Proceedings of Informing Science & IT Education Conference (InSITE) 2014

Cite as: Ahituv, N., Bach, N., Birnhack, M., Soffer, T., & Luoto, L. (2014). New challenges to privacy due to emerging technologies and different privacy perceptions of younger generations: The EU PRACTIS project. *Proceedings of Informing Science & IT Education Conference (InSITE) 2014* (pp. 1-23). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p001-023Ahituv0529.pdf

New Challenges to Privacy due to Emerging Technologies and Different Privacy Perceptions of Younger Generations: The EU PRACTIS Project

Niv Ahituv
The College for Academic Studies and Tel Aviv University, Tel Aviv, Israel
ahituv@post.tau.ac.il

Nicolas Bach
Nexus Institute for Cooperation Management and Interdisciplinary Studies in Berlin, Berlin, Germany
Bach@nexusinstitut.de

Michael Birnhack
Faculty of Law, Tel Aviv University, Tel Aviv, Israel
birnhack@post.tau.ac.il

Tal Soffer
School of Education, Tel-Aviv University, Tel Aviv, Israel
talsofr@post.tau.ac.il

Liisa Luoto
Finland Futures Research Centre, University of Turku, Turku, Finland
Liisa.Luoo@utu.fi

Abstract

PRACTIS (Privacy Appraising Challenges to Technologies and Ethics) is a research project initiated by the EU. It was carried out over three and one half years by research institutes of six countries: Israel (project coordinator), Poland, Germany, Finland, Belgium, and Austria. PRACTIS was concluded in April 2013 with the submission of a list of recommendations to the EU.

PRACTIS focused on three major research tracks: Technological forecast, ethics and legal aspects of privacy, and the changing perception of privacy among younger generations (Internet "natives").

This paper consists of two parts. The first part describes one of the most interesting studies which were carried out within PRACTIS – the high-school children survey about their perception of

privacy. The second part outlines some policy recommendation mostly for governments and regulators.

The major conclusion of the high-school survey indicates that there is, indeed, a different perception of privacy among teen-agers. For them, the individual sphere in which they wish to protect their privacy is not limited only to their immediate physical environment (home, diary, body), but it is expanded also to their virtual environment such as social networks sites (SNS). They are also willing to trade benefits provided by the digital environment for privacy.

The major recommendation conveyed to the EU is that there is no one "deus ex machine" solution to the threats privacy faces due to emerging technologies such as ICT, Genetics, Nanotechnology, Cognitive and Brain Sciences, and the like. There should be a comprehensive strategy and policy and a basket of solutions adhering to technology, law and regulations, organizational issues, education, and social issues. A detailed list of recommendations is exhibited in the article.

Keywords: privacy, privacy threats, privacy and technology, the internet generation, teenagers perception of privacy, privacy by design, social networks

Introduction

PRACTIS (Privacy Appraising Challenges to Technologies and Ethics) is a research project initiated by the EU. It was carried out over three years by research institutes of six countries: Israel (project coordinator), Austria, Belgium, Finland, Germany and Poland. PRACTIS was concluded in April 2013 with the submission of a final report and recommendations to the EU.

PRACTIS had two main goals:

- To identify and assess evolving impacts on privacy that might result from various emerging and future technologies and new scientific knowledge, and to propose means to cope with potential future risks to privacy in both the legal and social spheres, while maximising the benefits of these new technologies.

- To formulate a framework for thinking about the ethical and legal issues related to privacy in the future when the emerging technologies will prevail, and to explore novel policy options to address the needs of citizens in a world of new technologies while maintaining privacy.

PRACTIS was carried out through three major tracks:

- **A technology track**: This track focused on technology and privacy.
- **A legal and ethical track**: The track reviewed laws, regulations and legal approaches to privacy in various jurisdictions.
- **A behavioural and perceptive track**: This track dealt with the question how people perceive privacy and how they behave when privacy threats surround them.

This paper consists of two parts. The first part describes one of the most interesting studies which were carried out within PRACTIS – a high-school survey among adolescents about their perception of privacy. The second part outlines some policy recommendation mostly for governments and regulators (for detailed reports of each of the research tracks, see www.practis.org). The recommendations aim at policy makers: legislation, regulation, education, and other measures.

Part I: High-School Students Surveys: Privacy Perceptions

Introduction: Objective of the Survey

The objective of the survey was to get a deeper insight on the privacy perception of the digital natives, i.e., contemporary high-school students. To achieve this objective an exploratory survey was conducted in the countries of the PRACTIS project partners. To make potential generational differences visible the PRACTIS project consortium decided to include an adult control group that answered the same questionnaire as the students. The privacy perceptions of contemporary students are especially interesting for the PRACTIS project as they can help to predict future understanding of privacy. Those students will be the managers, engineers, regulators, and other stakeholders in the near future, thus their view of privacy will prevail in less than 20 years from today.

Methodology

To analyze the privacy perceptions of the so-called digital natives, the PRACTIS project decided to survey at least 200 high-school pupils in the six partner countries of the project. The questionnaire was designed to give insight into the following topics:

- Scale and scope of personal Internet use (online shopping, web-based social networks, etc.)
- Use and acceptance of personalized services and social networks on the web
- Preparedness to upload personal data on the web and attitudes towards data protection
- Acceptance of video surveillance in public sphere, of RFIDs, body scanning, police access of private computers, and the like.
- Use of data protection systems (Firewalls, anonymisation software)
- Attitudes towards governmental data collection and data collection by business organizations.

The Sample

Students from the six partner countries of PRACTIS project were surveyed. The total sample consisted of 1,428 students distributed as follows:

- 385 Israel
- 177 Finland
- 247 Germany
- 261 Belgium
- 222 Austria
- 136 Poland

55.7% of the respondents were female and 44.3% were male. This slight imbalance cannot be explained as whole classes were surveyed. The target age group of the survey was students between 16 and 18 years. Actually younger and older students were also surveyed but the majority of respondents (79.9%) were within that domain.

Additionally, a group of 125 adults (average age of 50 years) was given the same questionnaire in order to identify generational differences in the perception of privacy.

The PRACTIS school survey cannot claim to be representative for several reasons: Firstly, the number of students surveyed in the different countries is too low to meet the requirements for

having a representative sample. Secondly, the sample is not stratified and therefore does not cover all layers of the society. Therefore, the results of the PRACTIS school survey should be seen as indicators that may help to explore and describe current trends and developments. The same is true for the questionnaires filled out by the adults.

Nevertheless, the results are of interest for contemporary scientific discourse, as they allow for a comparative analysis of different European countries and can also be used to identify generational differences. Further research is required to substantiate them.

The Questionnaire

The questionnaire was divided into two parts. The first part consisted of questions on the following topics:

- Scale and scope of personal Internet use
- Social network sites
- Privacy and data security

This part of the questionnaire contained multiple-choice questions and statements that should be evaluated by the respondents. For the evaluation of the statements we used a five-level Likert scale, ranging from '1-Strongly disagree' to '5-Strongly agree'. For some questions we added as additional level '6-I don't know'. This level was not considered in the data analysis when averages were calculated.

