Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

FINLAND NATIONAL REPORT

AEDH

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH,EDRi,AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

December 2009

TABLE OF CONTENTS

SYNTHESIS

Methodology

The principle objective of this study is to understand and learn from the current situation with regard to privacy and data protection in Finland. In particular, the aim is to explore practices, technologies and legislations that affect the everyday life of young people and finally to draw some conclusions.
The main questions asked were:

- How are European laws and EU policies relevant to data protection implemented in Finland?
- What are the main risks for data protection in Finland?
- How are young people affected by these risks?
- How aware are young people of these risks?
- What is the role of the Dutch Data Protection Authority in eliminating these risks?
- What are the future challenges in this field?

This study is structured in 4 chapters: Mobility and Transport; Biological identity; Internet and telecommunications; Social Networks.

In order to determine the national situation, the observation method was largely used.
First, we have been supported by our member, the Finnish League for Human Rights as well as its partners and networks, who provided us measurable information on the four topics. We established a long and continuous correspondence with them which enabled us to exchange a lot of information and to confront the different points of view.
Using the observation method, the research panned out to gather data from all possible sources which include books, related internet sites, NGO reports, online newspapers, periodicals, academic publications, government studies, independent studies, papers from seminars and other institutional publications, to give us the widest choice of perspective on the subject area.
The direct communication method was used to conduct a face-to-face interview with two persons: Leena Romppainen, from EFFI and Matti Kari, the Communication manager at Sulaki Dynamoid. Most of the other sources were used to cross-check information, measure public awareness, determine public opinion and criticism.
Even though these sources have provided valuable information pertaining to data protection in Finland, it should however be noted that, as the AEDH worked on 3 countries and the EU, this study and the attached cards are not as thorough as those prepared by the partners working only on their own countries (France, Czech Republic and Spain).
Consequently, for the drafting of the cards priority was given to technologies and practices that have not been dealt with by other countries or that ascertain the main privacy concerns in the Finnish society.

Legislation regarding privacy

In 1988 the first Personal Data File Act came into force, being the first law concerning data protection in Finland. This Act was aimed at prevent violations of integrity at all stages of data processing. The functional objective was to promote the development of, and compliance with, good data processing practices.

On June 1, 1999 the Personal Data Act, which replaced the Personal Data File Act, came into force. The main principles of the protection of privacy remained largely unchanged, but basic rights and fundamental freedoms of individuals were even more strongly emphasised, also in the context of the processing of personal data. The Personal Data Act transposed the European Data protection directive of 1995.
On 1st September 2004 saw the enactment of the Act on the Protection of Privacy in Electronic Communications, which safeguards confidentiality and privacy in telecommunications. It seeks to clarify the rules for processing confidential identification data and to expand their scope to encompass corporate or associate subscribers. The Act on the Protection of Privacy in Electronic Communications repealed the Act on the Protection of Privacy and Data Security in Telecommunications enacted in 1999.
On 1st October 2004, the Act on the Protection of Privacy in Working Life was enacted, which addresses the key data protection issues by creating various procedures for the needs of working life. This new Act includes provisions on drug testing, camera surveillance and electronic mail privacy protection.
In 2009, 'Lex Nokia' (also called the 'snooping law') was passed. It introduced an amendment to the Finnish Act on Data Protection in Electronic Communications from September 2004. It also demolished some of the good privacy standards set by the Act on the Protection of Privacy in Working Life from October 2004. The new law was voted in parliament in February 2009 and came into force in the beginning of June 2009. The law is called 'Lex Nokia' in recognition of Nokia's fervent support for it. This law means a significant set back for privacy and human rights.
The European directive of 2006 on data retention still needs to be transposed as well as the Council regulation of 2004 and the decision of the Commission of 2005, both on standards for security features and biometrics in passports and travel documents issued by members States.

Privacy and Data protection Control Authorities

The Finnish Communications Regulatory Authority (FICORA) is a general administrative authority under the Ministry of Transport and Communications for issues concerning electronic communications and information society services in Finland and it is the national security authority in Finland. CERT-FI, which is a part of FICORA, is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. This body mainly supervises compliance with the Act on the Protection of Privacy in Electronic Communications and any provisions issued under it.
The Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. It guides and controls the processing of personal data and provides related consultation. The Ombudsman exerts power in issues related to the implementation of the right of verification and the correction of personal data. It also follows the general development in the processing of personal data, launching initiatives if necessary. The Ombudsman sees to the distribution of information related to the field of operation and participates in international co-operation. It has to perform its task under the conditions set forth by the privacy legislation. This entity supervises the processing of location data, telephone directories and directory inquiries, compliance with provisions pertaining to direct marketing by means of automated systems and compliance with provisions pertaining to a user's special right of access to information.
The Data Protection Ombudsman has been very active in the information campaign on the travel card.

Privacy Awareness

NGOs are not very active in the field of privacy in Finland. There have all the same been campaigns

that were useful.
For example, whereas the media in Finland reported in a very positive way on the introduction of biometric passports since they consider and represent it as an improvement in the fight against identity fraud, some national NGOs were opposed to that technology. EFFI was planning in 2009 to create a 'stop RFID'-cover for passports to prevent that third party -when carrying the passport- can pick up the signal of the RFID-chip. If successful, EFFI will offer this 'stop-RFID'-cover to other NGOs in Europe. By launching this action, EFFI wants to criticise the introduction of an RFID-chip in European passports by pointing out that they do believe that these passports will be used for illicit purposes by reading them out from a distance.
In a same way, the DPO is also active in a sense that it may acquire attention of citizens by launching debates and critics on a special initiative or law. Indeed, the travel card received heavy public criticism after its introduction when the DPO made public that it was theoretically possible to connect the traveler's identity with travel route information. After all, consumers were ill informed about the nature of the travel card system and the possibilities it opens up. People tend to accept new technologies very easily when they bring forth material benefits without ever reflecting on what could possibly happen with their personal data. The result of the DPO's criticism was that the company that owned the travel card, changed its policy and after a while public debate subsided again.
Also some private companies receive funding from the Government as to lead research on social networking. That's how the owner of IRC Galleria (the most famous social network in Finland) is became the leader of a research on social networks and awareness of people about the risks engendered by that. It raised two main issues: first of all is that parents don't think Internet is important and secondly, teachers in schools don't know much about it, so there is a huge generational gap.
Apparently, a lot of initiatives are going on at the moment about social networks, but everything goes really slow.

