Reengineering the user: Privacy concerns about personal data on smartphones

Matina Tsavli
Department of Digital Systems, University of Piraeus, Piraeus, Greece

Pavlos S. Efraimidis and **Vasilios Katos**
Department of Electrical and Computer Engineering,
Democritus University of Thrace, Xanthi, Greece, and

Lilian Mitrou
Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, Greece

Abstract

Purpose – This paper aims to discuss the privacy and security concerns that have risen from the permissions model in the Android operating system, along with two shortcomings of the permissions' model that have not been adequately addressed.
Design/methodology/approach - The impact of the applications' evolutionary increment of permission requests from both the user's and the developer's point of view, is studied, and finally, a series of remedies against the erosion of users' privacy, is proposed.
Findings - The results of this work indicate that, even though providing access to personal data of smartphone users is by definition neither problematic nor unlawful, today's smartphone operating systems do not provide an adequate level of protection for the user's personal data. However, there are several ideas that can significantly improve the situation and mitigate privacy concerns of users of smart devices.
Research limitations/implications - The proposed approach was evaluated through an examination of the Android's permission model, although issues arise in other operating systems. Our future intention is to conduct a user study to measure the user's awareness and concepts surrounding privacy concerns in order to empirically investigate the above mentioned suggestions.
Practical implications - The proposed suggestions in this paper, if adopted in practice, could significantly improve the situation and mitigate privacy concerns of users of smart devices.
Social implications - The recommendations proposed in this paper would strongly enhance the control of users over their personal data andimprove their ability to distinguish legitimate apps from malware or grayware.

Originality/value - We emphasize in two shortcomings of the permissions models of mobile operating systems which, in our view, have not been adequately addressed to date and propose an inherent way for apps and other entities of the mobile computing ecosystem to commit to responsible and transparent practices on mobile users' privacy.

Keywords

Personal data, privacy concerns, smartphone data taxonomy, user awareness, security issues

1. Motivation

As smartphone usage and capabilities grow rapidly, more complex operating systems and applications are developed that can offer a wider range of services to the users. Apart from the traditional mobile phone functionalities such as voice calls and text messaging, smartphones offer a variety of capabilities such as GPS services, email services, video recording, web-browsing and third-party apps (throughout this document we will use the term "app" as an abbreviation for mobile applications). Large volumes of users' personal data are generated and stored on the smartphones such as location traces, usage logs, contacts, photos, documents, calls and messages. Each data type serves a series of purposes ranging from the enrichment of the functionalities of the smartphone in order to improve the user experience, to the processing and storage of the data. Even when the smartphone is not actively being operated by the user, it produces personal information about the user such as location traces, date-time logs of smartphone activation or shutdown.

These data are often collected from the operating system or the apps on various occasions and for a number of needs such as to support their functionality requirements, create detailed profiles of the users, or get insight for a user's needs and behaviour. The user is asked and/or supposed to give her consent to these apps to access her personal data as dictated/required by the permissions model. Currently there is no general applicable policy model to effectively specify the terms, conditions and purposes for collection and processing of users' personal data. However, this practice is to be assessed at its compliance with the law. With regard to the respective regulations of the European Union, personal data are protected and their processing is regulated by the Data Protection Directive 96/46/EC. Data characterized as communication/traffic data (usage logs, location, duration etc.) are additionally protected by (tele)communications secrecy and rules embedded in e-privacy directive (Directive 2002/58/EC).

However, despite the fact that legal frameworks exist in many countries that specify how the personal data are supposed to be handled, there seems to be a considerable lack of transparency regarding the way permission requests are made. Questioned is also the lawfulness of these requests as well as the respective collection of data. Moreover, we diagnose a tendency of users and developers to unsubscribe from security awareness related actions. Users' fatigue of the consecutive acceptance of

more and more permission requests has been dramatically increased, as depicted in (Felt et al., 2012), where the authors describe an approach of users' attention, comprehension and behaviour as "warning fatigue" for gradually losing their privacy concerns. On the other hand, developers have to deal with the high complexity of the permissions model. In (Balebako et al., 2014) the authors conclude that developers lack awareness of privacy measures and make decisions in ad hoc manner.

On the other hand, the users are gradually becoming privacy-conscious and a number of privacy-enhancing tools for mobile users are discussed or even offered on App markets. A representative tool is TaintDroid, which examines thoroughly the personal data flows by analysing the operations of the underlying app (Enck et al., 2010). Another interesting work is (Sarma et al., 2012), where an approach to assess the risks of installing an app based on the category and the permission requests of the app is presented.