The second part of the questionnaire consisted of six short scenarios on different existing and emerging technologies (RFID, body scanners, video surveillance, and medical sensors). After reading the scenarios the respondents were asked to respond to multiple-choice answers with different options describing how they would behave in the given situation. Additionally, narrative statements were presented and evaluated using Likert scales as mentioned above.

The development of the questionnaire was based on the general research topics mentioned above and the results of the 'Literature Overview on Changing Privacy Perceptions' of the PRACTIS project. The literature overview also served to identify important questions that should be part of the PRACTIS questionnaire. Additionally, the results of the horizon scan on privacy intruding technologies served as an input to identify technologies beyond the Internet. We decided to consider emerging technologies in addition to the usual ICT stuff (social network sites and Internet use as impact factors on privacy).

After a multistage review process within the project consortium and pre-test by adolescents from the target age group (16 to 18 years), the questionnaire, which has been developed in English, was translated into the respective languages of the participating countries: Austria, Belgium, Finland, Germany, Israel, and Poland. After the translation, the questionnaire was once again pretested to assure the comprehensibility of the questions.

For the accomplishment of the survey a team of the project researchers went to the schools where they gave a short introduction in the objectives of the PRACTIS project, explained some central notions used in the questionnaire (privacy, data protection, data security), and distributed the questionnaire to the students. Additionally, all students received a questionnaire for their parents and were asked to return it to the school master after they have been filled out. As the completion of the parental questionnaire was done on a voluntary basis, a low response rate was expected.

Data Analysis

The SPSS software was used for the calculation of mode, mean, variance, standard deviation, interquartile range, percentiles, and histograms. For a more detailed insight, different subgroups were formed and analyzed. The following subgroups were examined:

- Countries
- Gender
- Time spent online
- Age groups

With regards to age groups, the main focus was on the target group of 16 to 18 years old students. To reach further insights a group of younger students (14 and 15 years old) as well as a group of older students (19 to 23 years old) was further examined.

The cross-national comparison between the different participating countries is an additional benefit of the present study. Besides the descriptive analysis of the data, we also examined possible interrelations between variables to identify potential interrelations and to explain patterns we found in the results.

Some questions included open answers that gave the respondents an opportunity to describe in greater detail their reasons or motivations for the closed answer given in advance. For the qualitative analysis of the open questions, we categorized them by assigning codes using the ATLAS.ti software. The categories allowed for a quantitative analysis of the open answers.

In a last step we compared the results of the students' survey with the results of the adult control group to identify generational differences.

Highlights of the Findings

Personal internet use

Almost all students have access to a computer at home with which they can surf the Internet. Of all participants, 93.6% possess their own computer. This computer is either located in their own room (70.2%) or in another room at home (25.3%). Adolescents spend a large percentage of their time communicating (e.g., in chats or on ***social network sites*** (**SNS**)), mostly without parental control. The participants of the PRACTIS survey report that SNS (84.3%), e-mails (76.2%), and instant messaging (70.2%) are used most frequently.

Most respondents are well aware of the need of security and of using some kind of security software: antivirus software (80.3%) and firewalls (55.6%) are widespread, followed by spam filters (29.7%), anti-spy software (19.5%) and other software (7.3%). Privacy-related anonymity software is hardly in use (4.3%).

To find out if the online behavior leads to privacy threats for the students, we asked if they have already experienced misuse of their personal data that is available online. In total 7**.8% had experienced a misuse of personal data**. According to the open answers given for that question, it was mainly misuse of photos, e.g., photos were copied and appeared in another site in the Internet, embarrassing photos were distributed or posted, modification of photos were made, etc. (27.1% of given answers) and the misuse of an account, e.g., change of a profile, sending messages from other peoples' accounts, hacking of accounts, etc. (14.6% of the answers). 10.4% of the answers mention the passing on of personal data without the knowledge of the respective person (e.g., passing on of e-mail addresses and other contact information) and identity theft as experienced misuse of personal data. Although only 7.8% of respondents experienced the misuse of personal data **nearly 25% of present-day students feel the need for more online protection**.

This is surprising, as those adolescents are digital natives by definition. One could expect that they feel safer with a medium that is an integral part of their everyday lives.

The use of SNS

88.1% of the total sample report that they have an SNS-profile. Other recent studies show comparable numbers of SNS users. Salaway and Borreson (2008) reported that among undergraduate students in the USA 85% are SNS users. Most of them use SNS to communicate and stay in contact with friends they have in their offline ("real") life. Those results are supported by the findings of Hampton, Sessions Goulet, Rainie, & Purcell (2011) that only 7% of Facebook friends are users that have never met in person.

Concerning the personal information students post online, the present survey showed that **adolescents put large amounts of information online**. A large percentage of students post their gender (88.4%), age (80.9%), real name (81.2%), and photos or videos of themselves (75.4%) online. They also publish personal image-related information like comments (64.0%), hobbies (58.3%), and relationship status (65.2%). Personal details leading directly to the "real-world self", such as addresses and phone numbers are accessible online to a comparatively lower extent. Nevertheless, 24.0% and 15.8%, respectively, avail this information.

When employing SNS, users have the ability to restrict access of strangers to their profile. To be able to judge possible privacy threats, we asked which information is put online and if privacy settings that restrict the access to their SNS profile are applied.

Most students restrict the access to their SNS profile. The large majority (76.0%) use simple mechanisms to restrict access, whereas 10.7% have a completely public profile and 11.8% use restrictions including defined groups. The remaining 1.4% employ other forms of restrictions.

The combination of both aspects (restricted access and information posted online) offers better insights into possible privacy threats. We observed that students exercising the most restricted access to their profiles also posted less information online. Adolescents with simple restrictions regarding their profile share more personal image-related information like photos, books, status, and hobbies. With regard to e-mail address, home address, and phone number online, those with a completely public profile share more information (60.0%, 31.9%, and 26.7%). These figures are higher than those pertaining to the total sample of SNS-users (52.5%, 24.0%, and 15.8%). A possible explanation could be the general awareness for privacy issues: persons sensitive to possible privacy threats care about who accesses their profile and, thus, use some or more elaborate access restrictions (partially public profiles for all friends or defined groups). Additionally, they think more carefully about which personal data they publish online. We can assume that people having a completely public SNS profile are less concerned about possible privacy threats and which personal data they post online.

To explore adolescents' views on SNS, we asked them to evaluate several statements regarding SNS ("1 – I fully disagree" to "5 – I fully agree"). The statements covered possible privacy threats, as well as positive aspects of SNS. It seems obvious that it is important for students to benefit from SNS: students agree that others should be able to find them on SNS (M = 3.44) and want to have an authentic profile (M = 3.56). However, the students agree that it is very important for them to be in control of the accessibility to their profiles (M = 4.01), and the distribution of their personal data (M = 4.43). If there is a conflict between the benefits of SNS and privacy threats, students are undecided regarding their reaction. Students slightly agree that a lack of data security would be a reason to quit SNS (M = 3.27), whereas the lack of tools to manage audiences would not necessarily motivate them to quit SNS (M = 2.93). While the students enjoy the positive sides of SNS, they want to have control over possible privacy and security threats. Yet, **when**

it comes to a preference between benefits of SNS and privacy threats the students would not clearly reject SNS in favor of data security and privacy.