The overview

Biometrics: RFID and passports

The technology is applied in the European passports that Finland is issuing since 28 June 2009 for the authentication of the identity of the passport's holder. The stated goal is to protect passports against falsification and to establish a reliable link between the genuine holder and the document.
The risks are known: we don't really know who an access to data stored, who can collect these data…and who therefore can use these data if they are usable. The main risk is to be able to read the chip from distance and thus, use data for illicit purposes.
Apparently, Finland is about to introduce safety measures, such as encryption, to make sure that the data on the RFID-chip can't be read and forged by other parties than the competent authorities and bodies. At the moment, it is still undecided how they will implement this in practice.
One of the good point is that a recent proposal for a Council Regulation introduces a provisional age limit for the retention of fingerprints although following technical considerations, not ethical ones. Children under the age of 12 (rather than 6), next to people who are physically unable to give fingerprints, will be exempt from the requirement to give fingerprints.

Mobility

Every relatively large city in Finland has its own system of contactless smart cards without them necessarily being interoperable with other systems used in Finland It is however intended to standardize these travel cards and strive for interoperability, at least at the national level.
These cards are gathering data about individuals without their consent since the tag can be read from distance. This constitutes a risk for the unauthorised access to and use of the information stored.
As in the Netherlands, paper tickets are available, as well as anonymous card but at a more expensive

price.
About the securisation of the card, we do not really know which data are stored and who can access the data. It has already been used as a tool for a criminal investigation which is not the purpose of the retention. This constitutes a real risk for people's rights. The data could also be used for commercial purposes and for illicit tracking of people.

Private communication

The 'Lex Nokia' law is very frightening since it provides for 'employees' to access and monitor certain data concerning the use of telecommunication services by their 'employees' if they suspect that one of its 'employees' is leaking out corporate secrets and copyrighted materials or is disrupting corporate networks with attachments and malware. However, only "after it has become evident that there is no other way to investigate this suspected leak or assumed disruption". Nevertheless, the law does not specify what exactly is regarded as a 'corporate secret', what 'unauthorised use' means or what constitutes a well-founded reason to suspect one of the above-mentioned cases. Also, the law remains vague on many other important issues and can therefore be interpreted to cover also "corporate subscribers", such as universities, libraries, and even apartment buildings with their own communication network. At the moment the University of Helsinki is considering to introduce this measure. This is however strange, since the law states that it is only possible after reasonable suspicion and when 'no alternatives are possible'; thus not preventatively on a general basis. It is unknown on what basis the University of Helsinki would introduce it.

The risk encompassed in this law is that employers will put their employees under an increasing surveillance scheme, for example by monitoring their browsing history as well, without respecting the right for private life. Moreover, the law is very vague. It should not become a generality.

Social networks

At the moment, IRC-Galleria is by far the largest and most used social networking site in Finland. IRC-Galleria is officially open to anyone who is over 12 years old and speaks Finnish. According to the statistics of IRC-galleria, most of the users are aged between 13 and 22, with the average age being about 20 years. The biggest user group is 16-year-old females. However, the age group above 30 tends to use Facebook.

The main data collected are: name, email address, gender, and other personal data (such as photographs, short messages and comments; each of which is associated with either a picture or a community) or preference information (links, friends' links). The extent to which IRC-Galleria collects information on browser type and IP address of the user is unknown.
Although most of the data are visible to everybody, in principle it is possible to limit photos to certain friend groups, but even then there remains the possibility for others to view them. Also comments are only visible to those who are logged in.

The risks are also know even if it is said that the information placed on IRC-Galleria will not be used for commercial purposes, with the exception of the diversification of advertising. Of course there is a risk that data posted on social networking sites are accessed without authorization (e.g. by hackers), are misused for profiling, can lead to discrimination, etc. Overall, the company claims there are not much problems due to their policy and awareness raising, however, sometimes there are complaints about cyber bulling or stalking but for this reason IRC-Galleria works in close cooperation with the police. That cooperation could constitute a risk since police services could want to access the data for criminal investigations.

Finnish legislation protects users of social networking sites from “character checks” by future employees. Indeed, under Finland’s “Protection of Privacy in Working Life Act”, an employer may only collect information on its employees or job applicants from the employees or job applicants themselves. If "other sources" are used, consent from the employee must be obtained. The Finnish Data Protection Ombudsman ruled in November 2006 that employers can’t use information which is obtained by using Internet search engines, such as Google. The statement was given in response to a job applicant’s complaint that a prospective employer had used a five-year old news group discussion posting found on the Internet to the detriment of the applicant.

IRC-Galleria has 10 paid full-time administrators monitoring the site on inappropriate discussions, pictures, etc. For example, 1 in 1000 pictures is considered inappropriate and deleted; this can be on several grounds: alcohol and tobacco are prohibited to be included on a picture for minors, the same counts for too much nudity. Everybody can tip a given picture on these criteria. The administrators receive a message of this and evaluate whether this is the case. When they agree, they will delete the picture, inform the people involved and can even decide to sanction them by refusing access to their account for 7 days. Both users and administrators react really fast in cases where something is absolutely wrong (e.g. pictures concerning the shooting accident in a school). In cases of real threats, administrators also inform the police (this happened in the past 8 years 20 times).

Recommendations

- No biometric passports with RFID
- Ensure that law enforcement agencies will not get an access to databases storing passports information for law enforcement purposes. The same for commercial purposes with private companies.
- Make sure that consumers maintain a real freedom of choice by allowing for a dual existence of paper and electronic tickets and ensure that both versions are available with the same possibilities as the personalized travel cards and that they are obtainable under fair conditions and under the same price.
- Ensure that people would be informed that their data will be colleted and make sure that they have the possibility to refuse or to give their consent for the collect of their data for the travel card.
- Better securisation of travel cards
- Make sure that during the transposition of the European directives, the definitions, purposes and conditions of data’s collect and retention would not be changed and broadened.
- We would like the University of Helsinki not to implement the ‘Lex Nokia’ law.
- Private companies should not be able to limit a fundamental right as the right to private life for economic interests even if proper guarantees are made.
- IRC-Galleria should not have any exception for the use of personal data in a commercial purpose.
- Lack of awareness campaign. NGOs should more focus on the problem of privacy.

