SECURITY OF THE DIGITAL NATIVES

TECH AND LAW CENTER

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

Bruce Schneier

CONTENTS

INDEX

PREFACE

The present report represents the first phase of a project aiming at understanding university students' perception of security related to mobile devices. The following phase envisages awareness raising and training events in various universities. The project *Security of the Digital Natives* is kindly funded by Google Italy and is currently implemented by the Tech and Law Center. *Tech and Law Center* is an interdisciplinary center promoted by a multidisciplinary research group composed by members from Università degli Studi di Milano, Università degli Studi di Milano – Bicocca, Università dell' Insubria and Politecnico di Milano. The Center's projects and events address digital technologies and their interaction with law and society.

The research team is composed by: Davide Ariu, Francesca Bosco, Valeria Ferraris, Pierluigi Perri, Giovanna Spolti, Pasquale Stirparo, Giuseppe Vaciago, Stefano Zanero.

We would like to thank Gillian Cafiero for the excellent editing.

A special thanks go to Brikena Memaj.

ABSTRACT

The *Security of the Digital Natives* project sets out to study the level of awareness and perception of IT security amongst university students, paying particular attention to the world of mobile devices. The report analyses the answers given by 1012 students from over 15 Italian universities to a multiple-choice questionnaire. The analysis shows that students' perception of their knowledge is generally wrong and that they are unaware of the risks arising from their behaviour. In view of these risks, a proposal has been made to implement technical and legal measures to reduce future problems deriving from faulty or lax adoption of security measures on their mobile devices.

EXECUTIVE SUMMARY

RESEARCH AIMS

The research focuses on the awareness and perception of IT security issues in mobile devices (for the purpose of this report, namely, smartphones and tablets). The report evolves around three main areas, each of which is studied in detail: analysis of the findings, technical considerations and legal analysis. The final aim is to formulate concrete proposals for the possible future regulation of the security of mobile devices.

REPORT METHODOLOGY AND STRUCTURE

The survey was carried out by means of a questionnaire containing 60 multiple-choice questions divided into sections corresponding to different aspects: the manner in which smart phones and tablets are customarily used, the approach to Internet and all related applications, the use of passwords, the perception of risks related to security, and the general interest in and knowledge of the subject. Students involved were from different faculties (scientific and humanist) at numerous Italian universities throughout the country distributed regularly in terms of gender, age and course year.

Subsequently, using SPSS software, we proceeded to analyse the findings by means of descriptive analysis techniques and cluster analysis techniques designed to define three "typical user profiles": light users, medium users and heavy users. These profiles are considered in order to establish a relationship between the frequency with which they use devices and behaviours characterised by secure use of these devices.

Taking into consideration the survey findings, the technical analysis investigated the university students' behaviours and possible ensuing risks for the security of their mobile devices, subdividing them into three categories: the first one focused on users' basic operations such as updating software and checking application authorisations; the second one focused on practices which may represent a risk for the individual's privacy and security; finally, the third one considered those behaviours which may have negative economic repercussions on individuals, such as unauthorised transactions, stealing credit card details etc.

Lastly, the legal part verified which behaviours may constitute or play a contributory role in law violations, also given that today's university students will be tomorrow's leaders. Furthermore, adopting a policy-making approach, the main weaknesses emerging from patterns of lax behaviour with regard to IT security were clarified, in order to outline a more consistent proposal for regulating the development and use of mobile devices in the future.

FINDINGS

The research project showed that there is an erroneous perception of the level of IT security knowledge, even amongst respondents studying technical subjects. Notably, male students tend to be less cautious, whilst female students prefer to refrain from certain behaviours with which they are unfamiliar. Furthermore, when faced with a choice between usability and security, students choose the former. For example, few logout from mobile applications or pay attention to the permissions requested by these applications, and in fact students tend to use passwords that are only slightly different from one another for a range of services.

For example, one of the most popular issues is the ease of access to a service (login and logout). The exponential increase in services or applications used by students gives rise to the increasing requirement to render security "usable".

Whilst, on one hand, there is a range of faulty behaviours with regards to implementing security systems, on the other hand there is a lack of knowledge or use, by developers, of secure programming rules for mobile applications.

Lastly, the research emphasised that students are interested in gaining greater knowledge of the issue and the need for a multidisciplinary approach in order to raise awareness on truly effective IT security.

CONCLUSIONS AND POSSIBLE INTERVENTION

Intervention strategies must be integrated, with both technical and legal requirements.
In particular, from a technical standpoint, enhanced security could be achieved through greater scalability (for example by making it possible to install applications, though selecting which permission to give), simplicity of use (for example simple creation and management of passwords to guarantee secure authentication) and improved, longer lasting support for applications from producers. In this regard, the fragmentation of the mobile operating systems plays a part in making it increasingly difficult for producers to centralise updates and security.

These suggestions, which are strictly speaking technical, do need legal support that, first and foremost, lays down duties and responsibilities on the producers of mobile devices and applications. In this regard, laws to be possibly passed in the coming months ought to already contain principles to support the adoption of programming techniques that are capable of guaranteeing *security by design* and *security by default*. However, the response must not only be regulatory; it also requires action in terms of raising awareness and encouraging privacy-protecting behaviours amongst users. Universities should also implement security policies with regard to students' use of mobile devices and this could encourage secure behaviour on the part of users. It shouldn't be forgotten that today's university students will be tomorrow's leaders and lack of education in the field of IT security can only have negative repercussions on how corporate policies will be framed in future. Speaking more generally, it is essential to create and disseminate a "security culture" which, now more than ever, with the constant transfer to mobile devices of activities that were previously confined to desktop computers, has become paramount.

MAIN FINDINGS

The following main findings have emerged from the survey:

1. Students have a wrong perception of their knowledge and awareness of information security. For example, the confidence of university students in their knowledge level fell from 82% of respondents before the survey, to 66% afterwards. Moreover, 76% of computer science students considered themselves to have a good level of knowledge, but only 45% answered the technical security questions correctly.
2. Students forced to choose between usability and security mainly opt for the first choice. A relevant issue is accessibility to the service (for example, login/logout procedures). The exponential growth of services and applications is enhancing the need for highly usable security.

3. Students lack awareness, both of protection tools and risks to the “incautious” user. For example, answers related to the use of Wi-Fi, tethering, passwords and apps stress how the user does not know the different possible consequences of inappropriate use of mobile devices.
4. App developers also lack awareness. There is a general disregard towards issues related to information security. The impression is that security and privacy are perceived only as obstacles for the use of mobile devices and not as fundamental requirements for the protection of the user.
5. University students actively use mobile devices, mainly for recreational and communication purposes. Female students use mobile devices more cautiously, often because they do not know how to use the different functionalities. Male students are more inclined to experiment, often disregarding information security.

1. INTRODUCTION

Smartphones and tablets have become an essential part of our life. According to a recent report commissioned by Google, “Our mobile planet: Italy” [1], fifty per cent of Italians who own smartphones access the Internet everyday from their mobile devices. These figures are confirmed by the International Telecommunication Union (ITU) [2], which estimated in 2013 that 67.6% of the people in Europe have active mobile-broadband subscriptions. Mobile devices with Internet connection satisfy people’s desire to always be connected, and to have immediate access to all information and social networks, everywhere, all the time.

As “smart” systems continue to grow in popularity, the mobile device has evolved from being a means of verbal communication or text messaging to become a multiple purpose device. It not only holds information of its owner, but also receives data relating to the various people in that person's life. Therefore vast quantities of diverse sensitive and confidential data are stored on these devices, as well as transferred over networks. Such transfers are potentially vulnerable to unauthorized access and thus present a security risk.

In the majority of cases, these risks translate into direct criminal offences (e.g. intrusion into other people's private lives or unauthorized interceptions of correspondence); however, they may also expose the user to more intricate types of criminal activity such as ID theft, blackmail, extortion, stalking, slander and libel.

AIM OF THE STUDY

The goal of this survey is twofold: on the one hand the focus is on the awareness and knowledge of the university students trying to understand what is their perception of security compared to their actual knowledge; on the other hand we focus on outlining the threat landscape on the basis of their habits, on the way they use their mobile devices, on the type of data they store and on the operations they perform. Altogether, this analysis lets us draw the technical-cultural picture of the digital natives in Italy. Moreover the study intends also to outline the security risks (i.e. cybercrime, identity theft, phishing, attacks by virus, etc.) and propose the possible solutions of the use of digital devices by digital natives. The solutions proposed ground on the idea that there is a need to pay more attention to the security risks, but without implementing a system that could limit the freedoms of the Internet as we are used to. As a matter of fact, every system that does not care about fundamental rights - like the freedom of speech – will not be able to

implement an adequate strategy to face the online security issue. The aim of the study is therefore to highlight possible suggestions for technical operators at various levels and for policy makers for the improvement of the security of digital natives.

THE FOCUS ON UNIVERSITY STUDENTS

The student sample was selected following a careful exploration of the term "digital natives". The research team explored several issues including answers to the following: Who are the digital natives in a country like Italy? How we can define this category taking into consideration the Italian social landscape?

In literature the concept of digital natives is defined by their approach at the ICTs as "native speakers". Some of the authors specify the birth dates of the digital natives (people born between 1977 and 1997 for Tapscott [3]; people born after 1980 for Palfrey and Gasser [4]; people born before 1991 for Oblinger and Oblinger [5]), others do not (Prensky [6]). This lack of common opinion generates different categorizations such as first and second generation of digital natives (Helsperand Eynon [7]), newcomers and veterans (Hargittai and Hinnant [8]), underlining that the concept is far more complex than a matter of age. It goes beyond one single generation (Jones et al., [9]) and it is geographically specific, according to the access to the technology, and socially situated, related to the digital literacy and the commonality of use (Helpser and Eynon [7]). Moreover, most of the studies carried out on digital natives are focused on United States or on high-income countries, among high-income communities [2].
All these academic accounts confirm that there is no single definition of digital natives that defines the concept entirely. For the purposes of this study, the definition of "Digital Natives" will require an understanding of the Italian context, taking into consideration the use of mobile devices and the access to the Internet, the digital literacy and the scope of digital devices' use.

University students present a good exploratory sample because they area 'population' that has the latest generation mobile devices, is under less parental control and spends a large amount of time in public spaces such as lecture halls, libraries and public transport, where the risk of a device being lost, stolen or accessed by someone else is far higher. Moreover hypotheses on the relevance of age, gender, and education background can be investigated.

2. OVERVIEW OF THE REPORT

The report is divided into three chapters. Chapter One focuses on the analysis of the answers given by Italian university students to the questionnaire developed within the research project. Some tables will help the visualization of key facts, about the students' habits and their perception of security risks.

Chapter Two will compare the students' awareness of the security risks involved in the use of mobile devices, with their overly confident understanding?; within this comparison the focus will be on the risks posed by the gaps between the students' understandings and their level of confidence.