Privacy and data security

The results show that **students care about privacy**. They are prepared to actively oppose to an online corporation challenging their personal interests and would hesitate to use Facebook applications if personal data is submitted to third party developers. In sum, the following conclusion can be drawn: When the students' privacy is at risk in an online context, their preparedness to take action depends on the extent of the consequences. The following declining levels of intervention can be identified:

1. Most respondents are prepared to actively oppose the threats (i.e., their SNS account is kept and they carefully keep using applications already being used).
2. Fewer students are willing to give up the use of risky applications.
3. The fewest students would be prepared to quit an SNS, despite identification of privacy threats.
4. As was previously described, most students were undecided when asked whether a lack of data security or tools to manage the audience would be a reason for them to quit a SNS.

These factors indicate that having an SNS profile and participating in social networking plays such an important role to students that they are even willing to accept a certain degree of privacy risks.

Another question asked whether or not the respondents have ever given the password of one of their accounts to other persons. Additionally, the students were asked to provide the account type and the nature of the relationship with the person to whom the password was given.

More than half of the students (54.9%) declare to have given at least one of their passwords to others. The passwords are mainly given to close persons. Mostly they are passed on to friends (56.9%), to boy/girlfriends (35.1%), and to family members (sisters/brothers: 34.3%; parents: 29.7%). Only 3.7% of the students give passwords to friends of friends, and hardly any passwords are given to strangers (1.4%). The general analysis of which kinds of passwords are passed on corresponds with the general usage of different communication services: Mostly, passwords of SNS accounts (62.2%) and e-mail accounts (56.4%) are passed on, followed by IM accounts (27.4%).

The detailed analysis of the data shows that passwords for SNS accounts are mainly given to friends (43.4%) and girl/boyfriends (30.0%), but seldom to family members (sisters/brothers: 18.3%, parents: 6.9%). Passwords for online-shopping accounts are mostly passed on within the family (parents: 40.3% of cases, sisters/brothers: 27.1% of cases, boy/girlfriends: 14.6% of cases, friends: 13.9% of cases). This indicates that passwords are (1) only passed on to well-known persons with whom a relationship of mutual trust is established and (2) passed around according to common interests (e.g., SNS with friends and boy/girlfriends). It would be an over-interpretation of the given data to say that this is a result of a conscious, deliberating process. Rather, the fact that SNS accounts, for example, are mainly used to stay in touch with friends and boy/girlfriends contributes to the fact that corresponding passwords are mainly passed on to these groups, rather than to family members.

In addition to focusing on the Internet (e.g., SNS), the second part of the questionnaire also focused on several emerging technologies that are related to privacy. The students were asked about their potential behavior, attitudes, and possible security threats related to technologies such as RFID, video surveillance, and body scanners. This was performed by facing the student with a scenario and inquiring about his/her behavior under the circumstances portrayed in the scenario.

The six scenarios are presented in the Appendix. The scenarios describe the use of RFID tags in the context of a rock concert and a shopping mall, the use of video surveillance in schools and public recreation areas, the situation addressing online security and the perception of threat in the Internet, and the use of implanted medical sensors (a detailed description of the scenarios can be found in the Appendix).

The results of the scenario section of the questionnaire show that **students are willing to use the emerging technologies** presented to them, especially when they entail benefits like discounts, convenience, but also security. **Adolescents are ready to trade-off privacy for the benefits**. Nevertheless, the scenarios also show that the students set limits to the use of emerging technologies when their privacy or physical integrity is heavily threatened (as it is the case for the scenario on implanted medical sensors).

In a deeper analysis of the results, we compared students who have a completely public profile with their statements concerning the use of the emerging technologies. The comparison shows that the 10.7% of the students who have uploaded a completely public accessible SNS-profile would use the RFID-bracelet on the rock concert to a higher extent (72.9% compared to 61.6% in the total sample). Furthermore they show a higher acceptance of video surveillance in lavatories (18.5% compared to 11.5% in the total sample) and are more likely to download the fake antivirus-software (26% versus 17.2%). Finally students with a completely public profile are more willing to use the medical sensor without any restriction on the final receiver of the data ("yes" 21.4% compared to 10.8% in the total sample).

On the other hand we had a closer look on those students who do not have an SNS-account. As already mentioned, the main reasons for not having an SNS-account are not only a lack of interest – maybe due to a lower technological knowledge base – but also privacy concerns. Both reasons should result in a more hesitant behavior in the technology scenarios. Accordingly, students without SNS-account are more suspicious towards the RFID bracelet (54.5% would use it compared to 61.6%) as well as towards RFID-tags in the shopping context (42.7% versus 52.5%). Among those without an SNS-account 8.3% fewer students rate patrolling security staff as appropriate to enhance safety in schools. Besides they would accept CCTV in public spaces to a lower extent (62.1% compared to 68.2%), and deny the use of medical sensor to a higher extent (37.1% versus 31.9%). These further analyses show that despite contradictions between attitudes and behavior in privacy-related issues, some patterns emerge where groups of students are either more or less concerned about privacy. These behaviors are consistent between different areas of privacy.

Generational differences of privacy perceptions

Generational differences are confirmed by the adult control group survey. Adults use the Internet differently from adolescents. Adults spend far less time in front of the Internet a day. 40% report being online less than one hour a day, compared to only 17% adolescents. Means for communication in the Internet also differ: Adults use mainly e-mail; SNS and IM do not play an important role. The 49% of adults who use SNS upload less information online. Large differences in information online were found for posting personal and others' photos (-22% and -27%), age (-22%), status (-21%), real name (-18%) and gender (-18%). Interestingly, students and adults show some commonalities regarding the use of SNS. They have the same distribution of public profile settings with 11% of the adults having a completely public profile, 80% having special profile settings for friends and 9% having more sophisticated profile settings (in comparison to 11%, 76% and 12% in the student sample).

Adults show a higher awareness for privacy and a lower preparedness to use emerging technologies. However, they are also willing to trade off privacy for benefits. When trying to explain privacy-related behaviors we always have to consider which trade-offs are made. With regard to

new technologies adults indeed show a lower acceptance, still similar advantages make the technologies interesting for them, namely convenience (e.g., to avoid waiting times) and financial benefits (e.g., discounts). Larger trade-offs are made concerning security. The parents are willing to give up privacy to a higher extent if security may be advanced. This is also reflected in a higher agreement for governmental control and higher acceptance of video surveillance.