The Data Protection Ombudsman should be allocated more resources and should be granted specific powers as to be able to hear complaints from citizen

1-MOBILITY AND TRANSPORTATION

TRAVEL CARDS

Identification of technology	Travel Cards[1]
Technology used/tool	**Contactless smart cards - RFID** A contactless smart card is usually a plastic card in which the chip communicates with the card reader through RFID induction technology. These cards require only close proximity to an antenna to complete transaction. The standard for contactless smart card communications is ISO/IEC 14443. It defines two types of contactless cards ("A" and "B"), which allow for communications at distances up to 10 cm. Used technologies are: Idesco (low frequency technology), Mifare Classic 1K, Ultralight, Desfire 4K, and Dual Interface cards. The new system will be based on ISO 14443 standards. There are also plans for using modern mobile phone technology in current public transport systems by applying the new Near Field Communication (NFC) technology. NFC is an international standard based on RFID technology.
Country/use area	Every relatively large city in Finland has its own system of contactless smart cards without them necessarily being interoperable with other systems used in Finland (as in other parts of the world). It is however intended to standardize these travel cards and strive for interoperability, at least at the national level.
Frame of use	The technology is applied in electronic travel cards, which are used as the main mode of

[1] The following information is based on an interview with Leena Romppainen from EFFI, (25/06/09), on the report 'Travel cards in Finland', Turku Public Transport Office, 23 april 2009 and on the following links: http://www2.hs.fi/english/archive/news.asp?id=20020919IE4; http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83553; http://www.gizmag.com/go/7320/; http://www.prdomain.com/companies/N/Nokia/newsreleases/200610636271.htm.

	payment for using public transportation in Finland (except for long distance traffic by State Railways). The plans for using Near Field Communication (NFC) technology would enable the use of the mobile phone as a smartcard in ticketing and payment transactions. Passengers would be able to load wirelessly from the network value to their mobile phone (and thus to the travel card on it) and check the balance and history of the travel card.
Population concerned: target and age	It concerns regular users of public transportation. Paper tickets are only available for simple journeys and at a higher price.
% of users/of young users	No specific numbers.
Trends (measured/supposed)	At the moment, the number of electronic travel cards in use throughout Finland is almost 2 million[2].
Known or potentials dangers/Risks	The use of contactless smart cards on this scale presents a risk for privacy, since it offers a range of new possibilities for tracing the movements of people using them. Next to this, there is also a problem with the securitisation of the information stored on such cards which makes it possible to gather sensitive data about an individual without their consent since the tag can be read at a distance without the knowledge of the individual. Using a simple commercial reader, one can often read all the electronic information stored on the smart card. After all, the security of these cards is usually minimal since these cards are expected to be profitable. Therefore, it is easy to hack them and certain research groups at universities have done this regularly to demonstrate the security problem.
Others	Although paper tickets or anonymous travel cards are still available, it is difficult for customers to opt out of the electronic travel card system since this is made the most economical choice.
Generated data bases	
Associated data base/creation	The application for and use of travel cards is recorded in a central database of the respective transportation company (e.g. the Helsinki Metropolitan Area Council (YTV), Helsinki City Transport, and the railway company VR). The massive computer system includes card readers and sensors in each public transport vehicle. The system constantly collects information into a gigantic database, recording an estimated 2.5 million events each day[3].
What justifies the inscription in the file/Risks?	The application for and use of an electronic travel

[2] Report 'Travel cards in Finland', Turku Public Transport Office, 23 April 2009.
[3] http://www2.hs.fi/english/archive/news.asp?id=20020919IE4.

	card.
Purposes/contents, main data included/Risks?	The information is stored in a central database for managing the Travel Card System and to aid transport capacity planning. The main data that are included at the moment are unknown, in the beginning they retained at least information on the travel periods, the amount of money a passenger has uploaded, where the card was last used, the social security numbers of the customers, etc.; thus making the illicit tracking of people possible. For example, YTV had designed a data system that recorded individual journeys first in the system's remote readers and then in its central system. The system also recorded personal data, including each cardholder's social security number, unless they opted for an anonymous card, which however is more expensive. After complaints of the Data Protection Ombudsman, YTV has modified its system so that journeys made by private individuals are no longer stored. Nevertheless, there was decided that YTV does have the right to use social security numbers since it needs them to verify cardholders' domiciles because different municipalities in the YTV region participate in the maintenance of public transport in different ways.
File masters? Risks?	The partners in this project are the Helsinki Metropolitan Area Council (YTV), Helsinki City Transport, and the railway company VR. A company called Buscom is responsible for issuing the smart cards, but another company will take over this task in the near future.
Who accesses the files/ Sharing of the database? Access limits? /Risks	Unclear, although employees of YTV municipal service points and the people in charge of the Travel Card System have the right to browse and update the customer data recorded in the system, as well as the data stored in the central processing unit. However, it is not possible to browse the travel data at the point of service. The data from the Travel Card System have already been used for crime investigations in serious cases. There is however the risk of an increased use of this information by public authorities without the proper checks and balances being installed; thus allowing for a gradual evolution to an authoritarian State.
Data retention period/risks Right to be forgotten	The information will be stored in the database for six months.
Rights to know or to modify data?	Unknown.
Covert purposes/Risks/uncontrolled future evolution	There is a risk that the information stored in the database will also be used for commercial

	purposes. The data from the Travel Card System have already been used for crime investigations in serious cases. There is however the risk of an increased use of this information by public authorities without the proper checks and balances being installed; thus allowing for a gradual evolution to an authoritarian State.
Others (interconnections…)	/
Legislation in application	
Law/rules/others (?) (implemented for this data base or this technology)	Presumably, the general Finnish privacy law, the Personal information law, from 22 April 1999 applies.
Risks for freedoms despite the law	The illicit tracking of people and the unauthorised access to and usage of the information stored on these travel cards.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen.
Conformity with the European right (Charter of fundamental rights, directives…)	
Implementation (or not) of the legislation?/Risks	
Others	/
This tools and young public or young adults	
How far are young people concerned?	The travel card received heavy public criticism after its introduction since it was theoretically possible to connect the traveler's identity with travel route information. After the Data Protection Ombudsman made the issue public, YTV changed its policy. However, debate subsided and in the future the system will be changed as well since the original company that provided for the cards will cease the activity and another company will take over.
Awareness of issues or of risks	The Data Protection Ombudsman has criticized the way YTV has informed the public about the nature of the new card system and the possibilities it opens up. However, thanks to his public critique a lot of people were informed about the issue although later on the public debate subsided.
Indifference or reaction	After a while, public debate subsided.
Awareness campaigns/results	The Data Protection Ombudsman tried to raise awareness and tried to influence the policy of certain transport companies for the better.
Good practises	/
Campaign to be led. On which themes?	/
Others	/
Conclusions	There is a risk that traveling with paper tickets leads to a poor service package and sometimes such cards are not obtainable under fair conditions. After all, transport companies try to

