SMARTPHONES AND TABLETS:
CURRENT SCENARIOS AND OPERATIONAL OUTLOOK

Italian Data Protection Authority

Table of Contents

1. The Current Scenario

1.1. Smartphones and Tablets

Smartphones are portable, battery-operated devices that work as both mobile phones and data processing and transmission devices after the fashion of personal computers. Moreover, smartphones rely on sensors to enable positioning (GPS) and acquire other items of user-environment information. Table 1 below lists the hardware that is usually to be found in these devices, whilst Table 2 shows their functional features and possible usages:

Table 1 – Smartphones: Features and Basic Hardware

Transmission Components	**Sensors and Devices**
Telephone module	< 5” touch-screen
Wi-Fi	In-built speakers and mike
Bluetooth	Digital (video)camera
FM radio	Location device (GPS)
	Digital compass, other sensors
	Payment modules

Table 2 – Smartphones: Innovative Applications and New Functions of Traditional Applications

New Features
Location Applications
Voice/Face/Image Recognition
Social Networking, including disclosure of users’ geographic location (geo-tagging)
Users mostly purchase applications via the specific dedicated market (OviStore for Nokia, Apple Store for Apple, Android Market for Google, Windows Market Place for Microsoft)
Possible mix-up of data with different sources (e.g. personal mailing list vs. work contacts)

Tablets (or tablet computers) are similar to smartphones as for their hardware and software components, the main differences being
-Screen size;
-Possible lack of telephone module; and
-Intended use.

Smartphones and tablets mostly share the same technological infrastructure, i.e. they show the same hardware components and rely on the same operating systems. However, screen size is larger in tablets, which are accordingly better suited for multimedia and editorial contents (e.g. online games, on-demand movies, news/journal subscriptions, etc.) and less handy for use as phones and PIM (Personal Information Management) tools. This is why some devices do not carry telephone modules, even though SIM cards are embedded in most models to enable data connection via cell-phone technologies (GPRS and UMTS).

It should be pointed out that tablets and smartphones can be considered jointly in a data protection perspective since the relevant applications work basically in the same way. It should also be recalled that the use of these devices for making phone calls is not addressed in the analysis described below.

1.2. Mobile Apps and Markets

Mobile Apps are software applications that can be installed on smartphones and tablets to provide additional functions. They expand the functions made available by the manufacturer's operating system and can be downloaded either via an ad-hoc application under the manufacturer's brand or via the operating system installed on the smartphone. The application in question is called "market", although it is named differently by the individual operators. The main markets are currently the following:

-Android Market (Google);
-Apple Store (Apple);
-Windows MarketPlace (Microsoft);
-Nokia Ovistore (Nokia)

All markets are special smartphone applications that display a virtual shop window where one can purchase additional applications.

1.3. Smartphones vs. Conventional Systems: The Main Differences

Tablets and smartphones differ from traditional netbooks and notebooks not only because of the specific features of the respective hardware and software, but also on account of their software acquisition and distribution mechanisms – which are centralized and usually placed under the control of the device supplier, the telephone operator, the operating system manufacturer or the "market manager"; the latter, in particular, works as a broker between the software/service developer/manufacturer (who is mostly a third party) and end-users. Users actually purchase add-on software (e.g. a video game) and services (e.g. a stock performance dashboard, a weather report service, a streaming movie, a multi-player mode video game) by way of an application called "market" that is supplied by the manager and is pre-installed on the device.

As already pointed out, each market is a sort of shop window to browse the available software and services in order to expand the functions of one's own smartphone. Users have to pre-register and accept the terms of service (ToS) set forth by the market manager as contained in an ad-hoc document.

Generally speaking, one may not purchase an application via conventional channels (like via a CD for sale in a shop) or rely on mechanisms other than those made available by the specific market manager; thus, the "market" arrangement can be considered to be the most widespread as well as preferential mechanism to distribute and purchase smartphone applications. Installing applications by any means other than the given market is accordingly a residual possibility.

By the same token, any third-party developer planning to create a mobile application will have to accept the ToS laid down by the relevant market manager and may only sell its products by the agency of the latter.