Chapter Three has the ambitious role of analysing the policy issues related to the security of the digital natives. Given that an *ad hoc* "mobile technology law" is still lacking, time needs to be invested in considering how current legislation can be applied in the context of mobile

technology. From the results of this survey, it is possible to envisage certain types of scenarios involving security malpractice and risks from a legal point of view; these need to be tackled by working both on technical devices' policies and policy practices.

PART 1: ANALYSIS OF THE QUESTIONNAIRES

1. METHODOLOGICAL REMARKS

The survey was carried out using a questionnaire containing 60 multiple-choice questions divided into sections related to the different aspects of the issue: practice patterns for smartphones, tablets and laptops; approach to the various networks; and for all the applications on the devices, the use of passwords, the perceptions of the security risks, and the general interest in and knowledge of the topic. Taking into consideration that this field of study is rather new, the questionnaire was drafted by a multidisciplinary team composed by jurists, technicians and sociologists. The questionnaire was tested and validated through a multidisciplinary *focus group*[1] held at Politecnico di Milano in September 2013.

The target population was university students. The administration of the questionnaire was carried out anonymously through the platform "Google Form" from September to November 2013 and it involved over fifteen Italian Universities[2]. Members of the research team presented the questionnaire to professors and students. Several professors[3] actively invited the students to fill the questionnaire. This method was chosen due to time constraints, which do not allow face-to-face interviews, but it was preferred to the e-mail questionnaire because it guarantees a higher degree of response by students.

One thousand and twelve questionnaires were collected. These presented responses from a wide range of geographic areas and degree choices (with a good mix of students from both the sciences and the humanities).

---

1 We would like to sincerely thank for the participation to the focus group: Paolo Dal Checco, Pietro Duva, Mattia Epifani, Giulia Franzoso, Davide Gabrini, Alessandro Mantelero, Brikena Memaj, Pierluigi Perri, Piero Tagliapietra.

2 The list of the Italian universities involved is the following: Politecnico di Milano, Università di Torino, Università di Cagliari, Politecnico di Torino, Università di Salerno, Università dell'Insubria, Università di Milano Bicocca, Università di Perugia, Università di Brescia, Università di Pavia, Università di Firenze, Università della Calabria, Università di Milano Statale, Università Federico II (Napoli), Università Parthenope (Napoli), Università di Bari, Iusve (Venezia). 16 questionnaires were administered in other 7 universities.

3 We would like to sincerely thank: Davide Ariu, Elena Baralis, Antonio Barili, Andrea Bondavalli, Roberta Bosisio, Michele Camerota, Laura Castelvetri, Giuseppe Cattaneo, Marcello Cinque, Luca Didaci, Stefano Federici, Nicola Frega, Giorgio Fumera, Davide Gabrini, Gianluigi Gatta, Giorgio Giacinto, Elisabetta Gola, Paolo Lollini, Alessandro Mantelero, Paolo Montuschi, Romano Oneda, Luca Ozzano, Marco Pelissero, Davide Petrini, Susanna Pozzolo, Franco Prina, Ivan Pupolizio, Serena Quattrocolo, Stefania Ravazzi, Andrea Rossetti, Stefano Russo, Claudio Sarzotti, Laura Scomparin, Giovanna Truda.

Due to the exploratory nature of the research the chosen sample was random. Universities were chosen in order to guarantee the variety of the geographical and curricula. The survey places a particular focus on students with a technical background (IT technicians and computer engineers) and with a legal background, in order to assess if the students of those subjects, which are directly linked to the issue of cyber security, show different behaviors to the others. Besides these two categories, attention has been paid also to Media and Communications students, who have a particular relation with communicating through Internet and new media. The collected data, presented in the following paragraphs, have been processed with the software of data analysis SPSS.

The following techniques were used to analyze data:

- techniques of descriptive analysis, such as the simple frequency distributions and the contingency tables with chi-square analysis used to investigate the relationship among the answers and some variable as gender, age, faculty and perceived knowledge of internet security;
- more complicated second level techniques, which allow an in-depth and a multi-varied analysis. In particular, cluster analysis[4] technique [11] was used to define three users' profiles differentiating the use frequency. The result has been obtained by considering question n.11, which foresees a list of 14 activities that everybody can do with a mobile device. Most common activities (like sending SMS or calling) and least common activities (like gambling and other activities) were deleted from the list.

The 10 activities analysed are the following:

- Sending and receiving e-mails
- Calendar/Agenda
- Photo / Video
- Online browsing
- Instant Messaging (Skype, Whatsapp, Viber, Hangout, etc.)
- Social Apps (Twitter, Facebook, G+, Instagram, Foursquare, etc.)
- Mobile banking/trading
- Cloud (Dropbox, Google drive, iCloud etc.)
- Online shopping (eBay, Groupon, ticket purchasing, etc.)
- Videogames

The statistical technique[5] helped to identify 3 well-diversified groups, each one presenting homogeneous characteristics useful to define 3 users' profiles:

- **Light users group:** the respondents who "never or seldom" engage in the activities envisaged in the list. This group represents the 38,3%.
- **Medium users group:** the respondents who "sometimes or often" engage in the

4 The cluster analysis aims at gather together the statistical units (i.e the students) on the basis of similarities of the values given to the answers. In our specific case, we took into consideration the frequency in the use of the smartphone for various activities. To learn more about cluster analysis, please, see Everitt B.S. 2011.

5 For the Two Step Cluster Analysis, please see http://pic.dhe.ibm.com/infocenter/spssstat/v20r0m0/index.jsp?topic=%2Fcom.ibm.spss.statistics.help%2Fidh_twostep_main.htm and Bacher J., Wenzig K., Vogler M. (2010), Spss Two Step Cluster-A first evaluation Available at: http://www.statisticalinnovations.com/products/twostep.pdf (Last accessed on 21.02.2014)

activities envisaged in the list. This group represents the 24%.

- **Heavy users group**: the respondents who "always" engage in the activities envisaged in the list. This group represents the 37,4 %.

The aim of these 3 profiles was to verify the relation between the frequency of use and the security behaviour.

2. ANALYSIS OF THE RESULTS

In order to proceed with the analysis of the results, it is important to start by outlining the profiles of the respondents. Of the 1012 respondents, 51 people (5% of the total) were students who declared not to have a smartphone or a tablet. Within this category, age, gender, high school and academic subjects were relatively homogeneous. It is interesting to note that even among IT students there are students who do not have a smartphone or a tablet. More than 80% of this group declared to have inadequate or just sufficient knowledge of IT security. There are no outstanding peculiarities within this category of people or within the geographical area of origin. These findings, therefore, confirm the studies (Livingstone and Helsper, [10]) that underline how in the digital society there are people who are not interested in internet and technology and it is not linked to cultural, social or economic deficits. They have other priorities and they attribute less importance, compared to others of the same age, to the use of digital devices.
The remaining 961 students have a mobile device and the following results refer to them.

I. WHO ARE THE USERS OF MOBILE DEVICES?

Smartphones and tablet users are 58% male and 42% female, in line with male higher presence in IT studies. As shown in the table below, regarding the age there is a prevalence of students between 21 and 23 years and a very regular distribution between males and females. In the users category there is a good distribution on the overall (more women between 21 and 23, more men between 23 and 29).

Age	Female	Male	Total
19-20	24,60%	22,20%	23,20%
21-23	48,60%	42,80%	45,30%
23 -29	21,60%	27,60%	25,10%
from 30 year-old onwards	5,20%	7,30%	6,50%

Table 1: Distribution of the sample by age and gender

Male and female students come from different high school backgrounds. There is a remarkable number of female students coming from secondary schools focusing on humanities and languages, while male students usually come from technical institutes, in line with the Italian national statistics.

The following table shows how male and female students are distributed between the different academic years (male students were primarily in their first year and female students in their fourth year).

Academic year	Female	Male	Total
1st	15,90	26,50%	22,10%
2nd	28,50%	28,50%	28,50%
3rd	25,30%	19,00%	21,60%
4th	14,40%	9,00%	6,50%
5th	15,90%	17,00%	16,50%

Table 2: Distribution of the sample by academic year

The survey involved various university departments. The respondents were divided as following:

- Law: 29.6%
- Computer science and engineering: 39.3%
- Communication science: 8.9%
- Other faculties, not particularly numerous, between humanities and scientific courses, without specific IT competencies: 22,2%.

The Schools of communications were selected to analyse a humanities' group but often with some technical knowledge, especially related to the use of Internet and new media.

Faculty	Female	Male	Total
Law	48,80%	15,70%	29,60%
Computer science and engineering	8,50%	61,60%	39,30%
Communication science and similar-e.g. web marketing	14,30%	5,10%	8,90%
Others-no IT	6,80%	10,60%	9,00%
Others	21,8%	7,0%	13,2%

Table 3: Distribution of the sample by subject studied.

II. THE USE OF MOBILE DEVICES

In the first part of the research we asked some preliminary questions aimed at understanding how students use their mobile devices. The first question posed to the participants of the study was how frequently they use the mobile devices to conduct some of their daily activities. Not surprisingly more than 75% their mobile phone or tablet "always or often" to make phone calls; send and receive text messages and e-mails; browse the web; and use Skype and social apps (see the following table 4). Beside the traditional activities such as making phone calls and sending text messages, most of the students stated that they use these devices to go on-line and interact with other people in the cybersphere. 70% of respondents stated that they also take photos and videos with their smartphones and tablets. The Agenda function is used "always or often" by 46,5% of the respondents. This lower popularity of the Agenda function can be explained taking into consideration the age of the sample and the fact that most of them have no working activities that require intense planning. The age and the limited disposable income also explain the minor frequency of activities such as on line shopping, mobile banking etc.

	Never	Rarely	Sometimes	Often	Always
Phone calls	2,4	4,6	14,6	32,6	45,9
SMS	2,2	5,0	10,8	26,0	56,0
E-mails	2,2	5,0	10,8	26,0	56,0
Calendar/agenda	5,9	17,3	30,3	25,5	21,0
Photo/video	0,6	7,6	21,1	42,0	28,6
Browsing	0,6	1,9	9,8	39,2	48,5
Messaging apps	4,7	2,4	7,3	22,9	62,7
Social apps	14,6	14,6	14,6	14,6	14,6
Mobile banking/trading	14,6	14,6	14,6	14,6	14,6
Cloud services	14,6	14,6	14,6	14,6	14,6
On line shopping	14,6	14,6	14,6	14,6	14,6
Video games	14,6	14,6	14,6	14,6	14,6
Gambling	14,6	14,6	14,6	14,6	14,6

Table 4: How frequently do you use your mobile devices?