	pressure customers into electronic travel cards by setting high prices for anonymous ones and customers are not well enough informed about the travel cards for them to give a deliberate and informed consent. Also, there have been many problems with the securitization of the data on OV-chip cards. The security of these cards is minimal since they are expected to be profitable. The result is that not only people can travel free of charge, but also with the balance of others using a hacked chip. Off course, sensitive personal information can be gathered as well without the knowledge or consent of the person involved. Finally, the use of contactless smart cards on this scale presents a risk for privacy, since it offers a range of new possibilities for the illicit tracking of the movements of people using these cards.
Recommendations	Make sure that consumers maintain a real freedom of choice by allowing for a dual existence of paper and electronic tickets and by making sure that anonymous versions are available with the same possibilities as the personalized travel cards and that they are obtainable under fair conditions. Last but not least, provide for adequate security measures.

2-BIOLOGICAL IDENTITY

EUROPEAN PASSPORTS

Identification of technology	**European passports**[4]
Technology used/tool	**Fingerprinting & RFID** The European passport will contain two fingerprints, one of the left and one of right index finger. The RFID-chip required by the ICAO, and agreed on by comitology procedure, must conform to ISO/IEC 14443 A/B, which means that it is an active RFID tag, but with a maximum reading range of less than 10 cm.
Country/use area	It is used throughout Finland (as in the other European Member States).
Frame of use	The technology is applied in the European passports that Finland is issuing since 28 June 2009 for the authentication of the identity of the passport's holder. The stated goal is to protect passports against falsification and to establish a reliable link between the genuine holder and the document.
Population concerned: target and age	It concerns every European citizen, without an age limit, under the principle of 'one person, one passport'. However, children under the age of 12 (rather than 6), next to people who are physically unable to give fingerprints, will probably be exempt from the requirement to give fingerprints.
% of users/of young users	It concerns 5,3 million Finnish citizens.
Trends (measured/supposed)	The number of passports with an RFID-chip and fingerprints is relatively low since they are only being issued since 28 June 2009, but their number will likely increase rapidly as citizens renew their passports.
Known or potentials dangers/Risks	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when

[4] The following information is based on an interview with Leena Romppainen from EFFI, (25/06/09).

	proportional in relation to the purpose, and with the utmost care. By combining several data sets (e.g. personal information when applying for a passport, location data from the RFID-chip, etc.) with biometric data, one can create a very detailed picture of a given person without the knowledge or consent of this person. After all, biometric data reveal al lot more information than strictly necessary for the identification purpose. Moreover, the choice of the Council for an RFID-chip raises the concern that this information will be used for other purposes as well since the possibility to read an RFID-chip from a distance is the sole object of this technology. If this wasn't the intention in the case of the European passports, than why didn't the Council of the European Union choose for another, less invasive technology? RFID-technology provides a way to know the presence of a passport's bearer at a given time and place, thus raising the traceably problem. Also, the distance of which the signal can be read does not only depend on the RFID-chip in question but also on the antenna used to receive those signals. Finally, the encryption measures (e.g. a Basic Access Control and Secure Messaging mechanism) that some Member States will take to secure the information stored on the RFID-chip can easily be countered, which has been proven already by many researchers in various Member States that use already RFID passports.
Others	Finland will probably introduce safety measures, such as encryption, to make sure that the data on the RFID-chip can't be read and forged by other parties than the competent authorities and bodies. At the moment, it is still undecided how they will implement this in practice.
Generated data bases	
Associated data base/creation	Finland decided to introduce this measure by using a central database in which the personal and biometric data of the citizens that apply for a European passport will be stored. Other Nordic countries however are deciding not to store this information. Perhaps, Finland will follow their example later.
What justifies the inscription in the file/Risks?	The application for a European passport.
Purposes/contents, main data included/Risks?	The stated goal is to protect passports against falsification and to establish a reliable link between the genuine holder and the document. The main data included are personal data (the standard passport information such as name, address, date and place of birth) and biometric

	data (the fingerprints of the right and left index finger and a digital facial image). However, a recent proposal for a Council Regulation introduces a provisional age limit for the retention of fingerprints following technical considerations, not ethical ones. Children under the age of 12 (rather than 6), next to people who are physically unable to give fingerprints, will be exempt from the requirement to give fingerprints.
File masters? Risks?	Unknown.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Unknown. In October 2008 a law was passed in Finland stating that the information stored in the national database for the issuing of European passports may also be used for other purposes, for example the identification of people in road accidents.
Data retention period/risks Right to be forgotten	Unknown.
Rights to know or to modify data?	Unknown.
Covert purposes/Risks/uncontrolled future evolution	In the future, law enforcement agencies probably will be able to access these data for law enforcement purposes.
Others (interconnections…)	The Finnish DPA will probably monitor this national database. In case of infractions, they can ask to resolve the problem by threatening with fines that are quite high or with court actions based on their right for injunction. The Finnish DPA can work fairly independent and feels satisfied with their powers to monitor the lawful processing of personal data.
Legislation in application	
Law/rules/others (?)	Council Regulation 2252/2004/EC of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [OJ L385, 29/12/2004] and Commission Decision of 28 February 2005 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.
Risks for freedoms despite the law	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. By combining several data sets (e.g. personal information when applying for a passport, location data from the RFID-chip, etc.) with biometric data, one can create a very detailed picture of a given person without the knowledge or consent of this person. After all,