Our motivation is to reflect upon the common practices by mobile platforms and App developers and to highlight the necessity for effective protection of the user's personal data flows. More specifically, due to the diversity of the data sources and the value of personal information, we suggest a data taxonomy based on the actors that have or request access to the user's personal data.

This work is organized as follows. In Section 2 we provide a smartphone data taxonomy according to the entities that have or request access to user's private data. Section 3 discusses the data protection requirements for data collection and processing. In Section 4 we address two main permissions' shortcomings while in Section 5 we study the impact of the apps' evolutionary increment of permission requests from both the user's and the developer's view. Finally, in Section 6 we critically reflect upon the ways that personal data have been manipulated and we provide suggestions to address the current state of privacy and security issues.

2. Data taxonomy on smartphone devices

Every smartphone consists of a multitude of components and structures that (when) combined provide a series of functionalities offered to the user. These components are hardware resources, network services, informational data and application services and constitute the assets of the smartphone. These assets can be classified in four distinct categories: i) Device, ii) Connectivity, iii) Applications and iv) Data (Theoharidou et al., 2012).

The Device asset encompasses all the hardware components of the device. These are the physical device and its resources (processor, memory, storage, sensors, display, battery, camera etc.).

The Connectivity asset refers to the technologies used in order to provide mobile network connectivity services. These are the i. GSM services (Global System for Mobile communications), ii. WPAN services (Wireless Personal Area Networks), iii. WLAN (Wireless Local Area Networks) and WMAN (Wireless Metropolitan Area

Networks) services, iv. Cellular network services, and v. Near Field Communication (NFC) interface services.

The Applications assets refer to all apps that are installed on the smartphone. These apps can be preinstalled by the manufacturer or the carrier or can be third party apps that have been installed by the user.

The Data assets are all the information stored and used in a smartphone. This information can be contacts, financial data, calling history, location information, usage history, pictures etc. and can be categorized into personal, financial, business, health, authentication or connectivity data types.

The data taxonomy according to their source is (Mylonas, 2008):

- *Messaging data*: data derived from the carrier's messaging services (SMS, EMS and MMS) or instant and e-mail messages. This category includes messaging logs as the receiver, the sender, the time and date of delivery, attachments etc.

- *Device data*: all the data of the device and the operating system that are not related to third party apps (contacts, images, IMEI, Wi-Fi MAC address, device serial number etc.).

- *(U)SIM card data*: these data include specific information of the user to be uniquely identified by the telecommunication carrier, such as the IMSI (International Mobile Subscriber Identity), the MSIN (Mobile Subscriber Identification Number) and the ICCID (Integrated Circuit Card Id). The SIM card contains the mechanisms for the operating system work flow, user authentication, data encryption algorithm, and it's file system resides in persistent memory and stores data as names and phone number entries, text messages, and network service settings.

- *Application data*: all the necessary data accessible by apps and necessary for their execution. These can be configuration files, logs or temporal data.

- *Usage history data*: all the log data relating to the usage of the smartphone. These can be the call logs, the browsing history logs, the network connection history logs and the event logs of the operating system.

- *Sensor data*: all the data relating to the sensors of the smartphone. These can be location data, temperature data, direction data, vibration data etc. The most significant sensors that exist in almost every smartphone are the camera, the microphone, the GPS, the compass and the accelerometer sensors.

- *User Input data*: these data are produced from the interaction of the user with the smartphone. For example, in this category we have the keystrokes, the button presses and the user gestures. As gestures we can characterize the

drags, swipes, taps, double taps, touch-n-holds and shakes, that is all the interactions a user can make in order to complete a specific task.

These data sources can handle many sorts of information, such as personal, business, authentication, financial, health and connectivity data. According to the category of the information the underlying data sources relate to, some can be more critical than others. For example, the apps can handle all types of data, including sensitive data, such as health information.

Different parties can have access to different data on the smartphones. A list of entities that can or/and have access to user information on smartphones is presented below:

- *Mobile device*: can have access to the device data and the sensor data.

- *Operating System*: can have access to the messaging data, the device data, the application data, the usage history data, the sensors data, the user input data and some of the U(SIM) card data.