Cultural influence on privacy perceptions

Another result shows that **political, societal, and cultural factors influence privacy perceptions.** This is in line with the observations of Cho, Rivera-Sanchez, and Lim (2009).Interesting differences are found between students from different countries. Concerning the country differences, two groups can roughly be identified:

- Countries where privacy concerns seem to be considered to a larger extent using the Internet and emerging technologies. The data of Germany and Austria, and Belgium to some extent, indicate that privacy seems to be an issue when they are online. It is expressed in a stronger agreement to the statements that ask for the importance of privacy, data protection, and data security in Austria and Germany. Furthermore, students from both countries are more reluctant to use Facebook applications when personal data is submitted to third party developers and are more skeptical towards the use of video surveillance. Additionally, those countries are more likely to actively oppose when personal interests are challenged by online corporations, and they are more hesitant to use emerging technologies that are presented in the scenario questions.

- Countries, where privacy concerns seem to be considered to a lower extent while using the Internet and emerging technologies are Israel, Poland, and Finland. Israeli, Polish, and Finnish respondents show less privacy concerns in many questions asked in the survey. They are more willing to use Facebook applications and emerging technologies that collect and submit personal data. Especially a greater acceptance of the use of video surveillance can be found in Israel and Finland. In both countries the preparedness to actively oppose when personal interests are challenged by online corporations is lower than in the other countries of the survey.

Implications

In the context of PRACTIS, the outcomes of the high-school survey support the assumption that the concept of privacy is not a universal one but rather a compendium of various aspects that are shaped by different factors. We see that cultural factors (differences between countries) and time (generational difference) influence contemporary privacy perceptions. Additionally, the behavior relating to privacy is shaped by emerging technologies; i.e., the individual benefits that arise from new technologies (convenience, new services in the network society, discounts, and the like) are traded-off against personal information that is forwarded or submitted to a service provider. Especially the younger generation is prepared to offer personal data for benefits.

On the other hand, the results clearly show that privacy is still important to adolescents, as they try to manage the access to their personal data. This gives rise to a dilemma: Students expose more personal data than their parents do, so we might conclude that they care less about privacy, while at the same time they seem to be aware of what they are doing when they are exposing that data. This implies that they do not perceive any privacy problem when they submit personal information to the network. It seems, therefore that according to our “traditional” view, **there is an inconsistency between the adolescents' values of privacy and their actual behavior.** Obviously, further societal and technological developments will influence the privacy perceptions of fu-

ture generations. Furthermore, the results cannot be easily adopted in the different cultural contexts of the participating countries as we observed that they have different privacy perceptions.

Major Conclusions and Recommendations

Our results show that adolescents consider privacy and data security as fairly important when asked explicitly, yet still exhibit risk-prone behavior, which can be observed when the actual activities of students are examined.

The conclusions drawn from this pattern of inconsistency are firstly, **adolescents perceive social network sites as part of their private sphere**, where they exchange private information with their peers; secondly, **they handle private data in a differentiated way trying to explicitly manage who gets which information.** For the decision on which information is given to whom, the context seems to matter. Finally, **they are ready to trade off privacy for benefits**, like discounts or increased convenience.

Generally, SNS and online activities are increasingly perceived as part of the sphere of privacy. The results indicate that students use social networks mainly for communicating and sharing content with their peers, so that it becomes something like a private marketplace where information between friends is exchanged. In this respect, the PRACTIS school survey confirms the results of the Ofcom report of 2008, which states that the main aspect of using SNS is communicating with friends and sharing personal information. This perception of SNS as being part of their private realm explains the huge amount of sensitive data that adolescents publish in social networks.

Privacy is a contextual construct for contemporary adolescents. Students have a differentiated handling of privacy. Often, the first impression is that students do not care about privacy and/or data protection. A more detailed analysis reveals existing patterns indicating that students are not thoughtless when it comes to privacy or data protection. A good example is the passing on of passwords to a third person. The general number 54.9% of respondents that state to have passed on a password seems to indicate that students' behavior contradicts privacy. A more detailed analysis reveals that passwords are mainly given to friends, boy/girlfriends, and members of the family, i.e., well known persons with whom a relationship of mutual trust is established. These persons might be seen as part of the students' sphere of privacy. Only few adolescents actually do not care about what personal data they exhibit and how it is processed.

As mentioned before, the handling of passwords shows that students differentiate which passwords they give to various persons. This indicates that for adolescents also the context in which passwords are used seems to matter: While passwords of SNS/IM accounts are mainly given to friends and boy/girlfriends, passwords of online shopping accounts are mostly passed on to family members. This corresponds to Boyd's (2008) notion of 'flexible audience management', which describes that teenagers decide which kind of information and communication they want to share with certain people online.

A good example for the management of personal data is the password-sharing behavior. For the general context of privacy perception the students show the following behavior:

1. A high level of preparedness to share passwords (nearly every second adolescent has passed on a password).
2. Passwords are shared with well-recognized persons, such as friends, boy/girlfriends, and family members. Hardly any password is given to friends of friends or strangers.
3. There is a correlation between the type of passwords that are given and the persons receiving it. Passwords for SNS and IM accounts are mainly given to friends and boy/girlfriends. Passwords for e-mail accounts are given nearly equally to friends,

boy/girlfriends, and family members. Passwords for online-shopping accounts are given mainly to family members.

In sum, adolescents demonstrate preparedness to share passwords, but not just to anybody. To some extent, privacy considerations play a role when passwords are shared. This can be concluded from the systematic passing on of certain passwords to specific persons. The handling of passwords indicates that privacy is contextual for students and they treat different types of accounts in a different approach.

The questionnaire used in the PRACTIS school survey cannot answer the question of whether or not the selection of persons with whom they share passwords and the accounts of which passwords are shared is a result of a conscious decision-making process. This could be an interesting question for further research.

The data collected in the PRACTIS school survey indicates that adolescents' perception of privacy is denoted by the following characteristics:

1. **Students are ready to trade off privacy for benefits.** What is perceived as benefit, once again, depends on the respective context. The answers to the scenario questions show that discounts, convenience, and an increase in security are such benefits in everyday life situations. In the SNS context an improvement in communication with the peers or a better self-expression in the Internet are also perceived as such benefits. Nevertheless, our results also show that students are not ready to completely sacrifice privacy for potential benefits of new technologies. The scenarios show that one third to one half of the students is not willing to use such technologies mainly because of privacy and data protection concerns. Additionally, even those who are willing to use such new technologies care about privacy. One scenario describes the use of RFID tags in a shopping center. 52.5% of the students are willing to use such paying method but strongly agree with the statement that the use of such technology must be clearly regulated (M=4.37) and are suspicious about not having control who is reading the information (M=3.89).[1] Another example is the use of video surveillance at recreation areas to increase the security in such places. 74.3% of the respondents state that they would go to such places if the pictures are not stored. Both examples show that students want to enjoy the benefits emerging from new technologies but are not willing to completely sacrifice their privacy in exchange.

   These results support the estimation of the experts in the online survey that **convenience of technology is changing our perception of privacy, with which 72% agree or strongly agree.**

2. **Concerning the cultural dimension of the perception of privacy, the survey shows that differences between countries are observable** but cannot offer detailed explanations, as this was not the intended goal of the study. The observed differences between countries only reflect tendencies found in the results of the PRACTIS school survey and serve as a rough orientation. Nevertheless, trying to give an explanation for the differences, we see that video surveillance is a common feature in schools in Finland and Israel. This helps to explain the great acceptance for this technology in these countries. Additionally, in Israel, being a significant high-tech developer and exporter country, a high trust in technologies can be observed. Combined with being early adopters, this might explain why privacy considerations in Israel are less important when the Internet and

[1] 1 – "fully disagree" to 5 – "fully agree."

emerging technologies are used. Further research is necessary to identify relevant factor that explain the differences of privacy perceptions between countries.