	biometric data reveal al lot more information than strictly necessary for the identification purpose. Moreover, the choice of the Council for an RFID-chip raises the concern that this information will be used for other purposes as well since the possibility to read an RFID-chip from a distance is the sole object of this technology. If this wasn't the intention in the case of the European passports, than why didn't the Council of the European Union choose for another, less invasive technology? RFID-technology provides a way to know the presence of a passport's bearer at a given time and place, thus raising the traceably problem. Also, the distance of which the signal can be read does not only depend on the RFID-chip in question but also on the antenna used to receive those signals. Finally, the encryption measures (e.g. a Basic Access Control and Secure Messaging mechanism) that some Member States will take to secure the information stored on the RFID-chip can easily be countered, which has been proven already by many researchers in various Member States that use already RFID passports.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Council Regulation 2252/2004/EC and the Commission Decision of 28 February 2005 needed to be transposed. This means a significantly set back for privacy and human rights
Conformity with the European right (Charter of fundamental rights, directives…)	On European level, there is also no specific legislation for the use of biometrics; only general rules for the protection of personal data apply. The European biometric passports clearly do not comply with the conditions of finality, proportionality and necessity of article 8 ECHR. Moreover, the choice of the Council for an RFID-chip raises the concern that this information will be used for other purposes as well. After all, RFID-technology provides a way to know the presence of a passport's bearer at a given time and place, thus raising the traceably problem. Also, under the current EC Treaty, the Council had no competence to harmonise provisions on passports, according to Article 18 EC. The fact that Regulation 2252/2004 was enacted without co-decision of the European Parliament and the possibility to modify the Regulation provisions by comitology procedure, and thus without democratic oversight, makes it all the more problematic.
Implementation (or not) of the legislation?/Risks	As of 28 June 2009 every new passport issued by Finland contains an RFID-chip with 2 fingerprints of the right and left index finger as well as a

	digitalized picture of the face, as requested by the European Regulation.
Others	/
This tools and young public or young adults	
How far are young people concerned?	Unknown.
Awareness of issues or of risks	The media in Finland reported in a very positive way on the introduction of biometric passports since they consider and represent it as an improvement in the fight against identity fraud. It is unknown whether or not Finnish citizens are aware of the issues and risks of biometric passports.
Indifference or reaction	Unknown.
Awareness campaigns/results	Some national NGOs are opposed to the biometric passports and for example the organisation EFFI has plans to create a 'stop RFID'-cover for passports to prevent that third parties -when carrying the passport- can pick up the signal of the RFID-chip. If successful, EFFI will offer this 'stop-RFID'-cover to other NGOs in Europe. By launching this action, EFFI wants to criticise the introduction of an RFID-chip in European passports by pointing out that they do not believe that these passports will not be used for other, illicit purposes by reading them out from a distance. After all, the possibility to read the chip from a distance is the sole object of this technology.
Good practises	/
Campaign to be led. On which themes?	The 'stop RFID'-cover campaign (see above).
Others	/
Conclusions	Biometric data are very sensitive data since they contain the unique body traits of a given person. Therefore it is of the utmost importance that the processing and storing of such sensitive data only happens when absolutely necessary, when proportional in relation to the purpose, and with the utmost care. The European biometric passports clearly do not comply with the conditions of finality, proportionality and necessity of article 8 ECHR. Moreover, the choice of the Council for an RFID-chip raises the concern that this information will be used for other purposes as well. After all, RFID-technology provides a way to know the presence of a passport's bearer at a given time and place, thus raising the traceably problem.
Recommendations	No biometric passports with RFID.

3-INTERPERSONAL COMMUNICATIONS

TELECOMMUNICATION SERVICES

Identification of technology	**Telecommunication services**[5]
Technology used/tool	**(Mobile) phone and IP-based telecommunication services** (such as email, VoIP, instant messaging)
Country/use area	Finland (as the rest of the world)
Frame of use	For the transmitting of information in a quick and easy manner to people residing elsewhere without having to move itself (physically). Most people use it on a daily basis for different purposes in their private and professional life.
Population concerned: target and age	Nearly everyone uses it, especially youngsters.
% of users/of young users	No specific numbers
Trends (measured/supposed)	The applications of telecommunication services keep increasing; at the moment it has become very difficult to nearly impossible to take part in the (Finnish) society without using those services. According to the 2009 ENISA report6, ICT in Finland is performing strongly and the country is a leader in information society developments in all respects. It also has one of the most competitive and dynamic ICT sectors in the EU. Skill levels are high both in the workforce and throughout the population.
Known or potentials dangers/Risks	Since telecommunication services are increasingly interwoven in our daily lives and

[5] The following information is based on an interview with Leena Romppainen from EFFI, (25/06/09) and the following links: http://www.theregister.co.uk/2009/03/06/finland_nokia_snooping/; http://www.express.be/business/nl/hr/finland-countert-bedrijfsspionage-met-lex-nokia/104081.htm; http://www.edri.org/edri-gram/number6.24/nokia-law-finland-snooping; http://www.hs.fi/english/article/%E2%80%9DLex+Nokia%E2%80%9D+gets+blessing+from+Constitutional+Law+Committee/1135241092046; http://www.hs.fi/english/article/Legal+experts+say+%E2%80%9CLex+Nokia%E2%80%9D+violates+constitution/1135241264898.

[6] http://www.enisa.europa.eu/doc/pdf/Country_Pages/Finland.pdf.

	since telecom operators and internet service providers (ISPs) register (although temporarily) most of the log data of these communications, there is a risk of an invasion to our right to privacy and of a limitation of our autonomy. After all, individual choices are registered and can be passed on to third parties (such as governments). Also according to the ENISA 2009 report, general IT developments clearly impact on network and information security. In general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more network and information security gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats. In short, an individual's online security risk increases in parallel with the time he or she spends online. However, Finland is very active in fighting against the spread of any kind of malware, and despite the increasing number of broadband customers it managed to reduce considerably the number of such incidents during the last two years.
Others	/
Generated data bases	
Associated data base/creation	a) The database retained by every telecom operator and ISP operating in Finland. b) The database to be retained (presumably by the telecom operators and ISPs operating in Finland) when the European data retention directive (2006/24/EC) will be implemented. c) 'Employers' can access and monitor certain data concerning the use of telecommunication services by their 'employees'. It is however unclear whether 'employers' also can register these data in a database.
What justifies the inscription in the file/Risks?	a) The fact that the data are necessary for the good operation of the communication network, to justify the amount of a given invoice, or when requested by the customer. It is also possible to retain data when these are needed for a market research when telecom operators and ISPs have the prior consent of the customers, although the latter is not always the case in practice. b) The fact that a European Directive requires those data to be retained although national member states tend to use this obligation to ask telecom operators and ISPs to retain additional data. c) The suspicion of an 'employer' that one of its 'employees' is leaking out corporate secrets and