As already outlined in the "Methodological Remarks" section, in order gain a deeper understanding of the data, we analysed the frequency distribution of the answers by age, gender, academic subject and by the students' self-assessment of their knowledge of security related issues. As we expected, the students over 30 were those who used the e-mail functions on their smartphones more frequently and the younger students who played more video games. However the gender analysis rendered the most interesting results. Female students resulted as those who use mobile devices most to make phone calls, send instant messages, browse Internet, make photos and videos, and use social and messaging apps. Instead, male students resulted as those who play video games and use cloud services. No statistically significant relation emerges in relation to the subject matter.

Another question posed to the students was what they save on their mobile devices. They were given different categories to choose from: Contacts, Emails, Events, Photos or Videos, and Personal Passwords.

	No	Yes
Contacts	3,5	96,5
E-mails on an application	41,3	58,7
Events and anniversaries	35,1	64,9
Photos o videos	3,3	96,7
Personal password (ATM Pin, Puk Sim, etc.)	72,3	27,7

Table 5: What do you save on your mobile devices?

Besides the contacts, almost all the students responded that they save photos or videos. Notwithstanding the fact that warnings are often issued against storing personal passwords on mobile devices, 27,7% of the respondents admitted to the practice. Most of these belonged the youngest age bracket, being aged between 19-23.

Another question asked aimed to explore the students' behaviour when updating their devices. More than 80% of the respondents claimed they update their devices as soon as the updates are

available. This is an interesting result. It shows that the students comply with a general security practice and they understand, on some level, the importance of updates.

A key concept, which recurs during the whole project, is that of usability: students positively react to tools and features that are easy to learn and to use, whilst complexity brings an uncaring attitude.

As the following tables show, the respondents appeared to pay more attention to updating mobile devices than their laptop.

	%
Yes, I install apps and operative system's updates when they are available	81,3
Yes, but I install only the apps' updates	8,8
No	6,8
Yes, but I install only the operative system's updates	3,1

Table 6: Do you regularly update your mobile device

When the updates are available and they do not require specific searches and manual checks, they are immediately installed.

	%
Yes, I install programs and operative system's updates when they are available	75,3
No	14,5
Yes, but I install only the programs' updates	5,1
Yes, but I install only the operative system's updates	5,2

Table 7: Do you regularly update your laptop

III. THE USE OF INTERNET SERVICES

The second group of questions was aimed at understanding the students' behaviour when they use Internet services. The following table shows how the data collected revealed extensive use of free Wi-Fi networks with only 20% of the respondents saying that they do not use free Wi-Fi. Almost half of those who admitted to using free Wi-Fi said they do not use it for activities that require passwords. This demonstrates a certain degree of concern and awareness of the possible risks. Students have a similar behaviour in connecting their laptop with a free Wi-Fi (table 9).

The majority of the students (41,8%) is not adequately aware of the risks of a free Wi-Fi.

We can deduce from the table below that the majority of the students (41,8%) is not adequately aware of the risks of a free Wi-Fi.

	%
You connect and use all the applications	41,8
You connect but you only use some activities that do not require log in credentials (pin, password…)	37,7
You do not connect	20,5

Table 8: If you find a free Wi-Fi what do you do with your mobile device?

	%
You connect and freely use Internet, with no limitations	43,6
You connect but you only use some activities that do not require log in credentials (pin, password…)	33,4
You do not connect	23,0

Table 9: If you find a free Wi-Fi what do you do with your laptop?

Interestingly Wi-Fi is largely used by students irrespective of gender, age or subjects of study. Heavy users are those who use more Wi-Fi with no limits (49,3% vs. 36,7% of the light users). 28,3% of the light users do not connect when they find a free Wi-Fi.

Tethering is a less common practice than Wi-Fi use. Almost half of the respondents (44,5%) do not use one device to connect another one. This percentage reaches the 59.5% among the light users. Those tether often prefer Wi-Fi. A small minority is still cautious or not familiar with Wi-Fi and Bluetooth and will only use USB cable (5.8%). Very few were found to exclusively use Bluetooth (1,7%).

	%
Do not use the mobile phone for tethering	44,5
Wi-Fi	42,1
Wi-Fi and Bluetooth	5,8
Only USB cable	5,8
Bluetooth	1,7

Table 10: What do you use for tethering?

Among those who use Wi-Fi or Bluetooth for tethering, 87,3% had password-protected access. There are no significant differences among heavy, medium or light users. This shows a rather cautious habit and would suggest a form of security awareness but it is worth underlying that most of the devices has a default password. As the paragraph VI will explore in more details,

when there are default settings that introduce some degree of security, students seemed to adapt to them.

	%
You set tethering connection with password	87,3
You set tethering connection without password	12,7

Table 11: Do you use Wi-Fi or Bluetooth for tethering?

With relation to gender, this set of questions shows that tethering is more common practice among male students. In fact, 54% of the female students do not use mobile devices for tethering. Also the use of free Wi-Fi is less common among female students (34% vs. 48% among male students). However, when they use it tend to be less cautious than male students and less aware of the risk: as a matter of fact they tend to use more free Wi-Fi for any kind of activities (44% female students against 40% male ones) and tend make less use of passwords (almost 20% of female students use Wi-Fi or Bluetooth without password against 9% of male students).

IV. THE USE OF APPLICATIONS

The third set of questions aimed to understand if, and how, students use apps. 97,2% of those interviewed responded that they use apps, with no significant difference among heavy, medium or light users. As the table below shows, a small minority (10,6%) claimed to have installed more than 50 apps. This percentage increases up to 18% among heavy users. This minority is mainly composed of male students, those who study IT and those who claim to have a good or excellent knowledge of information security. None of those who declared to have no knowledge of information security resulted as having more than 50 apps.

	%
Less than 20	49,8
From 20 to 50	39,6
More than 50	10,6

Table 12: How many apps do you have installed on your mobile device

Not surprisingly 83,1% of the students downloaded applications from official stores. Male students, computer sciences and engineering students and students that declare to have a good or excellent knowledge of information security were those who downloaded apps from alternative sources.

	%
Official stores	83,1
Other sources	16,9

Table 13: From where do you download the apps

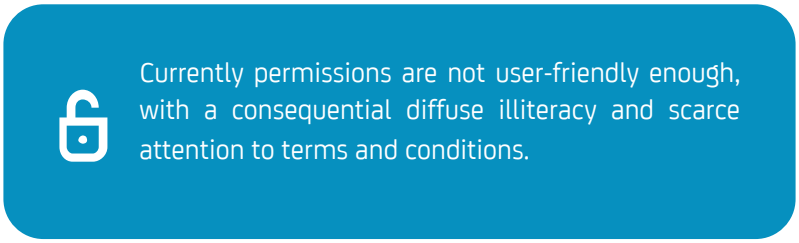
Log-out is one of the most relevant issues about applications. The majority of the students (40,2%, 46% among the heavy users) save the credentials to stay logged in. Almost 25% of the respondents log out but about 20% do not log out because they forget to do it. A minority does

not understand the importance of logging out or claimed to know how to do it. The students that declared to have an excellent knowledge of information security knew how to log out. However, some of them did not regard logging out as important or they admitted that they forget to do it. The gender analysis was also significant. Female students were generally those who seemed incapable of logging out and tended to forget. Male respondents were generally those who expressed a preference for staying logged in. Almost the same percentage of male and female log out.

	%
Save credentials to stay logged in	40,3
Log out	24,1
Do not log out because you forget it	19,6
Do not log out because you think it is not important	10,3
Do not log out because you do not know how to do it	5,6

Table 14: As soon as you have finished using an app, you...

The last question on the survey aimed at understanding if, and how frequently, students check the permissions that the application requires before completing the installation.
More than 50% of the respondents - no matter if light or heavy users - never or rarely control the permissions.



Older students and those with a higher knowledge of information security tend to control them more frequently. More than in the previous questions expertise and technical competence seem highly relevant.

	%
Rarely	38,2
Often	25,5
Always	20,7
Never	15,6

Table 15: How frequently do you check the permissions (access rights) that the application requires before completing the installation?

V. THE SELLING AND STEALING OF MOBILE DEVICES (D13 –D16)

Regarding the cases in which students might sell or give away their devices, 20% of the respondents said they had sold or given away their mobile devices. As the following table shows, not all the students demonstrated awareness as to the importance of erasing their personal information from the mobile devices prior to an exchange. The highest percentage cancelled only their contacts and their photos or videos.

	No (%)	Yes (%)
Delete the contacts	7,9	92,1
Delete the calendar appointments	12,8	87,2
Delete photos and videos	7,4	92,6
Delete the downloaded applications	13,7	86,3
Use a secure data deletion software or the built-in operating system functionality	17,3	82,7

Table 16: What do you do before selling or giving away your mobile device?

9,6% of the respondents reported they lost the mobile devices or they were stolen. It is worth noticing that more than ⅓ did not report the fact to the competent authorities.

	%
Yes	68,5
No	31,5

Table 17: Have you reported the loss or the theft to the competent authorities?

VI. THE KNOWLEDGE AND THE FEAR OF RISKS (D31 – D33)

The questions in this section were aimed at understanding the students' knowledge and fears of risks related to the use of mobile devices and laptops.

With regards to security-awareness female students demonstrated significantly less knowledge about the issue: the mean of the answers given by them is 4,97 for mobile devices (5,15 for laptops), with male students that reach a mean of 6.51 for mobile devices (7,23 for laptops). Beside gender, the other variable that correlates significantly with the level of knowledge is the degree subject. Computer engineers and scientists declared the highest scores. In general the mean level of security awareness resulted as 5,86 for mobile devices and 6,35 for laptops.

	Mobile devices (%)	Laptops (%)
1	2,5	3,6
2	4,7	2,4
3	5,5	5,6
4	10,8	9,4
5	15,1	11,2
6	20,8	16,2
7	19,6	16,5
8	14,2	18,6
9	4,8	10,4
10	2,1	6,2

Table 18: On a scale from 1 (none) to 10 (excellent), how do you assess your knowledge of issues and risks connected with the use of your laptop and you mobile device?

The majority of the students (61%) was not or was only slightly worried about the security of mobile devices, with no significant differences among light, medium or heavy users. On the contrary, they were very worried about the security of their laptops.

	Mobile devices (%)	Laptops (%)
No worried	8,0	8,9
A bit worried	53,0	38,7
Enough worried	33,4	40,8
Much worried	5,6	11,6

Table 19: How worried are you about the security of your mobile devices and your laptops?

However the question "How secure do you feel when doing the following activities with your mobile devices?" portrayed a more varied picture. The vast majority of students expressed not feeling safe when gambling, while on-line shopping and when mobile banking. Moreover the respondents said that they felt only marginally safe when browsing the Internet, using messaging apps, engaging social apps and accessing clouds services.