The complex findings of the study lead to the conclusion that adolescents' sensitivity for privacy seems to change towards a more flexible concept of privacy rather than to diminish due to future technologies.

Part II: Policy Recommendations

We first address the importance of having a long-term vision concerning privacy preservation. We name this a "grand policy". We then offer several recommendations, aimed to respond to the challenges we identify.

The Grand Policy

The **grand policy** is the ultimate goal towards which a legislating (or regulating) body strives, namely, how the legislature envisions the level of privacy to be preserved among citizens. Some examples of such directions are illustrated in the scenarios which are listed below, but there could be others.

The grand policy should be decided on before specific recommendations should be adopted and implemented.

The PRACTIS project has portrayed five possible privacy related scenarios towards which our society can proceed. These are[2]:

1. **"Privacy has faded away"**: Different goods have become more vital than privacy, which is still a value, but people have started to sell their "moral" for money.

   Technological context: For example "mind reading", commercial gadgets, robots with sensors, intelligent medical implants, and social map services are widely used.

   People make trade-offs in favor of goods and services (for example, health care and safety provided by new technologies have become more important than privacy).

   People have given up privacy voluntarily (see also Ahituv, 2001).

   Emerging technologies are widely accepted and treated with openness.

2. "**People want to maintain as much privacy as possible**": People believe in privacy.

   People do not accept new technologies as easily as before because of former experiences of privacy intrusions.

   Technology context: Due to the raised awareness of the possible privacy threats posed by new technologies people want to protect their privacy. The effective use of privacy enhancing technologies (PETs) is established (e.g., traceless biometrics, advanced automation technology, invisibility cloaking.)

   People prefer technologies where privacy settings are considered.

   The social norms have developed in such a way that the majority of people have started to oppose the "big brother phenomenon".

[2] The authors wish to acknowledge Prof. Burkhard Auffermann of the Finland Future Research Centre (FFRC), Tampere, Finland, who contributed much to the development and analysis of the five scenarios.

3. "**People have lost control of privacy**": People have become highly dependent on technologies and due to that they have become also highly oppressed by technologies.

> Technology context: brain-to-brain communication, smart carts and medical nanorobots are widely in use.
>
> Dependence on new technologies (such as household robots and social actor robots) has led to a situation where people are permanently monitored by the state or private sector both at home and in "public places".
>
> Information is gathered constantly about everybody.
>
> Citizens have equal access to others' information.
>
> People are "sleep walking" into a world without privacy without noticing anything and suddenly they have no choice but to live with it (see also Ahituv, 2001).

4. "**Segmented privacy**": The world is divided based on social and economic backgrounds.

> Technological context: Producers have made two versions of their technology applications – one version with high privacy settings and a higher price and another with low privacy settings and a lower price.
>
> Emerging technologies and privacy are perceived differently depending on which "class" a person belongs to.
>
> Privacy has become a market value.
>
> Only wealthy people can afford to buy technologies where privacy settings are considered and highly valued.

5. "**Tailor-made privacy – the right to close the door**": Technology enables people to achieve tailor-made privacy.

> Technology context: Privacy enhancing technologies (PETs) are available to everyone. Other technology applications allow people to choose privacy settings which are tailored to their individual needs.
>
> Privacy is understood differently by each individual.
>
> Freedom of choice and decision-making, as well as transparency in society, is highly valued.
>
> Awareness of the possibilities and disadvantages of emerging technologies is high.
>
> New technologies are treated with openness.

It might be that the above list is not exhaustive but each of those scenarios is feasible and can be reached, particularly when digital natives (usually referred to as those born after 1990) will replace the digital immigrants at the front seat of the governing bodies of our society. This will take place in the next few years. Legislatures and governments should delve and elaborate on those avenues and select what is the preferred direction. The fulfillment of the recommendations that follow should comply with the major question: where do we want to be in terms of privacy in the near future?

For example, if the aim is to achieve scenario 5: "Tailor-made privacy,"[3] some parts of the current trends of technologies need to be changed in the future. For instance, considerable investments are needed to make technologies more transparent. This means that the whole production

[3] Please note that this is not a recommendation to reach Scenario 5, but just an example.

chain needs to be reshaped, and more resources need to be invested to develop technologies towards the concept that they are transparent at an early stage of the development process. Another obvious conclusion would be that societies need to invest more in education. That is one truth, but the other truth is that if the technologies are not transparent, the education loses most of its benefit. An immediate conclusion is that governments need to regulate the development life cycle of an emerging product when it is suspected to be related to privacy maintenance. In order to obtain a future where technology enables people to achieve tailor-made privacy, consumers have to be able to make more informed decisions about whether or not to purchase certain kinds of products on the basis of prior knowledge about the possibilities and disadvantages of emerging technologies.

However, the solution is not so simple. Even if technologies such as smartphones were to become more transparent, it would not help to achieve tailor-made privacy because users are sometimes forced to use such devices in contemporary societies. For example, at the moment it is impossible to do most kinds of qualified work, if one does not use a mobile communication device or a computer. One conclusion would be to require the inclusion of privacy settings during the development phase of different technology applications so that people can really choose tailor-made privacy, even though they are forced to use these technologies. This is the guiding principle of the idea of **Privacy by Design**.

The above discussion is just one example of measures required to proceed towards Scenario 5. Similar considerations should be made if another scenario is selected as the goal for our privacy status.

Specific policy recommendations are listed in the next section.

The need for a Basket of Solutions

There is no single magic solution for privacy issues. The complexity of the technologies, the unsolved obscurity of the concept of privacy, and its inter-dependence on social norms and technological developments, means that this is a dynamic field and one that is unlikely to settle down in any near future. This, taken together, renders a panacea solution impossible. Accordingly, the project suggests a basket of solutions, which includes, in addition to some legal proposals, empowerment of individuals by way of raising awareness and education, the use of Privacy Enhancing Technologies (PETs) (for PETs see Burkert, 1997), concepts such as Privacy by Design (PbD) (for Privacy by Design see Cavoukian, n.d.), as well as organizational suggestions, such as adopting the procedures of Privacy Impact Assessments (PIA), and the appointment of Chief Privacy Officers (CPO) within organizations (public and private). Note that each of these avenues does not stand alone.

In order to present the recommendations in an orderly fashion, we clustered them into a number of categories:

1. Technology
2. Law and regulation
3. Organizational issues
4. Education
5. Social issues

Technology

1. Encourage the development and exploitation of Privacy Enhancing Technologies (PETs):

Privacy Enhancing Technologies (PETs) may be regarded as one of the outcomes (or enablers) of PbD. The EC Communication on PET issues a definition of PET deriving from the PISA project – *"PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system."* PETs' classification is based on functionality:

- PETs for anonymization (e.g., TOR software for anonymous web surfing18)
- PETs to protect network invasion (e.g., Latent Semantic Indexing to identify standard users)
- PETS for identity management (Credential systems providing authentication without identification)
- PETs for data processing (privacy preserving data mining)
- Policy-Checking PETs (e.g., EPAL, OASIS XACML – policy specification, organization and verification tools).