	copyrighted materials or is disrupting corporate networks with attachments and malware “after it has become evident that there is no other way to investigate this suspected leak or assumed disruption”. However, the law does not specify what exactly is regarded as a ‘corporate secret’, what ‘unauthorised use’ means or what constitutes a well-founded reason to suspect one of the above-mentioned cases.
Purposes/contents, main data included /Risks?	a) The prior reason to keep a database for telecom operators and ISPs is to ensure the smooth running of the communication network and services. Next to this, it is also meant as a service to the customer by allowing him/her to verify the invoice. However, there is a risk that these data are abused for commercial purposes, such as direct marketing, without the explicit consent of the customer. The main data included are traffic and location data (such as caller, recipient, date, time and duration of a given call/SMS/email, the technology used (phone call, SMS, email, VoIP), etc.) combined with the information needed to identify the regular user (e.g. name, address for invoice, bank account). b) The stated goal on European level is to ensure the retention of traffic and location data for the investigation, detection and prosecution of serious crime, although the usefulness and necessity thereof have never been proven. Finland hasn’t yet transposed the data retention directive in national law. As the European Directive is very vague, there is a risk that they will retain more data (however, the current law proposal does not contain an extension to for example web activity logs or banking data in contrast to other member states) than requested by the European Union and that they will broaden the scope for access to the data (exactly what constitutes as ‘serious’ crime?). However, the main data to be included in the database will also be traffic and location data (such as caller, recipient, date, time and duration of a given call/SMS/email, the technology used (phone call, SMS, email, VoIP), etc.) combined with the information needed to identify the regular user (e.g. name, address for invoice, bank account). Importantly, this database needs to be kept separate from the first one, thus obliging (presumably telecom operators and ISPs) to a dual storage of these data. c) The stated goal is to prevent corporate secrets

	leaking out, copyrighted materials being copied or corporate networks being disrupted with attachments and malware by allowing 'employers' to investigate the electronic communications of their 'employees' if the company has reasons to suspect that such things are happening. The main data that are included are the log data of employees' emails (i.e. the names of the sender and recipient, the time the email was sent and name and size of attachment) or other IP-based telecommunication services (such as Internet telephony and instant messaging). However, the employer would not be allowed to read the content of the messages.
File masters? Risks?	a) The respective telecom operator and ISP operating in Finland. b) Not yet decided, but the current law proposal refers to the telecom operators and the ISPs. c) Unclear, presumably the 'employers' since they use their own corporate networks. However, the law remains vague on many important issues and can therefore be interpreted to cover also some "corporate subscribers", for example universities, libraries, and even apartment buildings with their own communication network. At the moment the university of Helsinki is considering to introduce this measure. This is however strange, since the law states that it is only possible after reasonable suspicion and when 'no alternatives are possible'; thus not preventatively on a general basis. It is unknown on what basis the university of Helsinki would introduce it.
Who accesses the files/ Sharing of the database? Access limits? /Risks	a) Telecom operators and ISPs have access to their respective database (see above). There is a risk that they sell their data to third parties for commercial purposes. Law enforcement agencies can demand certain data from telecom operators and ISPs when they have a court order (unless it is very urgent, but then they need to confirm the court order later). This is only possible if the maximum punishment for a suspected crime is at least four years imprisonment. However, there are some exemptions: for example the communications between the suspect and his lawyer, priest, doctor, nurse, social worker, and psychologist can't be monitored. A court order is valid for 1 month and it is necessary to specify which particular service will be monitored. Also, the police needs to keep records on their surveillance activities. b) Not yet decided, but the current law proposal

	refers to law enforcement agencies provided that they have a court order (e.g. the same conditions as under point a). c) 'Employers' can access log data only after it has become evident that there is no other way to investigate a suspected leak or an assumed disruption. However, the law does not specify what exactly is regarded as a well-founded reason to suspect such a case. This way, private companies have more coercive powers than law enforcement authorities and they would be able to use them without the need for a court order.
Data retention period/risks Right to be forgotten	a) Telecom operators and ISPs may retain logs for a maximum period of three years for either business (invoicing, marketing) or data security-related tasks; there is also a minimum retention period for traffic data of three months for invoicing purposes. However, apart from the retention for invoice purposes, traffic and location data must be stored in such a manner that they can no longer be traced back to the communicating individuals. b) Not yet decided, but the current law proposal speaks of 12 months. c) It is unclear whether this information will be stored in a database and if so, for what period.
Rights to know or to modify data?	a) Customers receive a monthly invoice that they can challenge and they can always ask their operator or provider what kind of data is retained on them and ask for modification. However, as long as people are not informed about the processing of their data (e.g. in cases of direct marketing without prior consent), they can't exercise their rights such as the right to modification or deletion of their data. b) Not yet decided. c) Unknown.
Covert purposes / Risks / uncontrolled future evolution	a) Direct marketing, spam, the unauthorised transferring (e.g. selling) of sensitive information to third parties etc. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) The government acting as an authoritarian State, placing every citizen under surveillance, thus limiting autonomy and fundamental rights. If telecom operators and ISPs need to retain such a huge amount of data, certainly if they will not be remunerated for it, they will not be very keen on installing high (and thus expensive) security mechanisms to prevent security breaches and unauthorised use. In the worst-case scenario they

	will even be tempted to do something lucrative with it. c) Private companies can limit fundamental rights without proper guarantees. Economic interests are placed above fundamental human rights. Also, opponents claim that if one would really want to leak out corporate secrets the measures introduced are easily to circumvent, for example by using a personal email account. Therefore, opponents fear that employers from now one will put their employees under an increasing surveillance scheme, for example by monitoring their browsing history as well.
Others (interconnections…)	/
Legislation in application	
Law/rules/others (?) (implemented for this data base or this technology)	a) The general Act on Data Protection in Electronic Communications from 2004 applies. The act clarifies rules for processing confidential identification and location data, and provides new means to prevent spam and viruses. The Coercive Criminal Investigations Means Act regulates access to the data by law enforcement agencies. b) The law transposing Directive 2006/24/EC is still in preparation. The Coercive Criminal Investigations Means Act and the law on telemonitoring will regulate access to the data by law enforcement agencies. c) 'Lex Nokia' or the 'snooping law' was voted in parliament in February 2009 and came into force since the beginning of June 2009. The law introduces an amendment to the Finnish Act on Data Protection in Electronic Communications.
Risks for freedoms despite the law	a) Direct marketing, spam, the unauthorised transferring (e.g. selling) of sensitive information to third parties etc. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) An invasion to privacy and the risk of an authoritarian or Big Brother state. There is also a risk that if telecom operators and ISPs need to retain the data, certainly when they will not be remunerated for it, they will not be very keen on installing high (and thus expensive) security mechanisms to prevent security breaches and unauthorised use. In the worst-case scenario they will even be tempted to do something lucrative with it. c) Private companies can limit fundamental rights without proper guarantees. Economic interests are placed above fundamental human rights.