	Nothing	A bit	Enough	Much
Phone calls	5,9	12	45,1	37
Text Messages	5,1	14,2	46,2	34,5
E-mails	5,8	20,6	55	18,5
Calendar/agenda	6,6	8,8	40	44,6
Photo/video	5,2	14,6	47,2	33
Browsing	7,9	34	46	12,1
Messaging apps	8,5	26,8	48,4	16,2
Social apps	13	33,6	41,1	12,3
Mobile banking trading	41,7	31,5	18,8	7,9
Cloud services	15	32	41,3	11,7
Online shopping	31,8	35,4	27,1	5,7
Video games	12,9	19,6	41,9	25,6
Gambling	64,8	17,4	11,6	6,2

Table 20: How secure do you feel when doing these activities with your mobile devices

VII. ON THE USE AND MANAGEMENT OF PASSWORDS (D37 –D41) AND THE USE OF BLUETOOTH (D26)

Passwords (and passphrases) are the most widely used solution to prevent unauthorized access to data. For this reason one set of questions was on the use of passwords. Overall, the results suggested that if the password was a default setting and easy to use, the students were eager to use it.

More specifically, a small minority of the students (6,3% that increase up to 11,1% among light users) expressed that they do not use apps that require passwords; 41% (47% among heavy users) of them said they use small variations of the same password and almost 31% (only 26,7% among heavy users) claimed that they always use different passwords. A remaining 20% of the respondents admitted using the same password for all the apps. Given the difficulty in changing password, it is an encouraging result that the majority of the students do not use the same password for everything.

	%
I do not use apps which require passwords	6,3
I use slight variation of the same password for the different apps	41,3
I always use different passwords	31,7
I always use the same password/s for all the applications	20,6

Table 21: Do you use for the apps that require passwords? If so, what passwords do you use?

The vast majority (87%) use a password of eight characters, with no significant differences among light, medium or heavy users. In our opinion this is due to the fact that many websites and apps enforce the use of passwords that are at least eight characters long. Consequently, most of the students become accustomed to this kind of passwords. Here, we return to the concept of usability since an obliged path is forcing a kind of security compliance.

	%
Long password (at least 8 characters)	87,0
Short password (less than 8 characters)	13,0

Table 22: How do you characterize your password out of the following options?

Again here the default settings seemed to influence the large use of alphanumeric passwords. In general, alphanumeric passwords look safer, even if this is not always the case. However, what it is worth underlining is the common use of passwords with references to personal details and meaningful words. This suggests that students understand the importance of passwords but do not fully grasp the concept of a "safe password".

	No	Yes
You use passwords containing personal information (e.g. name and surname, birth date, favourite football team)	63,5	36,5
Your passwords contain simple letter characters	91,3	8,7
Your passwords are meaningful words	55,0	45,0
Your passwords contain numbers and special characters	25,4	74,6
When the system allows it, you do not insert any password and just click "enter"	93,8	6,2

Table 23: Which type of password are you most likely to use out of the following?

The easiness and the numerous apps and websites that give this possibility are probably behind the success of "Connect with Facebook" and "Connect with Google". These are the only means of authentication commonly used. A small minority uses OAuth and two-factors authentication. This suggests that easiness is a more relevant aspect than security.

	%
Connect with Facebook	39,9
Connect with Google	14,6
None	40,0
Two factors authentication	4,8
OAuth	0,8

Table 24: Which of these options do you use to authenticate you access to websites?

As it has been already underlined, passwords are perceived as useful and the table below confirms it. However, a significant number of students highlight that remembering several passwords is not easy. Automated solution for managing passwords (various solutions are already available on the market, like KeePass, 1Password, LastPass) could be an interesting tool for students, together with other systems of authentication that guarantee an adequate level of security (for similar results and conclusions Knott C. L. and Steube G., [12]).

	Nothing	A bit	Enough	Much
It is difficult to remember passwords	25,0	38,7	30,9	5,4
Without password it is easier	43,3	21,5	20,7	14,5
The password is useless	85,2	7,8	1,9	5,1
It is difficult to remember different passwords	13,6	25,7	39,4	21,2

Table 25: How much do you agree with the following statements?

VIII. THE TECHNOLOGIES TO PROTECT MOBILE DEVICES (D 34 –D36)

This smaller set of questions investigates the use by university students of technologies to protect the access to the mobile devices. 40% of the students do not protect the access to their phones. It is worth highlighting that during the survey, Apple released iOS7 that makes the Pin a default setting. This could be a reason why students that protect the access to their phones mainly use Pin or pattern lock.

	%
No	40,1
Yes, biometrics (voice recognition, etc.)	0,6
Yes, password/passphrase	6,6
Yes, pattern lock	23,9
Yes, PIN number	28,8

Table 26: Do you use some of the following solutions to protect access to your mobile devices?

The reasons behind this choice revealed that the students know these systems of protection but they do not use them. Respondents claimed that these systems render the use of mobile devices more inconvenient (52,5%). The data by age shows that older students are less sensitive do the inconvenience of these systems. A minority (27,7%) said that they are not interested in using them. An even smaller minority claimed that they never thought about using them.

These answers underline the need to enhance the students' awareness and of better informing them of the advantages that these systems render in terms of security.

	%
You know them but you never thought about using them	13,6
You know them but you are not interested in using them	27,7
You know them but they make uncomfortable to use the device	52,5
You do not know them	6,3

Table 27: If you have answered that you do not use any of the systems above, why is this the case?

Not surprisingly the question of the use of technical solutions to protecting the data in mobile devices revealed that the students lack knowledge on the subject. 20% of the students do not know what these solutions are and another 20% do not use them. Among the systems that were used, the most common ones were Find My Phone (20,3% of the answers) and Backup (27,7% of the answers). It is worth noticing that being a student of computer engineering or science did not make a significant difference in the use of these systems.

	%
Lock wipe	4,0%
Remote wipe	9,0%
Find my phone	20,3%
Backup	27,7%
Encryption	4,0%
Personal firewall	5,2%
VPN	3,5%
None	12,5%
I do not know what they are	12,5%
Other	1,3%

Table 28: Do you use one of these protection tools?

One question aims to understand if the access to the laptop screen was protected by a password or not. Only 57.5% of the students use a password to protect the screen. This could be related to a number of reasons: students think that the places where they use their laptop is safe (e.g. university library; home); they do not know or are not aware of the risks. For the purpose of this study it is worth noticing that students are more concerned about the security of their mobile device rather than their laptops.

IX. ROOTING/JAILBREAKING AND DEVELOPING OF APPLICATIONS

Rooting and jailbreaking seemed widely known by students. Moreover among those who knew what jailibreaking/rooting are, the vast majority (83,5%) knew that they are risky practices. However around 35% confessed to having jailbroken or rooted their mobile devices. The gendered analysis revealed that these practices are predominantly male. Similarly, the academic subject analysis revealed that it mostly computer scientists and engineers that more often jailbreak and root their mobile devices.

	%
Yes	84,2
No	15,8

Table 29: Do you know that smartphones and tablets might be jailbroken or rooted?

	%
Yes	83,5
No	16,5

Table 30: Do you think they are risky practices?

	%
No	64,3
Yes	35,7

Table 31: Have you ever done it yourself or asked someone to do it on your behalf?

Notwithstanding a general understanding of what jailbreaking and rooting are and the fact that a quite significant number of students have jailbroken or rooted mobile devices, they did not seem aware of the consequences of these practices. The questionnaire included some statements regarding the security implication of the practices and the respondents were invited to say if they were false, true or if they do not know the answer. Only in one case the relative majority of the students answered correctly; this was when they considered true that some jailbreaking methods disable some operating system's protections that can be exploited by malicious code. In all other cases, the answers were either wrong or expressive of a lack of knowledge.

The uncaring attitude builds on the presumption that technology is easy to learn and to use: it precludes a critical and informed approach to the subject matter.

Percentage values %	False	True	Don't know
Some jailbreaking methods leave a default password to connect to your iPhone through SSH protocol	7,0	26,9	66,1
Some jailbreaking methods delete some operating system's protections which can be exploited by malicious code	5,0	67,2	27,8
Some jailbreaking methods do not allow to install operating system's updates for a period longer than the usual one	24,5	36,5	39,0
Some jailbreaking methods allow the manual installation of the operating system's updates as soon as they are available	15,8	42,9	41,4
Some jailbreaking methods do not allow the applications to access to data contained in other applications	26,3	27,4	46,4

Table 32: Please, mark the following statements as true or false (the correct answers are the ones in blue) (d30)

As the following table shows, it is only a minority that developed at least one application (around 15%) and among them less than 6% developed several applications.

	%
I do not have any competence and I have never developed applications	55,3
I have some basic knowledge of programming but I have never developed mobile applications	29,9
I developed a mobile application and I have simple knowledge of mobile programming	9,1
I developed some applications	4,3
Professional development	1,6

Table 33: Have you ever developed an applications? If yes, what type of application was this?

In almost half of the cases students developed applications for other people, either for free or for sale.

	%
Only yourself	53,2
Other people (for free or for sale)	46,8

Table 34: The apps you develop are designed for...

Among those who developed applications, 1/3 did not demonstrate knowledge of the principles of Software Development Life Cycle. More than 20% of the respondents had never heard about the Secure Mobile Application Development Guidelines. 40% of them had heard about them but did not really understand them. Only 28% of the respondents claimed that they always apply them and tend to keep them up-to-date. This means that even students that develop applications are not consistently aware of the needed precautions.

	%
Yes	67,4
No	32,6

Table 35: Do you know the Software Development Life Cycle (SDLC) principles?

	%
No, never heard about them	23,2
Yes, I know them but I do not use them	8,5
Yes, I have heard about them but I do not use them	40,1
Yes, I always keep myself up-to-date and I consider them while developing my apps	28,2

Table 36: Do you know the Secure Mobile Application Development Guidelines?

3. CONCLUSIONS

The pilot study involved more than 1000 students from different Italian universities. Even if the study cannot really be considered statistically representative of the population of the university students, the variety of university departments involved and breadth of the students' backgrounds give a reliable overview of Italian students' behaviours and perceptions. As the following table shows, the percentage of people who knows nothing or little about mobile security doubled at the end of the questionnaire and those who believe to have good or excellent knowledge decreased to almost 10%. This result clearly shows that there is knowledge gap that needs to be addressed through of information and training.

	Beginning of the questionnaire (%)	End of the questionnaire (%)
None	1,6	3,1
Small	16,0	30,7
Enough	39,3	34,4
Good	36,6	27,4
Very good	6,5	4,4

Table 37: How do you assess your knowledge on mobile security?

The lack of knowledge does not always result in an unsafe use of mobile devices. Students easily comply with some security safeguards if there are tangible advantages (such as for the updates of the software and applications that provide them with additional or more advances features) or if they are default settings (such as 8 characters passwords, today commonly required).

When the security settings and the updates to enhance the security of the device are difficult to install or to implement students tend to avoid them. The key concept of usability mentioned throughout the report is definitely backed up by the analysis of the students' answers.

The difficulty might be technical (like for example the log out of the applications, often hard to find) or in understanding certain security operations (like for example the reading and acknowledgement of authorizations often presented as obvious but in reality sometimes, misleading).