There are not very many technologies that can be defined as PET. Some technologies can be exploited both ways – for privacy protection as well as to counter privacy. If the EU adapts the encouragement of PETs as a dominant policy, the EU can benefit economically from that by exporting such technologies to foreign countries.

2. Data Subject's Control:

The fundamental principle is that the data subjects should maintain control of their personal data and the flow of the data from one digital location to another: It is for the data subject to make decisions about whether her/his wishes to share the data, with whom, under what circumstances, when and how. The notion of control reflects the underlying theories of privacy (Westin, 1967) and its ethical basis of human dignity and autonomy.

A possible technical solution for increasing the data subject control over his/her data could be to ***reverse the roles of the data subject and the data collector***: Suppose each individual uploads his/her personal data to a cloud computer that can be accessed by everyone, subject to the subject's authorization. Each organization that wishes to retrieve data about an individual should obtain permission from the data subject to access his/her confined profile. The permission also designates what data items can be fetched from the depository. Consequently, the control shifts from the collector to the data subject.

Law and regulation

3. Privacy by Design (PbD):

PbD is described as a process of "building fair information privacy principles (FIPPs) into information technology, business practices, and physical design and infrastructures." In simple words, each engineering product and each ICT application has to undergo a development life cycle before being put on the shelf. The life cycle is strictly defined by organizations that set standards in various fields such as ISO, PMI, and the like. The life cycle examines many characteristics of the product such as its design, reliability, security, and user friendliness. So far, very little has been done about incorporating aspects of privacy into the life cycle of a technological development. Consequently, the threat to privacy raises as a "surprise" after the product has already been dis-

tributed to the market or the application has been installed on the computer/tablet/smartphone. At that point, it is difficult and expensive to address the privacy needs.

It is imperative to regulate that privacy considerations be examined during an early stage of the design, namely in the very beginning of the life cycle. This regulation should hold for every field of technology that might have an impact on privacy, in particular those areas such as ICT, Genetics, Nanotechnology, Cognitive and Brain Sciences, and the like. In addition to regulation, education and adoption of PbD voluntarily should be encouraged.

4. Consent:

The consent of the person submitting data to an organization is a critical key of privacy protection. However, it is, at the same time, the weakest link in the chain. Therefore, it should be more innovative and better reinforced in order to make it effective. Some proposals are made:

- First, technological innovations should support a better transparency of the flows of personal data;
- Second, consent should be given for a limited time: people should be able to change their mind and revoke consent;
- Third, consent should be given for categories or classes of service providers according to their concern for the privacy; providers that do not comply with generally accepted privacy requirements should not get the individual's consent;
- Fourth, labels could help this categorization and provide at least better information of people regarding to whom and for what they are giving their consent.

5. Define by law and regulations the right to close the door:

The right to close the door is the ability to enter into a state of non-'reachability' of an individual. At a certain moment, an individual may say "leave me alone. I give up your favors and benefits in return for keeping my privacy." This might prevail for a limited time or regarding a certain set of activities or until a change notice is announced. It relates to ***the right to be forgotten***, now renamed the right to erasure, namely to be deleted from a SNS and other voluntary depositories of data.

6. Define by law and regulations the right to be forgotten:

The requirement for consent and the right to close the door are necessary for privacy protection, but they are not enough. There should be an easy and "friendly" procedure to withdraw from every SNS and voluntary database on which individual's data are recorded. Today, in some SNSs and marketing databases it is almost impossible or very complicated to delete one self's information. It should be enacted that a withdrawal procedure should be clear, easily accessible.

7. Legislation targeting individuals that breach privacy:

Most of the privacy related legislation is directed to limit governmental and business organizations that collect, process, and disseminate data about individuals. However, what about individuals who collect data, distribute it without permission, and open their webpages, list of friends, photographs albums, and the like to the public or to a number of friends, whereas the subjects of those photos or addresses or personal stories and anecdotes have never granted a consent to do so? The area of friends revealing private information about other friends is hardly regulated or legislated. It should be deliberated because, due to the rapid growth of SNS use, the phenomenon poses a strong threat to privacy.

8. Meeting Points:

Today, usually the data subject and the data collector and controller have a meeting point at the first stage, if the data is collected directly from him or her, and if the subject understands the process. However, once the data is collected, the power of the subject to control the use of the data is limited. It is processed by the data controller, those who work for the controller (employees) or with the controller (outsourcing), and those who receive data from the controller, wherever they are located. The legal duties imposed on the data controller—where data protection laws apply—aim to assure that the data subject's rights and interests are not breached later on.

The policy recommendation is to create, by legal and technological means, additional *meeting points* between the individual data subject and the data controller, so to re-empower the data subject, so that he or she can (re)gain control over his or her personal data. These additional meeting points should enable the data subject to have a second and third choice, to make an informed, free decision, or to reverse a prior decision.

9. Define by law and regulations the fundamental principles of individual's rights that prevail in a democratic society:

The fundamental values (principles) are dignity, self-determination, and social justice. These values are threatened by the aforementioned emerging technologies. Therefore, it is required that they be protected by a legal "umbrella".

10. Define by law and regulations the requirements for transparency and proportionality:

The two main principles – ***transparency*** and ***proportionality*** – have to be complied with. Undoubtedly, the emerging technologies challenge these two principles. Therefore, the definition of both should be presented in laws and incorporated into the PbD procedures.

11. Define the roles and broaden the scope of the duties of Data Protection Agencies:

Data Protection Agencies (DPAs) have been established in all EU Member states and in other countries, inspired by the EU. However, their functions, scope of authorization, and enforcement power have not been commonly defined and harmonized among the various countries. Their domains of activity, their rights and authorization should be clarified and enshrined by laws. Governments and the EU should reassure that (1) the DPAs have enough autonomy to fulfill their tasks and that (2) the DPAs are financed well enough to fulfill their tasks. This will also enable coordination among DPAs in various countries, in order to cope better with the non-existence of national borders when it comes to Internet crimes.

12. Labeling and privacy seals:

The term ***labeling*** refers to instituting the requirement to label each pertinent IT product (e.g., smartphone, SNS, computer application) with a label stating its compliance with privacy protection. (This is analogous to the one developed by EU for sustainability, the Eco-Label). Labeling requires the definition of privacy criteria in order to rank the services providers according to their degree of privacy "friendliness". (This is similar to the way automobiles are categorized according to their avoidance of pollution, and food is ranked according to ingredients such as fat, gluten, and others.) It also demands independent experts to evaluate and to rank the providers according to the defined criteria. After the initial labeling, it needs a permanent follow up in order to guarantee the trustfulness of the labels system.