If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	a) Not foreseen. b) Legislation in progress due to European Directive 2006/24/EC. This means a significantly set back for privacy and human rights. c) This law is called 'Lex Nokia' in recognition of Nokia's fervent support for it. After all, in 2006 prosecutor Jukka Haavisto announced that Nokia had been illegally monitoring contact information of its employees' e-mail from 2000 to 2001 and Nokia would have threatened the Ministry of Employment and the Union of Salaried Employees to leave the country if a new law on the protection of electronic communications was not passed. However, Nokia categorically denies having made such a threat to Finland and states that the old law was problematic as it could be interpreted in different ways. However, the current law means a significantly set back for privacy and human rights.
Conformity with the European right (Charter of fundamental rights, directives…)	b) At the moment there is only a draft law proposal, but since the European Directive is a clear violation of art. 8 ECHR the final law will probably be too. c) Many organisations consider the new law in breach with the right to confidential communication; a fundamental right guaranteed under the Finnish constitution as well as by the European treaty on human rights. For example, the Chancellor of Justice, several law professors and NGOs (such as EFFI) have expressed concerns that this fundamental right will be weakened, while giving corporations excessive leeway. However, the Finnish Constitutional Law Committee stated that the bill was not unconstitutional and that it could be passed as a regular law instead of a special procedure used for constitutional amendments. Also, they claim that the economic significance of corporate secrets is so great that it would be appropriate to restrict fundamental rights in order to safeguard confidentiality even though the authority to significantly limit fundamental rights is being given to private companies, rather than public authorities.
Implementation (or not) of the legislation?/Risks	b) At the moment the European Data Retention Directive isn't transposed yet.
Others	/
This tools and young public or young adults	
How far are young people concerned?	a) Unknown. b) Unknown. c) Unknown.

Awareness of issues or of risks	a) Unknown. b) Unknown. c) Unknown.
Indifference or reaction	a) Unknown. b) Unknown. c) Unknown.
Awareness campaigns/results	a) Unknown. b) Unknown. c) Unknown.
Good practises	a) Unknown. b) Not yet implemented. c) None.
Campaign to be led. On which themes?	a) None. b) Unknown. c) None.
Others	b) The costs of the data retention obligation for the sector and consumers is also an issue of debate, but the available cost estimates are still vague. One of the reasons off course is that the precise scope of the data retention obligation for Internet traffic is unclear. c) Although many organisations consider the new law in breach with the right to confidential communication, Finland does not have a Constitutional Court where opponents can file a complaint against this law. There is only the Constitutional Law Committee which is a parliamentary committee made up of the same political majority as the one introducing the law... and the law was passed with a reasonable majority in parliament (96 in favour, 56 against, with 47 absent from the vote), with only the Green party opposing it.
Conclusions	a) Telecom operators and ISPs operating in the Finland keep a database to ensure the smooth running of their communication network and services. Next to this, it is also meant as a service to the customer by allowing him/her to verify the invoice. However, there is a risk that these data are abused for commercial purposes, such as direct marketing or the unauthorised transferring (e.g. selling) of sensitive information to third parties without the explicit consent of the customer. Also, there is a risk that national security and law enforcement authorities will increasingly ask for such data without the necessary guarantees. b) A general obligation to retain traffic and location data is a serious violation of the right to privacy and it turns 5,3 million Finnish citizens into potential suspects. Also, a general retention obligation disrupts the professional secrecy of

	doctors, lawyers, journalists and clergy, as well as political and business activities that require confidentiality. Moreover, the necessity of it has never been proven and experts question the value of this measure not only because data retention turns out to be unsuited in practice, but also because it imposes a disproportionate financial and practical burden on all parties involved. c) 'Employees' can access and monitor certain data concerning the use of telecommunication services by their 'employees' if they suspect that one of its 'employees' is leaking out corporate secrets and copyrighted materials or is disrupting corporate networks with attachments and malware. However, only "after it has become evident that there is no other way to investigate this suspected leak or assumed disruption". Nevertheless, the law does not specify what exactly is regarded as a 'corporate secret', what 'unauthorised use' means or what constitutes a well-founded reason to suspect one of the above-mentioned cases. Also, the law remains vague on many other important issues and can therefore be interpreted to cover also "corporate subscribers", such as universities, libraries, and even apartment buildings with their own communication network. This law means a significantly set back for privacy and human rights. After all, this law gives private companies more coercive powers than law enforcement authorities, without the need for a court order. Thus, private companies can limit fundamental rights without proper guarantees and economic interests are placed above fundamental human rights. Finally, opponents claim that if one would really want to leak out corporate secrets the measures introduced are easily to circumvent. Therefore, opponents fear that employers from now one will put their employees under an increasing surveillance scheme, for example by monitoring their browsing history as well.
Recommendations	a) A strong supervision of the Finnish Data Protection Ombudsman on the abidance of telecom operators and ISPs with the conditions set forth by the Finnish and European telecommunications laws. Strong competences and means for the Finnish DPO to allow them to do their job. b) No general retention obligation. c) No competence for 'employers' to investigate the electronic communications of their

	'employees'.

4-SOCIAL NETWORKS AND NEW GATE KEEPERS OF COMMUNICATIONS

IRC-GALLERIA

Identification of technology	**IRC-Galleria**[7]
Technology used/tool	**Social network site**
Country/use area	Mainly in Finland, but IRC-Galleria recently also became active in Germany (IRC-Galerie), in Lithuania (ManoGalerija), in Spain (Alacara) and in France, but sometimes under a different name.
Frame of use	IRC_Galleria, which is Finnish for IRC gallery, is the largest social networking site in Finland. It was founded in December 2000 by Tomi Lintelä as a photo gallery for the Finnish users of Internet Relay Chat (IRC). At the moment IRC-Galleria is an interactive service where users can for example post and share their photos and music on their own customized site, join different communities and communicate with people in many ways. Despite all the features, IRC-Galleria is basically a photo gallery and it is not possible to have a user account without at least one accepted image. The maximum number of visible images per user is limited but large (10,000 for VIP users, 60 for regular users), and the so-called default image must contain the face of the user. Communication in IRC-Galleria is based on short messages and comments, each of which is associated with either a picture or a community. Each user can be a member of at most 60 communities. Some of the communities are