A particular consideration should be dedicated to passwords. They are commonly used but addressing the difficulties in remembering different passwords appeared to be a priority. Automated solutions for managing passwords together with secure authentication systems could be interesting tools. It should also be noted that being a "heavy user" does not mean to be a more attentive user.
On the contrary, being a heavy user might lead to ignoring some security practices (e.g. heavy users exploit free Wi-Fi for every type of activity) and, on another aspect, the level of security required for being an attentive heavy user is unfortunately not that user-friendly.

An important consideration emerges in relation to students that develop applications and that might therefore be considered as expert users. Even if they develop applications, the majority ignores the Secure Mobile Application Development Guidelines or the Secure Software Development Life Cycle (SDLC). This implies that there is a diffusion of applications that do not match adequate security standards, and it means that potential new developers are not accustomed to paying appropriate attention to security features. The pilot study also suggests that an adequate definition of digital natives specifically related to the Italian context should be further studied.

As a matter of fact, further research on the use of applications, free Wi-Fi and passwords, in relation with the different age groups, will be key to understanding who can be considered a digital native in Italy. Moreover further research will allow understanding how to best train young people that are sensitive and attentive to security.
Moreover the development of technical solutions with security by default and legal solutions to facilitate those developments are needed.

REFERENCES

[1] Google Research Study "Our mobile planet: Italy". Available at: http://www.google.com/think/research-studies/our-mobile-planet-italy.html (Last accessed on 16/02/2014)

[2] ITU (2013) "Measuring the information Society", Geneva. Available at http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx (Last accessed on 16.02.2014)

[3] Tapscott, D. (1998), "Growing Up Digital. The Rise of the Net Generation". New York: McGraw Hill

[4] Palfrey, J. and Gasser, U. (2008), "Born digital: Understanding the first generation of digital natives". Basic Books.

[5] Oblinger, D. and Oblinger, J. (2005), "Is it age or IT: First steps toward understanding the net generation". *Educating the net generation*, 2(1-2), 20.

[6] Prensky, M. (2001a), "Digital natives, digital immigrants", Part 1. On the horizon, 9(5), 1-6. Available at: http://marcprensky.com/articles-in-publications/ (Last accessed on 16.02.2014) and Prensky, M. (2001b), "Digital natives, digital immigrants" Part 2: Do they really think differently? On the horizon, 9(6), 1-6. Available at http://marcprensky.com/articles-in-publications/ (Last accessed on 16.02.2014)

[7] Helsper, E. J. and Eynon, R. (2010), "Digital natives: where is the evidence?", *British Educational Research Journal*, 36(3), 503-520.

[8] Hargittai and Hinnant (2008), "Digital Inequality Differences in Young Adults' Use of the Internet. In Communication Research", vol. 35 n. 5, pp. 602-621.

[9] Jones, C., Ramanau, R., Cross, S. and Healing, G. (2010), "Net generation or Digital Natives: Is there a distinct new generation entering university?" *Computers and Education*, 54(3), 722-732

[10] Livingstone, S. and Helsper, E. (2007), "Gradations in digital inclusion: children, young people and the digital divide". *New media and society*, 9(4), 671-696.

[12] Bacher J., Wenzig K., Vogler M. (2010), "Spss Two Step Cluster-A first evaluation" Available at: http://www.statisticalinnovations.com/products/twostep.pdf (Last accessed on 21.02.2014)

[12] Knott L. C., Steube G. (2012) "Student Perceptions of Password Security and Maintenance", *in International Journal of Management & Information Systems*, vol. 16, bo.3, pp. 189 – 202

PART 2: TECHNICAL CONSIDERATIONS

1. AWARENESS, KNOWLEDGE AND (FALSE) PERCEPTION

The first interesting result of this study can be derived from the analysis of question 31, where we asked the respondents to evaluate their own knowledge of mobile security issues on a scale from 1 to 10, compared to the actual level of knowledge displayed from their replies in the detailed technical questions.

The results reflect a normal distribution, where most of the respondents (56%) fall between 5 and 7, which is somewhat expected (table 18) since by definition real-valued random variables tend to concentrate around a single mean value. However, a significantly high percentage (55%) was above the "pass" mark in terms of knowledge between 6 and 8. This contrasts with the average percentage of "correct" technical answers i of the questionnaire, which was 29%. These figures remained more or less the same when the computer science students were removed from the analysis (without them it resulted that 47% of respondents grade their knowledge between 6 and 8, and the average percentage of correct answers falls to 23%). It is striking that, while 66% of computer science students grade their knowledge of mobile security issues between 6 and 8, and 76% between 6 and 9, the average percentage of correct technical answers is only 45%.

The technical questions may seem at first sigh "too technical" for the average users. However, this is not really the case. The questions revolve around topics, such as rooting/jailbreaking a mobile device, the risk posed by mobile malware and system updates, which targeted users should be at least familiar with, in order to evaluate their own knowledge of mobile security issues as "sufficient". The results presented in table 37 on "How do you assess your knowledge on mobile security?" stresses the difference between the user's own perception of their level of knowledge, and the actual level of knowledge they could demonstrate (although the possibility of a potential bias induced by the Dunning-Kruger effect6 should be taken into consideration [1]). This discrepancy between perceived knowledge and actual knowledge conveyed through answers to technical questions was confirmed by the different levels of confidence at the beginning and at the end of the survey (See answers to the question "how do your perceive your own knowledge of IT security?" at the beginning and at the end of the questionnaire). After going through the security questions in the survey, the confidence of university students on their level knowledge falls from 82% of respondents evaluating their confidence above 6 before the survey, to 66% at the end. Figures remain similar if we divide the sample of respondents between computer

6 The Dunning–Kruger effect is a cognitive bias in which unskilled individuals suffer from illusory superiority, mistakenly rating their ability much higher than is accurate. This bias is attributed to a metacognitive inability of the unskilled to recognize their ineptitude. (Source: Wikipedia)

science students and all the others, ranging from 92% to 86% in the case of computer science students, and from 76% down to 53% for the rest.

2. SECURITY THREATS RELATED TO MOBILE DEVICES

Based on the answers received, we have identified three aspects of interest in relation to the threats that may arise from the students' behaviour and habits. The first is that of the "general habits", which concerns how they behave with respect to software updates and application permissions. The second is about the habits that involve personal data and potential privacy threats. The third considers the habits that will have economic consequences (losses) for the individuals, such as the silent subscription to premium SMS services by malware.

2.1 GENERAL SECURITY ISSUES WHICH AFFECTS ALL THE MENTIONED THREATS

Starting from general security issues, we consider habits and behaviours that may impact all security aspects, reflecting on all the threats that may derive from an improper usage of smartphones, tablets and their apps.

Just 6.8% of the students do not regularly update their mobile operating system (OS) or their mobile apps, while 81.3% performs regular updates to both (table 6).

Figure 1, which shows the adoption rate of iOS7, confirms this trend. This data is one of the most evident signs of cultural change between the mobile environment compared and the desktop environment, where (and still is nowadays) regular system updates were significantly less frequent. 14.5% of respondents said they do not regularly update their PCs compared with the 6.8% that admitted the same for mobile devices. Software updates are extremely important in order not protect systems from security vulnerabilities. Updating mobile devices is a smooth and easy process, and this data reflects this technical strength.

Figure 1: iOS 7 adoption rate [2]

Oddly enough, this data is inconsistent with the high presence in the market of old mobile OS versions, mainly related to Android phones as shown in Figure 2. It is worth mentioning that Gingerbread is 3 years old and still represents 24% of the devices. On the contrary, iOS devices outdated for longer than a year represent only 4% of the market. We can infer that this is not due to imprudent users, but rather to the huge fragmentation affecting the Android ecosystem. As Google's OS is only natively supported on the Google Nexus line of phones, each manufacturer has to tailor the OS to its own devices, to customize it a little bit for each different smartphone. Also the carriers often add custom apps or code. All of this makes the updates process slower because, for each update that Google releases, every manufacturer and provider have to test the new code against its customization. Since this process is time and money consuming, older devices get left behind in the update schedule, hence Gingerbread's strong market share.

Version	Codename	API	Distribution
2.2	Froyo	8	1.6%
2.3.3 - 2.3.7	Gingerbread	10	24.1%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	18.6%
4.1.x	Jelly Bean	16	37.4%
4.2.x		17	12.9%
4.3		18	4.2%
4.4	KitKat	19	1.1%

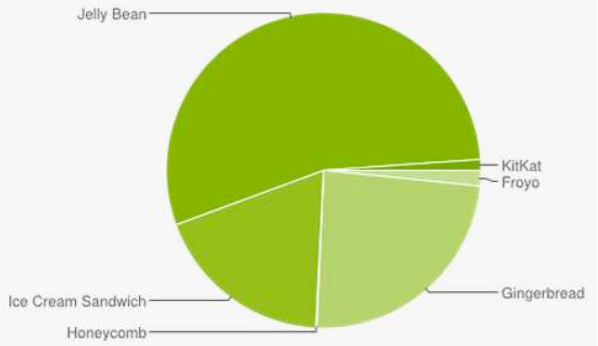


Figure 2: Android OS version distribution

Moving to the installation and usage of apps, 54% of the respondents never or rarely check the permissions apps require (table 15). As expected, this data rises to 60% if we do not consider computer science students. Such behaviour is a dangerous trend that needs to be addressed: overlooking the privileges an app requires increases the proliferation of malware, since users will install and click on "YES" on anything. Too much data are left improperly unattended due to scarce attention to apps' behaviour and to proper data cancellation from mobile devices.

2.2. IDENTITY THEFT

Two questions of the survey relating to Identity Theft were (a) the one concerning which type of data respondents are usually store within their devices and (b) the one related to the most used applications.

With reference to the first, we found, unsurprisingly, that

> 96% of users store their Address Book on their phones and equip it with personal photos and videos (table 5).

65% of users also used the mobile device as a planner or to access their email accounts. The percentage of users accessing their email accounts from mobile devices is slightly smaller

(approximately 54%) for the students of non-engineering faculties.

With regards to the second questions, about the most frequently used apps, we found that mobile devices are often used to access social networks (e.g. Facebook, Instagram, FourSquare, etc.) and instant messaging applications (e.g. Skype, Viber, Hangout, etc.). The vast majority of respondents (85%) used their mobile device for instant messaging. Slightly fewer (75%) accessed social networks.