- *Applications*: the app's functionalities define which data should be accessible by the app. According to the functionalities, a certain categorization applies. These types of applications can be:

  A. Games → can access sensor data and user input data.
  B. Content and media consumption apps (music, photo & video, sound recordings, books etc.) → can access device data, sensor data and user input data.
  C. Core functionality and utility (phone tools, mapping, navigation etc.) → can access sensor data.
  D. Social networking, communication & lifestyle (VoIP, micro blogging, instant messaging, social media, shopping, news, ad networks etc.) → can access messaging data, device data, some of the (U)SIM card data, usage history data, sensor data and user input data.
  E. Business and productivity apps (mobile banking, translation, office, calendar etc.) → can access usage history data and sensor data.

  Browsing apps combine C and E type functionalities. These hybrid functionalities can apply because even if most popular operating systems have a pre-installed web-browsing app, it is possible to install third party web-browsing apps. These functionalities allow access to browsing history data, GPS sensor data and application execution data. All apps have access to the application data related to their usage, such as logs and configuration files, but cannot access the application data of other apps.

- *Mobile telecommunication carrier*: service providers collect incoming and outgoing calls and text messages, location data and data concerning the Internet usage (the frequency the email is checked, the frequency and the duration of the

internet access). They can have access to the messaging data, the (U)SIM card data, the usage history data and the sensor data.

Data Sources / Entities	Messaging Data	Device Data	(U)SIM Card Data	Application Data	Usage History Data	Sensor Data	User Input Data
Mobile Device		✓				✓	
Operating System	✓	✓	~	✓	✓	✓	✓
Application Type: *A. Games*				*		✓	✓
B. Content & media consumption		✓		*		✓	✓
C. Core functionality & utility				*		✓	
D. Social networking & communication	✓	✓	~	*	✓	✓	✓
E. Business & productivity				*	✓	✓	
Mobile T/C carrier	✓		✓		✓	✓	

Table 1: Smartphone data taxonomy based on the entities that can gain access (✓ depicts access to the specified data, ~ depicts partial access, * depicts access only to the data related to their usage)

3. Data protection requirements

Obviously, smartphones are much more than communications tools; they combine features of a cell phone along with PC-like functionalities. Smartphones host a plethora of heterogeneous data generated from various hardware or software sources thus constituting a very rich set of personal information. As ubiquitous devices they merge or even interfere with a person's everyday life and respective privacy. Tracking a smartphone user and using applications to gain information may implicate in both the informational privacy and the communication secrecy of her (Mylonas et al, 2013).

App developers seem often unaware of their legal obligations. With regard to users living in the European Union, data collection and processing has to comply primarily with the Data Protection Directive (95/46/EC) as well as the e- privacy Directive (2002/58/EC), According to the provisions of the Data Protection Directive (95/46/EC), European data protection law applies also in case that an app developer or an app store is established outside the European territory if they make use of "equipment" situated on this territory.

The Data Protection Directive (95/46/EC) defines the fair and lawful access and treatment of personal data. App developers to the extent that they are collecting and processing users' personal data are to be characterized as data controllers, i.e. the entity/person that defines the purpose and means of processing. In this capacity they are required to provide users (data subjects in the terminology of data protection law) with comprehensive and understandable information concerning their identity, the purpose of data collection as well as the (potential) recipients of data. Furthermore there must be a legal basis for data collection as defined in the Data Protection Directive: in question are either the consent of the user-data subject, the performance of a contract or the collection for achieving a purpose of the legitimate interests pursued by the controller or by the third party. Irrespective of the legal ground app developers have to comply with the core principles of data protection: a) purpose limitation and prohibition of secondary, incompatible uses, b) proportionality (adequacy, relevance and strict proportionality in relation to the purposes for which they are collected and/or further processed) and c) time limited retention of data collected.

Smartphone applications request access to users' personal data in order to provide them services but also for advertising, analytics and other secondary purposes. Many apps often collect data, including sensitive data, biometrics, location data or browsing history (Urban et al, 2012). The most serious privacy concerns stem mainly from the lack of transparency and - respectively - awareness of the fact, the extent and the types of processing an app may undertake (Data Protection Working Party, 2013).

The situation is aggravated due to the disregard app developers show for the principles of specified purpose and proportionality. Data are collected and stored for a variety of unspecified, further purposes and often they aren't adequate, relevant, and proportional in relation to app functionality. The multiplication of actors involved (app developers, app owners, operating systems manufacturers etc.), the rapidly growing use for market research and advertising, the respectively significant aggregation and wide distribution of personal data and the "lack of meaningful consent" (Data Protection Working Party, 2013) increase privacy risks. It is, indeed, highly doubtful if the actual permissions' model complies with the consent requirements.

