Directive 2002/58/EC as amended by Directive 2009/136/EC, the so-called e-Privacy Directive. With the aim to clarify the legal implications of apps so as to provide useful, although non-binding, guidance to all the parties of the app ecosystem who need to comply with European Law, Article 29 Data Protection Working Party issued the Opinion 2/2013 on apps on smart devices.

Privacy in Mobile Apps

Technology has changed along with user behavior. People use the Internet through smartphones and tablets in order to "post and search for personal, often intimate, information online; communicate with friends and colleagues on social networks" (Tene, 2011) These mobile device have substituted other traditional means such as PCs, traditional telephones, photographic and video cameras. Types of data such as "text messages, numbers and the unique identifiers are stored automatically" enabling the access and process of enormous amount of personal information for example "circles of contacts, health-related or other personal research queries, along with a wide variety of intellectual and political interests, of information" (Urban, et al., 2012). Privacy advocates and researchers have addressed the privacy issues generated by app technology. There have been a number of investigations as well as studies on the risks such technology poses for the everyday user.

A few examples of these studies are outlined in this section.

- In 2011 a podcast called "This Week in Tech" revealed that popular apps could actually activate mobile phone's microphone enabling the collection of "sound patterns from inside user's home, meeting, office or wherever the user was" (Elgan, 2011).
- The French National Commission on Computing and Liberty CNIL and the IT research institute INRIA, have studied the behavior of 189 apps on six iPhone users for a period of 3 months. The results were stunning. The investigated apps were accessing users' private data and transmitting it to remote servers far more than necessary, while users were in no position to effectively monitor or control such access (INRIA, 2013).
- In 2013 the popular messaging platform "WhatsApp" has been found guilty of breaching Dutch and Canadian privacy laws. "WhatsApp" forced customers to grant it access to their entire address book which contains phone numbers of both users and non- users (Office of the Privacy Commissioner of Canada, 2013).
- It has been observed that individuals use mobile apps to monitor their health, learn about specific medical conditions or achieve personal fitness goals. A number of applications have been developed in order to "support diet and exercise programs; pregnancy trackers; behavioral and mental health coaches; symptom checkers that can link users to local health services; sleep and relaxation aids; and personal disease or chronic condition managers" (Privacy Rights Clearinghouse, 2013).

In a 2013 Financial Times article titled "Health app users have new symptom to fear" the results of a research conducted by Evidon mobile research was presented. Researchers scanned 20 of the top health, wellness, and fitness apps looking for the presence of third-party data collection technologies. The results revealed an active practice of sharing user data with third parties since among the top 20 apps, as many as 70 third parties were present, collecting data about the app users (Financial Times, 2013).

One more study conducted by Privacy Rights Clearinghouse found that many of these pose a direct threat to privacy. They evaluated 43 paid and free health and fitness apps on Google Play and Apple's App Store revealing that many of these apps lacked