From this data, it can be argued that social networks and instant messaging platforms are used not only to send text messages to friends and classmates, but also for sharing (and, perhaps, to publish), personal information and data. From this data, it can be argued that social networks and instant messaging platforms are used not only to send text messages to friends and classmates, but also for sharing (and, perhaps, to publish), personal information and data. This is particularly true for photos and videos, tons of which are continuously uploaded on social networks without any restriction on the access rights. Indeed, this makes the users potentially exposed to a series of threats and attacks [3,4,5]. Nevertheless, this also raises ethical issues of their inappropriate management of data [6].
Although users appeared to not care too much of the protection of photos and videos, they did express concern over the loss of data that can result in economic loss (table 18). This conclusion is suggested by three tends highlighted during the analysis:

1. Even if they largely claimed to use mobile devices to browse the web, more than 50% of the students admitted to not engage in online banking. The percentage of users who responded that they frequently their mobile devices for online shopping was also low, totalling only 15%
2. Less than 25% of the students said that they store access information like pin codes or bank account credentials on their mobile device. Also very few of the respondents (less than 10%) played on-line games that involve winning or loosing money, such as online poker or virtual slot machines.

A worrisome conclusion can be drawn concerning the practice to sell mobile devices or give them away as a gift (see Chapter 1, paragraph iv). About 25% (table 16) claims to have done it at least once: that is not a small percentage at all if we take into account the average age of the interviewed. It is important, thus, to consider if users properly erase all of their personal data from the devices before giving them away. Almost 8% of users did not erase either photos, or videos, or the address book. An even higher percentage of users did not remove the installed applications and did not clean the calendar (about 12% for both), and that of users that did not reset the device to factory settings (about 13%). From this data, we can estimate that approximately a 3% of the circulating devices are sold or given away as a gift while still containing personal data of the original owner.

Another important issue is how the users manage their application passwords. The analysis revealed that Just 25% of responders regularly logged out when they were done using an app (table 14).

The vast majority (about 55%) remained logged-in, whereas the others logged-out occasionally. Users also claimed that the choice to remain logged in is not due to any technical obstacle (e.g. they can not find the logout button), but is deliberately made. This renders addressing the issue complex; it involves more than simply redesigning user interfaces and calls for a more in-depth review of the authentication mechanisms.

About 40% of students does not use any lock mechanism to prevent non-authorized access to the device.

Also, a large group of the respondents (52.5% of those who don't use lock the device) is claimed to forsake the security feature in order to maintain easy access of the device (tables 26-27).

In addition to this, there is a second large cluster of users (40%) who did not express interest or concern about locking mechanisms.
Such results become particularly relevant when considering the amount of personal data, and log in credentials, stored by App stores, [7,8]. This ambivalent attitude towards password protection increases the chances of identity theft, particularly in the event of a device being stolen or lost.
The first result obviously suggests to study lock mechanisms that are both secure and straightforward for the customers to use. The research community is already working on this issue and a number of papers have been proposed [9,10]. The second result suggests that work still needs to be done to raise awareness of the importance of protecting all personal data stored on mobile devices.

2.3 ECONOMICAL THREATS

From the survey (table 15) it appears that users very often do not check the permissions required by the apps. This may be due to the fact that on some mobile platforms (Android, Windows Phone) permissions are granted in an "all or nothing" form- meaning that users have to accept all permissions required by the app in order to be able to install it. This is a dangerous model that trains people to overlook permissions, because they want to install that application not matter what the requisites are.

This result becomes more worrisome if linked with the fact that 17% of the respondents install mobile applications from untrusted sources other than the official application markets (table13).

These two results together support the proliferation of mobile malware and particularly of the category of "toll fraud" [11], where the application silently subscribes the user to premium-rate SMS services, threatening overcharges to the users' bill and other types of financial hindrances.

3. MANUFACTURES, DEVELOPERS AND DEVELOPMENT

As mentioned in Section 2 above, the respondents were inclined to regularly update their devices. We can infer from this that they were conscious of the importance of software updates, and that the procedures to update mobile devices and apps are considerably more intuitive than they used to be. This result appears to be in contrast with a number of worrisome statistics concerning the number of mobile devices running out-dated OSs. As we already mentioned, we can argue that the responsibility of this lies not on the end-users, but instead on other reasons such as the market policies of carriers and manufacturers and, in the case of the Android platform, even in the extreme fragmentation of the market.

Another interesting consideration is about the degree of consciousness of the risks arising from the development of insecure code. According to a recent Linkedin study [12], iOS and Android software developers are currently the two most sought job profiles.

Unfortunately, among the respondents who declared to develop mobile applications (either for fun or profit) only 28% was aware of the guidelines for secure mobile programming (tables 33-34-35-36).

This easily translates in a worrisome proportion of the circulating applications being developed without having these principles in mind. This issue pairs with other well-known risks for mobile users, such those arising from over-privileged [13] and repackaged [14] applications.
There is a generally inadequate attention to security also by the apps developer.

4. PROPOSED SOLUTIONS AND INITIATIVES

Starting from the results of the survey, we finally propose several possible countermeasures to prevent or mitigate the main security issues that have been identified in the previous sections.

The identified priorities are listed here below:

- Mobile Operating Systems
  - Should allow users to install the applications without being obliged to accept all the permissions required. It has to be possible for users to revoke/grant any single permission at any time, without being compelled to reject the entire application;
  - Should provide, beside the device reset functionalities, the possibility to remove the users' private data stored within the installed applications in a centralised and straightforward fashion.
  - Should deliver advanced solutions to ease password usage and management. In fact, although most of the respondents (85%) agree and understand the importance of having a passlock mechanism in place, still most of them struggle in using them.
- Vendors
  - Should be required to provide software updates for their products for a longer period of time (e.g. 2 years);
- Mobile software development companies and individual developers
  - Could enforce the use of (good) passwords, imposing that advanced features of certain applications are enabled only if passwords have been properly configured. A similar approach could be adopted also to enforce the use of non rooted/jailbroked devices.
  - Should be liable in case the application does not implement the security mechanisms required to ensure the adequate storage and transmission of the users' data. Policies, standards and laws should be introduced that establish the responsibility.

Among the various countermeasures, a key role is played by vendors, who should grant software updates for their products for a longer period of time.

Beside the technical and legal solutions, raising the awareness on the security issues and threats appears to be a fundamental step, as it clearly emerged from Chapter 1 analysing the raw data. As immediate countermeasure, campaigns on the media (Internet, TV channels, newspapers) would provide tangible benefits. More in perspective and considered the age of the respondents, we can envision courses and trainings at the universities, both for technical and non technical students.

REFERENCES

[1] J. Kruger, D. Dunning (1999), "Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments." *Journal of personality and social psychology* 77.6: 1121.

[2] Mixpanel, "iOS 7 Adoption Rate". Available at: https://mixpanel.com/trends/#report/ios_7/from_date:-112,to_date:0 (Last accessed: 16-02-2014)

[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, M. Ripeanu (2010), "The socialbot network: when bots socialize for fame and money", *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 93,102, December 6-10, 2010.

[4] G. Wondracek, T. Holz, E. Kirda, C. Kruegel (2010), "A Practical Attack to De-anonymize Social Network Users", *2010 IEEE Symposium on Security and Privacy*, pp. 223,238, May 16-19, 2010.

[5] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, C. Pu (2011), "Reverse Social Engineering Attacks in Online Social Networks", *8th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 55,74, July 7-8, 2011.

[6] J. M. Kizza (2013), "Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems", *in Ethical and Social Issues in the Information Age*, pp. 255,280, Springer.

[7] P. Stirparo, I. Kounelis (2012), "The mobileak project: Forensics methodology for mobile application privacy assessment," *Internet Technology And Secured Transactions, 2012 International Conference for* , vol., no., pp.297,303, 10-12 Dec. 2012.

[8] P. Stirparo, I. N. Fovino, I. Kounelis (2013), "Data-in-use leakages from Android memory — Test and analysis," *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, vol., no., pp.701,708, 7-9 Oct. 2013.

[9] S. Uellenbeck, M. Dürmuth, C. Wolf, T. Holz (2013), "Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns", *20th ACM Conference on Computer and Communications Security*, vol., no., pp.161,172 November 4-8, 2013.

[10] A. Serwadda, V. Phoha (2013), "When Kids Toys Breach Mobile Phone Security", *20th ACM Conference on Computer and Communications Security*, vol., no., pp.599,610 November 4-8, 2013.

[11] Lookout, "State of Mobile Security 2012". Available at: https://www.lookout.com/resources/reports/state-of-mobile-security-2012 (Last accessed: 16-02-2014)

[12] LinkedIn Talent Solutions, “Top 10 Job Titles That Didn’t Exist 5 Years Ago”. Available at: http://goo.gl/cxx3Gn (Last accessed: 16-02-2014)

[13] A. Porter Felt, E. Chin, S. Hanna, D. Song, D. Wagner (2011), “Android permissions demystified”, *18th ACM conference on Computer and communications security*, Pages 627-638, October 17-21, 2011.

[14] W. Zhou, Y. Zhou, X. Jiang, P. Ning (2012), “Detecting repackaged smartphone applications in third-party android marketplaces”, *Proceedings of the second ACM conference on Data and Application Security and Privacy*, vol., no., pp. 317-326, February 7-9, 2012.

PART 3: LEGAL POLICY MAKING CONSIDERATIONS

1. RESULTS OF THE SURVEY AND POSSIBLE SCENARIOS

The analysis of our research, which was undertaken on a random sample from across Italy, leads us to conclude that there are three key practices that policymakers should address. They are as follows:

1. The first scenario that emerged concerns mobile devices without any security policies in place designed to restrict access (such as a password or a locking system). From the results of the survey it emerged that 87 % (table 22) of those interviewed use a password for apps and/or websites but pay absolutely no attention at all to the relevant security requirements, with the result that, more often than not, they simply use the predictable password or a word that someone else could quite easily guess on the strength of various personal information that they have regarding the owner of the device (tables 22-23). On the matter of caution when selecting a password, the Italian legislator has stepped in (the only one in the EU to do so), laying down certain requirements regarding length and complexity in Annex B to Legislative Decree 196/2003, which will be referred to here for convenience as the Privacy Code. This particular step highlights how security is increasingly extending beyond the boundaries of a purely technical sphere and into a legal sphere. However there is still a long way to go on the legal and policy side.

2. The second key practice that needs to be addressed is the installation of software and applications from unauthorized stores and the installation of apps that need rights of access to the device and to its higher-level functions. In the former case, which involved 17% of those who took part in the survey (table13), the risk is that malware will be unwittingly installed on the student's device, whilst in the latter case, despite being an application from an official store, there is a chance that the way that the application operates proves to be overly intrusive as a consequence of the user having been rather rash when granting authorization. In both cases, the risk here is that the content of the mobile device is now at the mercy of all and sundry.

3. Finally, the third practice that emerges from the survey is one that gives particular cause for concern and has clear technical and legal repercussions in terms of security and privacy. This is where a mobile device is passed on to someone else, in particular where they are sold as second hand or lent to someone. This practice, which reflects the desire to have the very latest product on the market, with the previous model therefore becoming redundant, can lead to the exposure of a huge amount of data and a vast

number of security problems, given that virtually any type of information and media is transported via mobile devices and many of those who took part in the survey save their passwords for a wide range of services on their phone and fail to log out.