It should be recalled here that the mobile apps scenario is quite lively and evolving fast, partly because the underlying technologies – such as the newly introduced smartphone sensors, the new touch-mode interface, etc. – along with their user-friendliness and the innovative distribution channels applying to the relevant services have paved the way to new, tangible business opportunities, the implementation of technological solutions and the dissemination of services and applications that are utterly unprecedented. There are currently several developers worldwide, including small-sized enterprises or even individuals without specific business ambitions, that can leverage an idea or vision to create and make available highly innovative solutions to a potentially world-wide market via the shop window provided by the market manager – with reduced investment costs. Users are in turn able to purchase those solutions quite simply and directly. However, it can be assumed that this home-made dimension will evolve in time and lead ultimately to a reduction in the number of developers, who will become more structured as well as larger entities. Indeed, it is quite likely that consumer expectations will grow and products will have accordingly to become more complex and customized in order to remain competitive; this will entail increased research and development costs.

2. The Survey

2.1. Preparation of the Survey

The DPA launched a survey in early 2011 involving the main producers of smartphone operating systems (Nokia, Microsoft, Apple, Google) to verify the mechanisms implemented by those companies in order to ensure secure use of the mobile apps developed for the respective systems.

The following items of information were in particular to be provided by the said companies:

1. What mechanisms were in place and/or what requirements were to be met (e.g. in terms of reliability or compliance with security measures) to pre-select third party developers (i.e. those not directly employed by the given company) that were authorized to sell their own applications on the company's market platforms; what conditions and procedures were in place to withdraw this authorization, if any;
2. What mechanisms were in place to assess the functions of an application and check whether the personal data collected by the developer via the said application were actually relevant to the functions in question as well as to the purposes of the processing;
3. Whether in-house policies were available to ensure compliance with personal data protection legislation and what mechanisms were in place to check that the applications already marketed were compliant with such legislation in case of complaints lodged by users.

2.2. Replies Received by the DPA

Based on the replies received from the respondents, it appears that corporate policies only share some traits.

For instance, a common feature is that a third-party developer may put up an application for marketing on the market platform of the given company only upon finalizing a registration process and accepting specific contractual clauses that are pre-determined by the company. This entails that the contractual clauses applying to developers vary considerably depending on which company they decide to turn to.

The replies, which included partly confidential information, pointed to more or less marked differences as also related to supervision, liability arrangements, and the remedies available in case of technical (malfunctioning of an application) and/or legal (mostly contractual) issues.

Additional gaps could be found also with regard to the issues that are of special interest to this DPA, i.e. the protection of users' personal data. In this connection, two opposite practices could be identified – their differences consisting in how the security of marketed applications is ensured. They can be termed "privacy by process" and "privacy by platform", respectively.

In the "privacy by process" approach, the accrediting of potential developers and the inclusion of their applications in the market are subject to stringent controls that usually take shape by way of ToS between the prospective software supplier and the market manager. Additionally, applications are controlled prior to being marketed in order to ensure that they are technically sound.

In the "privacy by platform" approach, no prior checks are performed by the market manager on the individual applications, since the protection of users' rights is committed to the soundness of the operating system platform and its functions – which should enable users to know which data will be processed by the specific application as available on the market, via ranking mechanisms that are managed directly by users. More specifically, any user visiting a market can browse, for each available application, the opinions of other users that have already implemented it as given in the form of a score and/or comments. Additionally, the smartphone software platform informs the user, when installing an application, on what functions that application is about to use and which data it may possibly access.

3. Criticalities Related to the Use of Smartphones

The widespread use of modern smartphones results into a fast-pace growth in the use of the relevant applications; the main markets can boast a portfolio by now that at times includes several thousand apps.