4. Permissions' shortcomings

Popular operating systems for smart devices provide a large and heterogeneous list of permissions to handle the access of apps to the vast set of personal data. For example the Android operating system version 4.4 supports over 140 different app level permissions to control the access of apps to the resources of the smart device.

However, the permissions handling framework of modern operating systems for smart devices is far from adequate with respect to the European legislation according to personal data, as there are noteworthy shortcomings in the way the current features are implemented. App developers have to comply also with the consent requirements laid down in the e-privacy directive (art. 5 par. 3 of Directive 2002/58/EC) if they

offer services to users living in the European Economic Area (EEA), regardless of the location of the service provider. According to the law the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

Even if the law requires a free and informed consent of the user as legal ground for store information or gain access to information stored, information is often neither clear nor comprehensive. The Data Protection Working Party, consisted by representatives of European Data Protection Authorities underlines that small screen is not an excuse thereof. Moreover, consent is reduced to a "just click submit" (Giochetti, 2008) process as notice and consent scheme is actually an "all or nothing" permission (Egelman et. al, 2013) which leaves no room for users' preferences and choices.

We will focus on the Android operating system but similar issues arise in other operating systems such as iOS and Windows Mobile. We start with a brief description of representative known issues of the permissions model of Android and then focus on two particular shortcomings which in our view have not been adequately addressed to date.

In Android, when an app is installed the user is prompted to approve the permissions that the app requests. The user has no option to "negotiate" or to form the access and use options. For example, if a "compass" app requests access to read the specific sensors but also the identity and the contacts of the user, the user cannot grant access only to the permissions that are related to the functionality of the app.

Certain permissions would be much more effective if they could support a more fine-grained access control. Jeon et al., (2012) evaluate a fine-grained approach for app permissions. For example, an app that needs to connect to a specific Internet address in order to provide certain functionality should be granted only the permission to access the particular address instead of the permission to access the whole Internet.

In Wei et al., (2012), the permission evolution and usage in the Android ecosystem since its inception in 2008, is studied. A key finding is that the permission model of Android is becoming more complex and hard for users and even developers to understand. A further observation is that permissions are not becoming more fine-grained and that, in general, the whole platform is not moving towards an approach that will enhance the confidentiality and privacy of the personal data from the user's point of view.

A technical issue with a negative impact on the effectiveness of the security model is that certain permissions are grouped in a way that makes the fair agreement between users and apps hard, if not impossible, to achieve. Less sensitive data are grouped together with critical PII (Personal Identifying Information) fields. For example, an application that needs to know if the phone is currently in a call, must be granted the

"read phone state" permission. However, the same permission provides access to sensitive PII information, like the IMEI of the device, the subscriber ID, the serial number of the SIM, etc.

Even though the "read phone state" permission is one of the most critical from a privacy point of view, there is another technical issue related to this permission. For backwards compatibility reasons, any app that supports older versions of Android must request this permission because in early versions of Android this was granted by default to the apps. The app developers have no other option if they intend to support the early versions of Android.

Thus, several applications are requesting the particular permission without actually needing any of the collected personal data; a practice that infringes a fundamental principle of the European (Data Protection) Law, namely the principle of proportionality which requires only the necessary, suitable and appropriate data to be collected and/or processed, considering the purpose to be achieved, namely the service to be provided. From the users' point of view, it is not possible to distinguish if and how apps will make use of the data collected on the legal basis of this permission, which serves as a consent, and also to realize and assess if these data are necessary for make use of the application or if they serve advertising purposes for example.

Another issue is that the permissions have become too complex. For example, in (Vidas et al., 2011) the authors address the complexity of the permissions framework and propose a utility to support developers in aligning their permission requests with the needs of their apps.

Finally, we would like to emphasize two shortcomings of the permissions models of mobile operating systems which, in our view, have not been adequately addressed to date:

1. The first shortcoming is the apparent failure of the permissions model of the Android ecosystem to sufficiently support the rights of the users with respect to the protection of their personal data. Smart mobile devices carry an enormous amount of (sensitive) personal data of their owners. In the current permissions framework of Android, the app simply requests permissions without specifying the purpose of accessing the personal data and terms of using these data. Consequently, fundamental rights of the users, like the right to be informed about the purpose of the access to their personal data are simply ignored by the mobile ecosystem and the current market practices.