2. IDENTITY THEFT RELATED TO MOBILE DEVICES: LEGAL ISSUES AND POSSIBLE SCENARIOS

Among the possible risks related to the lack of adequate protection measures, one of the most significant is identity theft. Despite a growing awareness at European level of the risk of falling victim to identity theft [1], the replies provided by the students in the survey demonstrate how, in Italy, insufficient attention is afforded to the safeguards to be adopted in order to prevent this. We therefore decided to focus our analysis on this threat.

As mentioned above:

- 27.7% of students interviewed save, on their device, pins and passwords used for private services (table 5);
- 40.3% of students interviewed do not log out after using a service online (table 14);
- 53.8% of students interviewed very rarely or never check the type of permissions required when downloading an app (table15);
- 41.8% of students interviewed use open Wi-Fi systems to connect to the Internet on their mobile device using all types of functions (table 8).

Looking at these initial figures, it becomes evident that attacking a student's mobile device is an easy affair. At the international level, the Federal Trade Commission received more thean 290.000 report of identity theft in 2013 [2]. At the national level, more than 24.000 users fell victim of identity theft as a consequence of bank fraud, with a higher incidence among under 30. [3]. However, with only 12.5% of those interviewed regularly using their mobile device for mobile banking (table 4), it would be reasonable to conclude that the reluctance on the part of students to use their mobile devices for this purpose stems from an awareness of financial risk alone, with students seeing their personal data as being less relevant.

This ignorance towards the value of personal data can expose students to a vast number of offences.

From the classic trick of impersonating someone often just for a joke and as part of general student antics, to extremely complex fraud for significant financial gain (financial identity theft) or even to obtain health care services in a country where the health service is, in the main, run on a private basis (medical identity theft). Finally, it should be remembered that many students have debit and credit cards that draw on accounts held in their parents' names and they do not have the perception of the importance of personal data.

In the United States, the country where identity theft is being witnessed the most, a recent research by the Family Online Safety Institute has shown that the trend is changing; teenagers

are now demonstrating a greater awareness of the risks of identity theft [4]. It is significant, however, that in the same research project 34% of teenagers said that they have shared one of their usernames and passwords with someone other than their parent or guardian.

It follows that one of the most critical issues to be tackled in the IT field is the fact that users need to be persuaded to use a password that can actually operate to protect their data. Our research in fact revealed that:

- 40.1% of students interviewed do not use a password to protect their mobile device (a PIN number. or autolock code) (table 26);
- 41.3% of students interviewed said that, when asked to change their password, the new password that they create takes the form of a minor variation on the previous one (table 21).

Whilst more than half a century has gone by since 1961, the year in which the MIT designed the first personal computer with a password to accommodate multiple users at the same time, the system used to safeguard such a device has really not changed very much at all. This is despite the staggering increase in the number of services that demand ID authentication and provision of a password. It is for this reason that a system of protection on the basis of biometrics and of two-step authentication procedure may be a solution which, over the coming years, will at least be capable of securing a fair compromise between usability and security, as we will see in more detail in the paragraph below [5].It is worth mentioning that 4.8% of the respondents is currently using two-factors authentication (table24).

From a legal point of view, amendments to the law have been tabled and, at times, implemented, in a number of countries in an attempt to establish a more precise definition of the constituent elements of the offence of identity theft in the virtual world. Despite this, the most important aspects still calling out for decisive action to be taken are related to penalties and the activation of online reporting systems for victims. From a recent comparative study of 34 countries carried out by Rand [6], it emerged that only seven countries have adopted ad hoc legislation to tackle identity theft, and only five have an ad hoc online reporting system in place to monitor cases of identity theft and provide victims with assistance at the outset. The penalties imposed for this offence vary in Europe from country to country. Whilst in Finland, for example, the maximum punishment is four years' imprisonment, in Greece a life sentence can be passed, which is still preferable to the death penalty that can be imposed in China.

Against this backdrop, the introduction of ad hoc legislation in the various countries in Europe would certainly be a welcome development. First and foremost, however, the collaboration currently underway between national investigative bodies via an EU contact network needs to be reinforced, with reporting being handled on a centralized basis subject to the limits imposed by the law in each individual country. As is the case with any offence committed on the Internet, jurisdiction is at the top of the list of problems, often proving to be insurmountable.

3. SOME LEGAL AND POLICY MAKING CONSIDERATIONS OF MOBILE DEVICES

In tackling the various scenarios set out above, devices of a technical nature alone are not a panacea. What also needs to be engineered is a significant shift in user behaviour in order to

eliminate this misconception of security that, unfortunately, is one of the main reasons behind the rather overly relaxed use of mobile devices.

Whilst it in fact emerged from the survey that 56% thought to be aware of the problems associated with the security of mobile devices, evidence of the worst forms of malpractice was significantly more widespread. This was clearly evidenced in the answers concerning habitual security measures (e.g. 27.7% reported having saved their password in the apps on the device (table5), and 75.9% do not log out once they have finished with a particular application).

Steps therefore need to be taken in the form of policies and regulations that govern the work done by manufacturers and users alike and which result in enforcement of the default privacy policies that are currently receiving significant backing on an EU level, where discussions are underway for a new Data Protection Regulation[7].

The adoption of legislative policies and regulations on security would also have the not insignificant effect of reducing the number of offences connected with erroneous configurations in relation to the security of devices. A parallel can quite properly be drawn here with other laws and rulings that govern safety and security in other sectors, placing obligations upon manufacturers (e.g. Council Decision 93/465/EEC of 22 July 1993 regarding CE mark that certifies that the product complies with certain applicable safety requirements) as well as on suppliers (e.g. the security requirements to be met by certifying parties where electronic signatures are used) and users (e.g. Article 172 of the Italian Highway Code, which requires the use of seat belts and child seats in cars).

In the IT-legal field, however, the steps taken to date by the legislator in order to place manufacturers and users under a duty to comply with security requirements are few in number, and concern parties, sectors and situations that are very specific in nature. In particular, provisions governing IT security are almost always to be found incorporated into legislation that concerns duties on the provider (in a broader sense) or, in terms of legislation concerning data protection, on data controllers. This should not, however, mean that we lose sight of the fact that security is an essential prerequisite not only in order to safeguard privacy, but also in order to establish effective governance in all sectors associated with the processing of computerized data.

3.1 HOW TO PREVENT SECURITY THREATS

There has been evidence for some years now of attempts on the part of the EU and Italian lawmakers to regulate security and, therefore, prevent the problems that can arise as a result of second-rate security policies. In terms of mobile devices, the particular pieces of legislation that are most significant concern the security requirements placed on services providers, such as Directive 2002/58/EC [7]. This Directive in fact establishes that:

> *"Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risk of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing*

7 For more information, please see: Data Protection Day 2014: Full Speed on EU Data Protection Reform. Available at: http://europa.eu/rapid/press-release_MEMO-14-60_it.htm (Last accessed on 21.02.2014)

> *security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies."*

This Directive, however, must now be combined with the recent data breach regulation [8], there is one exception to the general data breach notification in art. 4, which is the following:

> *"Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it."*

These two Directives have already been implemented by the Italian Parliament and have come together to make up the Privacy Code.

The results of the survey demonstrate, however, that problems with security often arise as a result of a failure by the user to use the device correctly, rather than a failure by the provider to implement effective security measures.

This is exactly what prompted the Italian Data Protection Authority to focus attention, for example, on the use of mobile devices with its 'Fatti smart!' ['Be Smart!'] campaign [9]; it also explains why, in certain cases, the policies adopted by American universities require centralized security measures to be set up on mobile devices owned by anyone that wants to use the services offered by their college.

3.2 SECURITY V USABILITY: IS THIS THE REAL DILEMMA?

We previously reported the discovery that 41.3% of students who took part in the survey reported that, when asked to change their password, the new password that they create takes the form of a minor variation on the previous one to make it easy to remember: this fact needs to be put together with the discovery that

54.5% of the students go onto sites that require authentication via Google or Facebook.

This confirms the extent to which usability is a determining factor in terms of the level of trust

that a user places in an online service. Usability can, however, in turn potentially lead to a reduction in the levels of security offered by the device, especially if it is a mobile device that is involved. For this reason, it is essential that proposals for a security and usability threat model be put forward, detailing the different factors that are pertinent to the security and usability of secure systems, together with a process for assessing these. [10]

This is without doubt the objective to be worked towards over the coming years, not only from a technical point of view but also from the point of view of policy making. Use that is 'simple but safe' could, however, give rise to greater risks on the privacy side: one way of ensuring greater security for the user is without doubt by storing a larger quantity of data in relation to the user that is potentially sensitive in nature, evidencing the fact that security requirements are not always entirely compatible with those linked to the protection of privacy.

Ultimately, the amount of data that is shared by users on a daily basis and the statistics regarding cyber-attacks, particularly in relation to cases of identity theft, suggest that it is of paramount importance that consideration be given to formulating IT-security legislation that impacts devices used on a daily basis. It is important to raise awareness such that users are forced to appreciate just how important IT security is, not just in terms of eliminating risk but also to ensure that the device is more efficient and has greater output.

3.3 THE RIGHT TO FORGET AND MOBILE DEVICES

One of the pillars of the forthcoming regulation on personal data processing is the so-called “right to forget and to erasure”, being “the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data” (see art. 17 of the draft regulation).

Here we are concerned with the processing of personal data, where a data subject consents to their data being processed by a data controller, who is required to guarantee a series of rights, including the right to forget. In this context, the sample taken for the purposes of the survey will generally find that they are not subject to the provisions of the forthcoming data protection legislative framework: digital natives process the personal data on their mobile devices for personal reasons only, and the regulation does not apply to data processing “by a natural person without any gainful interest in the course of its own exclusively personal or household activity” (see art. 2 (d) of the draft regulation).

Venturing beyond the strict application of the law, however, it is of course entirely possible that, when dealing with a specific example of data processing, the data controller will also be forced to delete certain content from a mobile device that someone is using. We have of course seen that the main purpose of using a mobile device is to share data and information. In this sense, where the right to forget is enforced against a certain data controller (e.g. a content provider), it is essential that the data controller is able to enforce that right in relation to any device being used by a third party, in the absence of which the content in question will remain on the Internet permanently.

In the Opinion of Advocate-General Jääskinen of EUCJ in Google Spain S.L. and Google Inc. v Agencia Española de Protección de Datos (Case C-131/12) he said that “Even if the Court were to find that internet search engine service providers were responsible as controllers, quod non, for personal data on third-party source web pages, a data subject would still not have an absolute ‘right to be forgotten’ which could be relied on against these service providers. However, the

service provider would need to put itself in the position of the publisher of the source web page and verify whether dissemination of the personal data on the page can at present be considered as legal and legitimate for the purposes of the Directive. In other words, the service provider would need to abandon its intermediary function between the user and the publisher and assume responsibility for the content of the source web page, and when needed, to censure the content by preventing or limiting access to it."