Organizational issues

13. Technology scouting:

Usually, our attention to privacy threats focuses on ICT. However, the report has identified a large variety of technologies that might pose potential threats to privacy. Included among them are nanotechnology and new material development; medicine, biology and biometrics; robotics and cyborg development; cognition ("mind reading"); and ICT. The only way to explore the threats to privacy posed by those technologies (and maybe by some others) is to establish a permanent scouting unit whose main duty would be to identify threatening technologies far in advance of their implementation and proliferation. Such a unit should be composed of a small number of experts specializing in the aforementioned technologies, who are capable of tracing new R&D projects, forecast their outcomes, and ring the alarm when needed. The scouting should be independent and not affected by commercial considerations. (It might be a department within the DPA). Just as an example, imagine how the smartphone technology would look today if ten years ago it was examined for its threat to privacy.

14. Data categorization:

Not every data item is required to have the same degree of privacy protection. For instance, name and address are less sensitive data than political affiliation or medical records. The opinion of the boss about an employee is more sensitive than the job title of the employee. Generally speaking, we can divide personal data into two categories: informative data (e.g., name, address, academic degrees) and evaluative data (e.g., the opinion of a boss, what the teacher is thinking about a student). Evaluative data, in principle, should be treated in a more sensitive way. However, this categorization is too rough and should be much more refined by dividing the organizational and governmental data into layers, where each layer requires a different degree of privacy protection.

15. Chief Privacy Officer (CPO):

Appoint a CPO in each organization in the business, the NGO, and the public sector**s**. The CPO will be on charge of privacy preservation and compliance to privacy laws and regulations. This person will also handle complaints regarding breach of privacy and advise decision makers on privacy related issues. It should be assured that the CPO will be independent in the organization (similar to an internal auditor or to an ombudsman).

Education

16. Education programs towards "safe use of the Internet":

The findings of the student survey indicate a clear and risky trend of adolescents to disregard privacy considerations when they interact online with a so called "friend" over the SNS. The digital natives' perception of privacy is significantly different from that of the digital immigrants. We must assume that the amount of time the young ones spend on SNS (be it via a PC, a laptop, a tablet, or a smartphone) will not decrease in the future, but rather grow significantly. It is already and become more so, an integral part of their lives. Therefore, the most effective way to prevent the "privacy fading out unconsciously" scenario is by education. Law and regulation can be complementary to education but cannot replace it. Appropriate education will encourage the demand for satisfying privacy by way of bottom-up in addition to top-down (namely, regulation).

17. Education of adults in the spirit of "yes we can":

The focus groups show that even for those who value their privacy, as it is the case for most of the non-native people met during the focus group, protecting their privacy is becoming an impossible challenge due to the *digital economy* (personal data versus access to services). The weakness of the *"informed consent"* has been pointed out as one of the most critical difficulties they

experience in their everyday life. It is important to educate adults that they should insist on maintaining their privacy when they wish to, that it is possible to obtain privacy policy from various businesses and organizations and to select privacy preferences, and that they should not surrender to privacy threats believing that there is nothing they can do. They do not have to grant consent when they don't accept the privacy terms.

Social issues

18. Initiation of a "grey ecology":

Explore the potentialities of the initiating a "grey ecology" concept (suggested by Paul Virilio, 1995). The grey ecology will function like the current "green ecology", namely a set of values and standards that maintain a sufficient level of privacy. The grey ecology will orientate the political and industrial authorities towards actions and research which promote "clean technologies" and which are sustainable regarding privacy protection.

19. Reduce privacy divides:

The project indicated that privacy is not equally shared. Some people enjoy more privacy than others – not because of their choice, but for external reasons, such as technological literacy, educational gaps, financial gaps, and the like. These are privacy divides. The recommendation is to study and identify the many causes of privacy divides, so to determine which need to be addressed and how. Based on the findings of such further research, possible policy responses may include:

Raising awareness of privacy issues, so to address divides that are the result of ignorance. The form of raising awareness can range from "soft" avenues of general campaigns, to compulsory forms, such as including the issue in school curriculum.

Providing assistance to those in the need, such as people with disabilities, the elderly, and children.

Simplifying enforcement means so that they are more accessible to more people; adding legal avenues for enforcement on behalf of those who do not access the judicial system. For example, allowing NGOs to sue, or permitting class actions in appropriate cases.

Regulating data controllers' behavior, by requiring them to use simple, easy to understand, ways of conveying information about their data practices. The data collector and controller should invest in additional ways to convey information (such as the use of images, non-textual means).

Mandatory PETs; regulation of prices of technologies. More specifically, the regulation could also require that whenever a traceless technology alternative exists, it must be offered at the same price as the tracing technology.

Conclusion

There is no one "deus ex machine" solution to the threats privacy faces due to emerging technologies such as ICT, Genetics, Nanotechnology, Cognitive and Brain Sciences, and the like. Rather, governments and international organizations (e.g., EU, UN, ITU) should develop and implement a comprehensive strategy and policy and a basket of solutions adhering to technology, law and regulations, organizational issues, education, and social issues. Since the Internet does not recognize national borders, the "toolbox" for privacy protection should be coordinated among nations and continents in order to avoid abuse of privacy by employing lax regulations in another country.

References

Ahituv, N. (2001): *The Open Information Society*, Communications of the ACM, Vol.44, No. 6 (June 2001), pp 48-52.

Boyd, D. (2008): *Taken out of context. American teen sociality in networked publics* (Doctoral dissertation, University of California). Retrieved 07.05.2010 from http://www.danah.org/papers/TakenOutOfContext.pdf

Burkert, H. (1997). Privacy-enhancing technologies: Typology, critique, vision. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 125-142). Cambridge, MA, USA: MIT Press.

Cavoukian, A. (n.d). *Privacy by design* at http://www.privacybydesign.ca

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009): A multinational study on online privacy. Global concerns and local responses. *New Media & Society, 11*(3), 395–416. Retrieved 07.07.2010 from http://nms.sagepub.com/content/11/3/395

Hampton, K. N., Sessions Goulet, L., Rainie, L., & Purcell, K. (2011): *Social networking sites and our lives*. Pew Research Center's Internet & American Life Project. Retrieved 30.06.2011 from http://pewinternet.org/Reports/2011/Technology-and-social-networks.aspx

Ofcom (Ed.) (2008): *Social Networking. A quantitative and qualitative research report into attitudes, behaviours and use*. Retrieved from http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_04_08_ofcom.pdf or http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf

Salaway, G., & Borreson Caruso, J. (2008): The ECAR Study of Undergraduate Students and Information Technology. ECAR. Retrieved 07.05.2010 from http://net.educause.edu/ir/library/pdf/ers0808/rs/ers0808w.pdf

Virilio, P. (1995). La vitesse de l'information *[The Speed of Information]*, In le Monde Diplomatique, http://www.monde-diplomatique.fr/1995/

Westin, A. (1967). *Privacy and Freedom*. Bodley Head Publishers.