Users basically delegate the management of many elements of their personal and professional lives to new technologies, which resort increasingly to location information for this purpose. The data are not always stored exclusively in the device, as they are often kept in remote areas and may be accessed potentially by other users. The same smartphone may be used for the most diverse purposes: for managing a customer portfolio along with a corporate agenda and price list; sharing pictures, information and videos with one's friends or relatives; comparing supermarket prices with those of an online store; monitoring one's bank transactions; locating one's parked car; knowing whether some friends are nearby at a given time; creating wellness plans based on one's dietary habits; setting the hormonal monitoring of the menstrual cycle; and even – perhaps in the near future – for opening garage doors (as a remote control) or unlocking house doors. The gamut of possible applications is really impressive and is bound to expand further. However, using the applications in question entails processing data – including personal data as well as confidential or even sensitive data. In many cases the data are kept and stored in the device; however, mobile apps are increasingly relied upon that consist actually in web-based services – which means that the personal data are transferred and/or copied to the service provider's cloud. The mobile app developer and/or provider may be either the market manager or an independent developer. In other words, many smartphone applications are actually services provided via cloud-based systems (according to the SaaS - Software as a Service configuration) that move all or part of user-related information into a cloud.

The shift from a traditional application model to one where software is a cloud-based service impacts on both providers and consumers, whilst the cloud model is only seemingly meant to facilitate users. In fact, users often do not realize that they are using a cloud-based service – but they are perfectly aware that they can access the same data via different devices (e.g. from their smartphone and from their desktop PC) or can find all their cherished information on their newly purchased smartphones, as if by magic, without having to perform boring transfer operations from the old to the new device (e.g. to transfer one's directory).

An additional feature that is perceived to be an added value consists in the possibility to merge data sets from different sources. For instance, a smartphone using Google's Android software can retrieve Google account contacts (including email contacts) and add them to the device contacts. Furthermore, a few smartphone manufacturers allow users to add additional information to contacts by retrieving data from their Facebook accounts such as pictures and home addresses.

To sum up, the main criticalities applying to the use of new generation smartphones are as follows:

- These are pervasive devices and can be used in all areas of one's personal and professional life;
- It can be assumed that they will be used increasingly also to handle "confidential" information;
- Data outsourcing is fostered by the resulting facilitation of use;
- Facilitation of use fosters the integration of data relating to different walks of life (e.g. work contacts and Facebook friends).

3.1. Specific Risks and Threats

The above considerations are meant to highlight the main features related to the use of mobile systems that can give rise to specific risks and threats to users' personal data. They include, in particular, the following:

- -The boundary between digital identity and real identity is getting increasingly blurred and may ultimately disappear. Any user of smartphone applications can be identified rather easily via factual, non-modifiable information (e.g. phone number, IMEI code, identification data of the contacts stored in one's device, etc.);
- -Social networking is increasingly pervasive and includes a growing set of additional personal information (e.g. a user's geographic location);
- -Generally speaking, it is increasingly difficult (or downright impossible) to keep the flow of one's personal data under control because of the growing integration of IT services along with the data exchanges between applications, smartphones and services;
- -The loosening of users' control over their personal data and the merge of digital and real identities are fraught with increased risks in terms of IT security and give rise to new dangers and threats (social stalking, interception, theft of payment accounts);
- -Applications can access data and tools via mechanisms that are even more invasive than in the past (phone numbers, contacts, messages);
- -Applications can match different features of users' lives (both private and professional) in ways that are not always perspicuous, accessible, foreseeable, controllable and desirable in the users' perspective;
- -Users can be traced and profiled unwittingly and unique information items (like IMEI and phone number) are available that can be used, for instance, with a view to behavioural advertising, to enforce agreements, or to protect copyright;
- -Some manufacturers fail to timely distribute the software patches that are meant to cope with IT security flaws on account of market considerations.

The risks and threats users are exposed to when using mobile apps either unwittingly or in the absence of specific rules can be summed up further as follows:

- -There is not enough TRANSPARENCY regarding the mechanisms and purposes of data collection;
- -Data subjects do not know how and/or are unable to exercise or reaffirm their CONTROL over their data and the mechanisms used to disclose such data to third parties;
- -There are issues related to IT SECURITY.

Transparency	Control	IT Security

Table 3: The three dimensions of data protection in smartphone apps.

4. How to Enhance Safeguards for Users

This paragraph will list some operational proposals to foster users' knowledgeable handling of the tools and devices in question as well as the exercise of their rights concerning personal data processing.