Future regulations governing the right to forget will, therefore, have to include a series of technical and legal stratagems that will enable personal data to be 'flagged' or 'deleted' in order that the full range of rights connected with that data can be exercised [11].

It is no coincidence that ENISA itself published a paper in 2012 [12] in which it concluded that "[...] all existing technical approaches to ensure the right to be forget are vulnerable to unauthorized copying while the data is publicly accessible and a re-dissemination of such unauthorized copies once the data has expired. Therefore, the right to forget cannot be ensured using technical means alone. A possible partial solution may be a legal mandate aimed at making it difficult to find expired personal data, for instance, by requiring search engines to exclude expired personal data from their search results."

4. POLICIES AS A SECURITY TOOL: THE REGULATION OF MOBILE DEVICES IN UNIVERSITIES

Given the scope of our research, there is certainly some mileage to be had in focussing on the security policies currently in place in the university environment. Of equal interest is a comparison between the security measures adopted on university campuses in the US with those implemented in at universities in Europe. Whilst certain universities in Europe certainly cannot be criticized for the amount of attention that they pay to the matter of IT security [13] their efforts would appear to focus on the issue of liability arising from the unlawful processing of data as opposed to enforcement on a practical level in order to ensure that their IT systems boast greater levels of security. From this standpoint, is it interesting to note that in certain American universities [14] security standards (e.g. HIPAA) are imposed for mobile devices owned by students and university staff (Bring Your Own Device- BYOD) in order to verify their security levels (use of anti-virus software, updates to the operating system and encryption systems).

It emerged from a paper recently written by the JISC in partnership with the Universities of Strathclyde and Glasgow that the most complex challenge faced by universities (and they are not alone here) is in managing the multitudes of different types of devices to be found on the market [15]. This prompts the need to set up different forms of control over access to the network services provided on campus. It also calls for the creation of measures that target situations of loss or theft of devices and data.

An analysis of the security policies adopted by some of the leading Italian universities suggests that, when it comes to regulating mobile devices owned by students and university staff, these institutions could be open to criticism for falling short of what is required. We have plans over the next few months to carry out a comparison of the security policies adopted by the universities involved in the project, aiming at drafting a sound comparison between Italian and European universities.

In conclusion, the current system of online access to university resources calls for review. This is not only to bring it in line with legislative provisions, but mainly in order to reinforce existing security policies in order to prevent possible cyber-attacks that take advantage of shortcomings in the safeguards in place to protect mobile devices that are connected to the university network.

5. PROPOSED SOLUTIONS AND INITIATIVES

The analysis of the results of the survey produced clear evidence that any solution put forward needs to be examined on the basis of a holistic approach to security that provides answers from both the technicians and the legislator involving not only the providers but also the users.

As mentioned on a number of occasions in this report, it is essential in this sense to invest time and effort in raising user awareness of security issues and, in particular, in encouraging a better understanding and adoption of privacy-protecting behaviour [16]; this issue was in fact emphasised by the Italian Data Protection Authority on the occasion of the recent European Privacy Day on 29 January of this year with its 'Educare alla Rete' 'Understanding the net'] event. [17].

Forthcoming actions must focus on privacy-protecting behaviours.

It is, on the other hand, also essential that hardware and software manufacturers carry out their design and programming work with a focus on security for the user, with 'user' here not intended as someone who simply picks up pre-packaged solutions, but someone who is an active participant where the security of the mobile device is concerned and is the living subject of the data that is holds or channels.

It is in fact clear for all to see how a form of 'centralized' security in the hands of the manufacturers or the providers could quite possibly be circumvented.

resulting in damage on a colossal scale, or how it could easily be placed under some form of control, thereby contributing to the creation of a society that is monitored to an even greater degree, against the principles enshrined by law. Similar obligations need to be imposed upon providers in their role as owners of the channels of communication and the areas that the data is sent through or is stored in.

In short, what is required is to embrace the principles of privacy by design [8] that constitute another fundamental pillars of the forthcoming data protection regulation, with even greater attention being afforded to the issue of security. The ideal goal would be to have a system that integrate security by design and by default.

Finally, from a legislative standpoint, it is important that schemes be set up to provide information and draw attention to this issue in order to create a proper 'culture of security'; this point was in fact made as far back as 2002 by the OECD in its guidelines for the security of information systems and networks, [18], which were based on the following points:

1. **Awareness**
   Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. **Responsibility**
   Participants are responsible for the security of information systems and networks.
3. **Response**
   Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. **Ethics**
   Participants should respect the legitimate interests of others.
5. **Democracy**
   The security of information systems and networks should be compatible with essential values of a democratic society.
6. **Risk assessment**
   Participants should conduct risk assessments.
7. **Security design and implementation**
   Participants should incorporate security as an essential element of information systems and networks.
8. **Security management**
   Participants should adopt a comprehensive approach to security management.
9. **Reassessment**
   Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

On this point, it is finally worth mentioning the recent Horizon 2020 programme, which makes provision for the funding of specific research into issues of digital security to increase "*the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets & market incentives in Europe, following an end-user driven approach, including for instance law enforcement agencies, first responders, operators of critical infrastructures, ICT service providers, ICT manufacturers, market operators and citizens.*"

8 Privacy by Design is an approach whereby privacy and data protection compliance is designed into systems holding information right from the start, rather than being bolted on afterwards or ignored, as has too often been the case.

REFERENCES

[1] Special Eurobarometer, "Report on Cybersecurity July 2012". Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (Last accessed 21-02-2014).

[2] Federal Trade Commission, "Consumer Sentil Network 2011-2013", 2013. Available at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf (Last accessed 21-02-2014).

[3] Osservatorio CRIF, "Osservatorio CRIF sulle frodi creditizie, 2013, available at http://www.crif.it/News/Comunicati-stampa/Pages/furti-identita-primo-semestre-2013.aspx (Last accessed 21-02-2014).

[4] Family Online Safety Institute, "Teen Identity Thef, Fraud, Security, and Steps Teens are Taking to Protect Themselves Online", November 2013, available at http://www.fosi.org/research/1326.html (Last accessed 21-02-2014).

[5] Cynthia L. Knott, G. Steube, "Student Perceptions Of Password Security And Maintenance", *International Journal Of Management & Information Systems (IJMIS)*, Vol 16, No 3 (2012), available at: http://journals.cluteonline.com/index.php/IJMIS/article/view/7071 (Last accessed 21-02-2014).

[6] N. Robinson, H. Graux, D. M. Parrilli, L. Klautzer, L. Valeri, "Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report", RAND Europe, June 2011, available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf (Last accessed 21-02-2014).

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available at. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF (Last accessed 21-02-2014).

[8] Commission Regulation (EU) No 611/2013 of 24 June 2013. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF (Last accessed 21-02-2014).

[9] Data Protection Authority, "Fatti smart! Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet", availble at: http://www.garanteprivacy.it/fattismart (Last accessed 21-02-2014).

[10] R. Kainda, I. Flechais, A.W. Roscoe, "Security and Usability: Analysis and Evaluation", *Oxford University Computing Laboratory*, 2010, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.162.374&rep=rep1&type=pdf (Last accessed 21-02-2014).

[11] V. Mayer-Schoenberger, "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing", *Working Paper, John F. Kennedy School of Government, Harvard University*, April 2007 available at https://research.hks.harvard.edu/publications/workingpapers/citation.aspx?PubId=4830&type=FN&PersonId=79 (Last accessed 21-02-2014).

[12] ENISA, "The right to be forgotten – between expectation and practice", November 2012, available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten (Last accessed 21-02-2014).

[13] See, for example, the security policies in force at Bristol Unviersity available at http://www.bristol.ac.uk/infosec/policies/ and Oxford University available at: http://www.it.ox.ac.uk/infosec/ispolicy (Last accessed 21-02-2014).

[14] See, for example, University of California - University of California IS-3 Electronic Information Security, available at http://policy.ucop.edu/doc/7000543/BFB-IS-3 (Last accessed 21-02-2014).

[15] JISC, "Legal Mobile Technologies and the Law: An Overview", 2012, Available at: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2645/Mobile-Technologies-and-the-Law-Overview-19-November-2012.aspx (Last accessed 21-02-2014).

[16] A. E. Marwick, D. Murgia-Diaz, J. G. Palfrey, *Youth, Privacy and Reputation*, *Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10-29*. Available at: http://ssrn.com/abstract=1588163 (Last accessed 21-02-2014).

[17] Data Protection Authority, Educare alla Rete. L'alfabeto della nuova cittadinanza nella società digital, available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2893366 (Last accessed 21-02-2014).

[18] OECD, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: http://oe.cd/2002sg (Last accessed 21-02-2014).

CONCLUSIONS AND RECOMMENDATIONS

We would like to conclude this report with some recommendations addressing the different areas of interest we took into consideration in the report. From a technical perspective, our recommendations are categorized by different technological actors:

- Mobile Operating Systems: should allow users to install applications without being obliged to accept all the permissions required and should deliver advanced solutions to ease password usage and management.
- Vendors: should be required to provide software updates for their products for a longer period of time (e.g. 2 years).
- Mobile software development companies and individual developers: should enforce the use of (good) passwords, enabling advanced features of certain applications only if passwords have been properly configured.

From a legal and policy side, we formulate recommendations aimed at the wider category of policy makers and legislators:

- To create more awareness on security, lawmakers should take into consideration measures to impose the adoption of minimum security standards on the services provided by the sector's main players (e.g. passwords of at least 8 alphanumeric characters).
- Strong security measures (i.e. biometric passwords) are not always compatible with privacy measures. Since security is a fundamental prerequisite for privacy, it will become more and more important to find a fair trade-off between these essential interests.
- Considering the scope of the survey, Italian and European universities should think about revising security policies, with specific references to students' use of mobile devices.
- It is necessary to remember that the user is an active subject of the security process and not just a "dumb component". Only starting from this point is it possible to draft policies and norms to adequately provide effective results in the coming years.

Aside from the technical and legal solutions,

as it has clearly emerged from analyzing the raw data in Chapter 1. As immediate countermeasures, media campaigns (Internet, TV channels, newspapers) would provide tangible benefits. Considering the age of the respondents, we can envision the development of courses and training sessions at universities, for both technical and non-technical students.

CONTACTS & CREDITS

Tech and Law Center

www.techandlaw.net

info@techandlaw.net twitter.com/techlawcenter facebook.com/techandlawcenter

Thanks to:

University of Milan – Bicocca
(Cattedra di Informatica Giuridica)

Amapola Association

Politecnico of Milan
(Dipartimento di Elettronica,
Informazione e Bioingegneria)

The project is kindly funded by

SECURITY OF THE DIGITAL NATIVES