2. The second shortcoming is about whether the requesting app has the right to transmit the personal data outside of the smart device. Apparently, this permission is a qualitative characteristic of the terms and conditions discussed above (bullet 1), but, in our view, deserves to be discussed separately. An app requesting personal data on a smart device differs from web or client desktop applications in that the app is running on a platform

owned by the user. More precisely, when an app requests access to personal data it should be clearly stated if this information will be used only within computations on the device or if this personal information can be transferred outside the device. For example, if an app requests information about the age and the gender of the user simply to adjust the user interface to the corresponding age class, then there is no reason for the app to transmit this information anywhere outside the smart device, and consequently, the privacy of the user is not seriously threatened. If, however, the app plans to transmit these personal data anywhere outside the smart device, then this fact should be clearly stated in the request.

5. Untraining the user and the developer

The progressive erosion of privacy caused by the increasing permission requests on each and every app update may have adverse effects on the user's attitude toward security. West (2008) enumerated a series of psychological attributes involved in security depriving actions and the lack of user motivation is one of the main traits a user may exhibit. As the user may be predisposed towards not performing security enhancing actions - such as software updates in this case - it is reasonable to expect that the privacy degenerative app updates will further fuel such lack of motivation or even provide the user with an alibi not to perform updates. As a consequence, the emerging norms of the app ecosystem to request more personal data than required (by/to fulfil the purpose of the app), may result in the convergence or even the degeneration of the behaviour of privacy aware users and those who unconsciously consent in making their personal data available to third parties.

Not performing software updates is particularly problematic for smartphones that are part of a corporate network. According to the Bring Your Own Device (BYOD) trend where an employee prefers to use her personal devices (laptops or smartphones) in order to carry out work related tasks, the security risks of an organization may rise significantly. With BYOD the traditional network (firewalled) perimeter does not exist, as user devices can "freely" enter and leave the corporate network, bypassing the perimeter controls. This situation has triggered a significant amount of research on risk analysis, security policy requirements and security controls for managing BYOD insecurity. In addition, when the device is a smartphone and also an employee's property, the risk of introducing malware in the corporate environment is high, as the administrator will not have adequate control over the device.

Therefore the software app provider's appetite to collect and exploit the users' personal data may eventually reach and impact the organisation's security, if the underlying smartphone user is the employee of the organization. Furthermore, the increased complexity of the permissions may also cause similar effects to the app developer.

Furthermore, a developer herself may not fully understand the different permissions, or may not appreciate the need for requesting the minimum set of permissions - she may in fact prefer to "play it safe" by requesting more permissions in order to avoid

time consuming troubleshooting and debugging in case of software failures due to restrictive policies.

At this point we would like to note that providing access to personal data of smartphone users is by definition neither problematic nor unlawful. On the contrary, the functionalities of many apps make it mandatory for them to access sensitive personal data of the users. Moreover, one has to take into consideration that even privacy-aware users appreciate the value apps provide and not rarely concede to the commodification of their data as a price to pay in return for free applications, as free applications often request more permissions than paid applications (Pearce et al, 2012). However, any disclosure of personal data of smartphone users has to comply with the European etc. regulations for the protection of personal data and the applied practices of platform and App vendors must effectively protect the rights of the users with respect to if, why and how their personal data are used.

6. Discussion and outlook

It is highly worrisome that today's smartphone operating systems do not provide an adequate level of protection for the user's personal data and it is possible that they are consciously developed with vulnerabilities. As depicted in Table 1, sensor data are the most critical, because they can be read by any entity that has access to the smartphone device. Moreover, the entity that seems to be the most threatening is the operating system, which has access to all personal data and yet has security vulnerabilities.

As discussed earlier, several interesting ideas such as fine grained permissions and a better grouping of the permissions have been proposed in the recent literature. If applied, such ideas can significantly improve the situation and mitigate privacy concerns of users of smart devices. In this perspective we make the following additional suggestions:

- The permissions framework of mobile platforms should be adapted to comply with the requirements of the data protection framework concerning transparency towards the user, informed consent, purpose limitation, clarity and proportionality with regard to the extent and the duration of data storage. For example, when an app requests the "read phone state" permission it should at least clearly state how it will use each of the affected data items, for how long, that it will be securely stored during this period and that it will be securely deleted afterward.

- For each data requested by an app (and, in general, any applications running on the user-side), it should be clearly stated if these data will be transmitted outside the smart device (the data item as it is or results obtained from this data item) or if they will only be used inside the smart device. If the item will be sent outside the smart device, then its transfer, storage and usage should comply with the requirements specified in the Data Protection legal framework.