Appendix
Scenarios of the PRACTIS High-School Survey

Scenario 1: Rock Concert

A venue that hosts regular rock concerts offers the option to get a personalized electronic bracelet. A Microchip on this bracelet saves the events a customer visits, his favorite drinks, and everything for which he will have to pay, like drinks or maybe food. Those who decide to take this bracelet benefit from different advantages: They get a personalized newsletter and can use separate entrances and separate places to buy their drinks, where waiting times are much shorter than for conventional users as their personal data stored on the bracelet can be compared to information in a database about banned guests and people who are considered as potentially violent. So waiting time when entering the rock concert is reduced as the security check can be done faster. Furthermore clients have the chance to either get a pre-paid account for the venue which is used to pay the bill or to provide the owners of the venue with their bank account data so that the bill can be charged off.

The students were asked (a) if they would use such a bracelet and (b) what motivates them to use it.

Scenario 2: School

The second scenario focused on possible security measures in schools.

At your school lockers have been cracked and robbed, there has been bullying and physical fighting, pupils have been extorting money and there has been vandalism. To improve security the school administration decides to install a technological security system at your school.

Next, several possible measures to enhance security were assessed both with regard to their appropriateness and their effectiveness.

Scenario 3: Shopping

The third scenario addresses RFID technology once again, this time within a shopping context.

A shopping mall introduces a new way of paying. All articles sold in the mall are equipped with microchips so that customers don't have to pay in the single shops. When leaving the mall the tags of the goods a certain customer took are read out and the customer can pay at automated teller machines without having to wait in a line. There is also the opportunity to create a prepaid-account or to allow the shopping mall to charge off the money from your bank account or credit card so that you can just walk out of the mall with your new clothes. To participate in this new way of paying you have to register with your name and email address. All products you buy are stored and the information is used for marketing purposes. You can also register with more detailed information (gender, age, social status, address, etc.) to get personalized consumer information. Furthermore the mall offers a lottery to make their new paying method more popular.

The students were asked (a) if they would use such a paying method, and (b) what makes it attractive to them.

Scenario 4: Public Places

This scenario describes the observation of public places with video surveillance.

The city administration builds a new place, which is meant to serve as a hangout point for local youth. Part of this place is a video surveillance system to make sure that there are no criminal activities, violence, or vandalism.

The questions asked with regard to this scenario were designed to assess the likelihood of students choosing to spend time in this place and, if yes, under what conditions. In addition, students were asked to report their opinions on observation/surveillance in public places in general. Finally, they were asked whether surveillance would potentially deter them from visiting specific places (metro stations, employment agencies, shopping malls, shops, private houses, or public recreation areas).

Scenario 5: PC/Internet

This scenario addresses issues of online security and the perceptions of threat in the Internet. Students were provided with the following scenario description including a screen shot of a pop-up window:

After surfing the web the following window appears on your computer desktop screen informing you that spyware has been detected on your computer. Additionally it proposes a link to download the latest spyware remover software to solve the problem.

Window text: “**Danger: possible spyware infection!** Your PC infected with spyware, adware or similar malicious programs. Please download spyware remover immediately to protect your computer against spyware! Malicious programs can change, damage and delete important system

components, what can cause slower performance, valuable data loss and unstable system operation. Click here to download spyware remover from Security Center web site… **Scan your computer for FREE!!!**"

The students were asked whether they would use the link or not and; if yes, under which circumstances (multiple answers were possible for this question).

Scenario 6: Health Monitoring Sensors

This scenario addresses the use of implantable sensors in the medical area.

In order to improve people's health, new miniature sensors are introduced and given for free. Sensors that are worn on the wrist (or implanted under the skin) continuously measure blood pressure, heat and breathing rate, oxygen and sugar in the blood, temperature, caloric intake, and other health parameters. All these are displayed on your cell phone and are sent to the medical service providers. It helps you to know your health condition and to get better and cheaper medical treatment, including significant discounts for medications if necessary. The same data informs the doctors and your insurance company what and how much you eat, drink, or smoke, and when you go to bed.

Students were asked if they would use such medical sensors. In the questionnaire, students were able to deny the sensor completely or to allow the usage of the sensor under certain given circumstances.

Biographies

Niv Ahituv is the Dean of Dan School of Hi-Tech Studies at the College of Academic Studies. He is a Professor Emeritus at Tel Aviv University. He was the Academic Director of the Institute of Internet Studies and the Marko and Lucie Chaoul Chair for Research in Information Evaluation at Tel Aviv University. From 1999 to 2002 he served as Vice President and Director General (CEO) of Tel Aviv University. From 1989 to 1994 he served as the Dean of Graduate School of Business Administration at Tel Aviv University. In 2005 he was awarded a ***Life Time Achievement Award*** by ILLA, The Israeli Association for Information Technology. He is a member of the Executive Committee of CODATA, an international organization dealing with scientific data sharing. His recent research focuses on Privacy and Technology.

Nicolas Bach is research fellow at the nexus Institute for Cooperation Management and Interdisciplinary Studies in Berlin. He studied philosophy and Eastern European Studies at the Free University in Berlin. In this context he specialised on political, societal and economical transformation especially in the post-communist countries. Besides privacy protection his main fields of research are participatory democracy, civil society, and political and societal developments.

Michael Birnhack is a Professor of Law at the Faculty of Law, Tel Aviv University. He teaches and rights about privacy. Michael was a member of the Israeli Council for the Protection of Privacy, a member of an expert committee for the revision of Israeli data protection law, and sub-contractor to the EU Commission on the adequacy of Israel's data protection law. Currently, he is involved in studies about privacy by design, data leakage from social networks, biometrics, and CCTV in schools.

Tal Soffer, PhD, senior academic staff member at the School of Education at Tel Aviv University. Director of two academic units: Technology and Society Foresight (TSF) and the Center for Web-Supported Academic Instruction - Virtual TAU. She has a Ph.D. in Education and an M.A. in Labor relation from the Tel-Aviv University. She has an extensive research experience of more than 20 years, in the field of Technology Foresight and its relations with societal implications: education and cyber technologies specialization in e- learning, community learning and Life Long Learning; privacy and cyber technologies; future of work and leisure and it's relation to occupations and skills. She has been involved in vast of Israeli and EU research projects as principal investigator such as: Future Opportunities of Middle Triole Pupils, OPET, e-Living, NBIC, SSH-FUTUERS and FESTOS projects; and as coordinator of the ELOST project – e-Government for Low Socio-economic Status Groups and the PRACTIS project: Privacy - Appraising Challenges to Technologies and Ethics. In addition she has consulting experience to policymakers in the Israeli Ministries such as: Ministry of Education, Ministry of Science and technology, Ministry for the development of the Negev and the Galilee and other clients, such as the EU. She is a member in several comities such as: the academic advisory council of World ORT Kadima Mada, FEMIS - Euro-Mediterranean network. She has an extensive amount of publications in Journals and EU reports as well as presentations of papers in conferences papers on various subjects.

Liisa Luoto is a project research in Finland Futures Research Centre (University of Turku). She is currently working with futures studies, which are targeted into the Finnish countryside and young people. She has also worked with issues like security, privacy, and emerging technologies. Her background is in political science and she graduated from University of Tampere in 2011.