A two-fold assumption should serve as the starting point:

a. Manufacturers of smartphones and similar devices, software producers and the telephone operators that market these devices under their own brand play a key role in terms of device security; accordingly, they are in charge of ensuring timely updates if new threats to IT security are detected. In this connection, it should be pointed out that the features of the operating system working on a given device may change to the extent that the telephone operator has marketed the device under its own brand or not; accordingly, such features may be somewhat "customized" as a function of the individual brand. More specifically, the software configuration of a device that is to be marketed under a specific

brand (like Telecom Italia, Vodafone, Wind, H3G, etc.) is determined, at least in part, by the individual telephone operator in order to achieve the best possible fit with the services that operator makes available to its customers. This means that two smartphones that were originally identical (at least outwardly) because their model and make were the same may actually differ significantly in terms of software configuration depending on the operator's customization; accordingly, the changes made to the software installed in a device that is marketed under a telephone operator's brand might impact on the software updates/upgrades made available by the smartphone manufacturer (e.g. Nokia, Sony Ericsson, Samsung, Lg, etc.) and thus prevent its seamless use;

b. Unlike the conventional software acquisition model for PCs, there is usually a single intermediary in the mobile apps sector that comes between the service developer/provider and the end-user. In other words, the only interface between the manifold world of developers and the equally manifold world of potential users is made up exactly of the few intermediaries that run their business and entrepreneurial activities in this specific market sector.

This prevalent scenario points to the desirability of targeted measures that should leverage the pivotal role of the said intermediaries in contractual and business terms so as to effectively impact on the widest possible number of stakeholders. This would be aimed ultimately at laying the foundations of clear-cut, effective regulation to protect users' personal data without in any way placing constraints on market competition or hampering the creative potential of leading-edge technology developers.

In this perspective, one should highlight that it is exactly intermediaries – i.e. market managers, who often also manufacture the operating systems installed on smartphones – who are vested with the ultimate deterrent power, i.e. the power to ban software produced by third-parties on the basis of contractual agreements.

A first conclusion can be drawn from the above considerations – namely, that it is indispensable to raise users' awareness of the opportunities and risks related to smartphones and mobile apps in order for them to decide knowledgeably on the processing of their data.

It is equally fundamental for users to remain in control of their data after committing – indeed, entrusting – them to another entity.

These are the considerations and objectives the Italian DPA has on its mind in deciding to tackle the challenge raised by the ever-increasing use of smartphone applications. The DPA will take tangible steps, if necessary via targeted information campaigns, to disseminate a new type of cultural awareness in which the fascinating as well as innovative opportunities provided by new technologies are taken into account alongside some especially important criticalities such as

-The risks due to users' poor familiarity with highly important issues that impact directly on them and may result into jeopardizing their personal data protection rights;

-The peculiarities related to the use of applications, in particular those by third-party developers, that collect data on users' private life (from contacts to location up to consumer habits and health/relational information);

- The possibility that the entities processing users' personal data (including sensitive data) may "publicize" them or disclose them to other specific entities for commercial or other purposes that are unrelated to data collection and – generally speaking – are not part of the users' wishes; this has to do first and foremost with the unquestionable suitability of such data for user profiling purposes;

-The possibility that, in the absence of specific rules, the data collected in this manner may be stored in the app provider's systems for longer than is necessary in order to provide the app service as such, or that the data may continue to be processed even after a user has switched off a specific application and/or device.

The dual objective of implementing transparency in the functioning of smartphone apps – with particular regard to processing of users' personal data – and providing users with mechanisms for

effective control, on the one hand, and the consideration of the supra-national scope of producers as well as of the world-wide nature of the mobile apps market, on the other hand, point to the appropriateness of taking up the challenge in a non-exclusively national context. One might envisage coordinated actions with (institutional) partners at Community level.

This would appear to be feasible especially in the light of the specific mediation role played by the manufacturers of operating systems, who are also managers of the respective markets and/or apps catalogues and can, inter alia, ban any developers that are found to be in breach of the relevant Terms of Service.

Against this backdrop, more stringent safeguards for users can be achieved by a mix of technical measures – which should be sufficiently general in nature in order not to affect market strategies, but also reasonably effective – and contractual clauses to be added to the Terms of Service used by market managers to deal with both app developers and end-users.

In a nutshell, the future has already begun.