Both suggestions are technically feasible and would strongly enhance the control of users over their personal data without burdening the legitimate app providers. Moreover, such measures would improve the users' ability to distinguish legitimate apps from malware or grayware (apps that carry out questionable actions without sufficient user notification or approval (Sarma et al., 2012)). Even though there are some tools, such as TaintDroid mentioned earlier, that a skilled user can use to try to figure out the risks of using an app, there is no established way for apps and other entities of the mobile computing ecosystem to commit to responsible and transparent practices on mobile users' privacy. Our proposal is an inherent way of supporting this functionality into the operating system, along with the obligation of the apps to state why and how the users' personal data will be manipulated.

Another suggestion for limiting the often disproportionally rich list of permissions set by the app vendor is to leverage market attitudes and consumer behaviour that will demonstrate susceptibility on unjustified and/or extensive permission requests or lack of transparency. More specifically, a reputation system based on the evolution of permissions during version updates that is made public could allow a user to make an informed decision on the privacy respecting attitude of an app vendor. As with most community networks, their value follows Metcalfe's Law and in order for this recommendation to have impact, it requires commitment and subscription from a significant number of end users. If processing of data is proven to be an additional revenue source, privacy preserving app services could function as a competition advantage for data protection loyal developers.

Our future intention is to conduct a user study to measure the user's awareness and concepts around privacy concerns in order to empirically investigate the above mentioned suggestions.

7. References

Balebako, R., Marsh, A., Lin, J., Hong, J. and Cranor, L. F. (2014), "The Privacy and Security Behaviors of Smartphone App Developers", *Workshop on Usable Security* (USEC 2014), San Diego, CA.

Ciocchetti, C. (2008), "Just Click Submit: The Collection, Dissemination and Tagging of Personally Identifying Information", *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 10 (Spring 2008), pp. 553-642.

Data Protection Working Party, Opinion 02/2013 on apps on smart devices (2013).

Egelman, S., Felt, A. P., & Wagner, D. (2013), "Choice architecture and smartphone privacy: There's a price for that", In *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, pp. 211-236.

Enck, W., Gilbert, P., Chun, B., Cox, L.P., Jung, J., McDaniel, P. and, Sheth, A.N. (2010), "TaintDroid - An Information Flow Tracking System for Real-Time Privacy Monitoring on Smartphones", *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, pp.1-6, Vancouver, BC, Canada.

European Parliament (1995), "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 of the EC*, *23*, pp. 6.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D. (2012), "Android permissions: User attention, comprehension, and behavior", In *Proceedings of the Eighth Symposium on Usable Privacy and Security,* ACM, pp. 3.

Jeon, J., Micinski, K.K., Vaughan, J.A., Fogel, A., Reddy, N., Foster, J.S. and Millstein, T. (2012), "Dr. Android and Mr. Hide: fine-grained permissions in android applications", *In Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '12),* ACM, New York, NY, USA, pp. 3-14.

Mylonas, A. (2008), "Smartphone spying tools", *MSc Thesis, Royal Holloway*, University of London.

Mylonas, A., Meletiadis, V., Mitrou, L., & Gritzalis, D. (2013), "Smartphone sensor data as digital evidence", *Computers & Security*, *38*, pp. 51-75.

Pearce, P., Felt, A. P., Nunez, G., & Wagner, D. (2012), "Addroid: Privilege separation for applications and advertisers in android", In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ACM, pp. 71-72.

Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., and& Molloy, I. (2012), "Android permissions: a perspective combining risks and benefits", In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, ACM, New York, USA, pp. 13-22.

Theoharidou, M., Mylonas, A. and Gritzalis, D. (2012), "A risk assessment method for smartphones", *In Proc. of the 27th IFIP Information Security and Privacy Conference*, Springer (AICT 376), pp.443-456.

Urban, J., Hoofnagle, C., & Li, S. (2012), "Mobile phones and privacy", *UC Berkeley Public Law Research Paper*, (2103405).

Vidas, T., Christin, N. and Cranor, L. (2011), "Curbing android permission creep", *In Proceedings of the Web*, Vol. 2.

Wei, X., Gomez, L., Neamtiu, I., and Faloutsos, M. (2012), "Permission evolution in the android ecosystem", In *Proceedings of the 28th Annual Computer Security Applications Conference,* ACM, New York, NY, USA, pp. 31-40.

West, R. (2008), "The Psychology of Security", *Communications of the ACM*, Vol. 51, No. 4, pp. 34-41.