[7] http://irc-galleria.net/ The following information is based on an interview with Matti Kari, Communications Manager at Sulaki dynamoid and Leena Romppainen from EFFI, (26/06/09) and on the following links: http://www.sulake.com/irc-galleria/, http://en.wikipedia.org/wiki/IRC-Galleria.

	representations of actual IRC channels, and joining them requires IRC-based identification. Comments are only visible to those who are logged in.
Population concerned: target and age	IRC-Galleria is officially open to anyone who is over 12 years old and speaks Finnish.
% of users/of young users	The company Sulake is the largest internet company in Finland (after them comes Linkedln and then Facebook[8]) and their social network site, IRC-Galleria, is the most popular one in Finland for the age group around 20 years of age. In Finland they have half a million registered users. Most of the users are aged between 13 and 22, with the average age being about 20 years. The age group above 30 tends to use Facebook.
Trends (measured/supposed)	Currently IRC-Galleria is by far the largest and most used social networking service in Finland. More than 850,000 Finns visit the site every week and the service has over 500,000 active members. On an average the users spend close to 20 hours in the service weekly, communicating and interacting with others in their own sub-communities. The site receives an astonishing 1.7 billion monthly page impressions, which makes it one of the most active online communities in the world. Sulake's objective is to launch a new international social networking service based on the IRC-Galleria concept to carefully selected countries. Sulake wants to become a major global player in online entertainment by focusing on virtual worlds and social networking services for different target groups and for different user needs.
Known or potentials dangers/Risks	Overall, the company claims there are not much problems due to their policy and awareness raising (see below). However, sometimes there are complaints about cyber bulling or stalking but for this reason IRC-Galleria works in close cooperation with the police (see also below). Next to this, there have been some problems with incitement to racism after the Danish Mohammed cartoons were published but this is covered by the Finnish blasphemy legislation. Certain members of a Finnish political party with racist tendencies held a discussion on facebook. The police is investing this and it will probably be prosecuted. But sometimes it is difficult to draw a

[8] Sulake also owns a site called "Habbo" which is a sort of 'second life' for young children. The basic package is free which allows children to communicate with another and they can pay for virtual goods and games. Another Finnish social networking site is Kuvake.net, but this site has a tendency to ask for sexy pictures which creates a general negative image on social networking sites in Finland that also becomes problematic for IRC-Galleria although they screen the uploaded pictures on criteria such as too much nudity.

	line as of where law enforcement should be involved to actively prosecute things online.
Others	Basic usage of IRC-Galleria is free, but users have an option to purchase additional services and enhancements (e.g. a VIP-service set). The company also makes profit through advertisement.
Generated data bases	
Associated database/creation	Data submitted by the users and collected by IRC-Galleria.
What justifies the inscription in the file/Risks?	The subscription to IRC-Galleria and thus the consent of the user with the prevailing user conditions.
Purposes/contents, main data included/Risks?	The purpose of the service is to offer a platform for the online sharing of personal data and social contacts. It is also used for advertising and marketing purposes. The main data collected are: name, email address, gender, and other personal data (such as photographs, short messages and comments; each of which is associated with either a picture or a community) or preference information (links, friends links). The extent to which IRC-Galleria collects information on browser type and IP address of the user, and uses cookies on their website, is unknown.
File masters? Risks?	Users submit the data; Sulake dynamoid processes and controls the data.
Who accesses the files/ Sharing of the database? Access limits? /Risks	Profiles and communications on IRC-Galleria are -with a few exceptions- all public. IRC-Galleria was not created to be an anonymous site; for private communications Finnish people use for example MSN messenger. The policy choice to make everything public resides in the conviction that this creates fewer problems. IRC-Galleria also makes it very easy to search for new friends on the basis of criteria such as music preferences. Although most of the data are visible to everybody, in principle it is possible to limit photos to certain friend groups, but even then there remains the possibility for others to view them. Also comments are only visible to those who are logged in. In case of problems, the administrators of IRC-Galleria can retrieve who did or said what. Apart from the information that is visible to all, other information (such as IP-address) isn't shared with third parties unless these are law enforcement agencies and only within the conditions set forth by the law. Nevertheless, the police try to access this kind of information on a weekly basis.

	Finally, the information placed on IRC-Galleria will not be used for commercial purposes, with the exception of the diversification of advertising.
Data retention period/risks Right to be forgotten	Unknown.
Rights to know or to modify data?	Unknown, although IRC-Galleria promotes itself as a privacy friendly SNS, referring for example to the fact that people remain the owner of the information they put online (in contrast to Facebook or Google)
Covert purposes/Risks/uncontrolled future evolution	
Others (interconnections…)	In Finland there are no real other big players in the field of social networking sites, therefore IRC-Galleria is not interlinked with others. However, there are plans to interlink IRC-Galleria with other social networking sites in the future, for example with you tube allowing users to upload videos.
Legislation in application	
Law/rules/others (?) (implemented for this data base or this technology)	No specific legislation was adopted; the general Act on Data Protection in Electronic Communications from 2004 applies. Also the law on the Protection of Privacy in Working Life protects users of social networking sites from "character checks" by future employees. Thus, an employer may only collect information on its employees or job applicants from the employees or job applicants themselves. If "other sources" are used, consent from the employee must be obtained. The Finnish Data Protection Ombudsman ruled in November 2006 that employers can't use information which is obtained by using Internet search engines, such as Google. The statement was given in response to a job applicant's complaint that a prospective employer had used a five-year old news group discussion posting found on the Internet to the detriment of the applicant[9].
Risks for freedoms despite the law	There is a risk that data posted on social networking sites are accessed without authorization (e.g. by hackers), are misused for profiling, can lead to discrimination, etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen.
Conformity with the European right (Charter of fundamental rights, directives…)	
Implementation (or not) of the legislation?/Risks	
Others	/
This tools and young public or young adults	

[9] http://www.linksandlaw.com/news-update49-job-applicants-finland.htm.

How far are young people concerned?	According the IRC-Galleria, young people know very well how to use social networking sites. In contrast, the age group 30+ does not know how to use social networking sites.
Awareness of issues or of risks	IRC-Galleria also provides internet information for parents, since there is a serious generational gap when internet is concerned.
Indifference or reaction	
Awareness campaigns/results	IRC-Galleria tries to educate the people (through educational videos, going to schools) that are subscribing to their services by pointing out some general guidelines such as: "*Are the pictures you are uploading yours or do you have the consent to publish them? Are you aware that everyone can see them, are you sure you can live with the fact that your future employee might see these pictures*", or: "*Would you also hang these photos up on the school board?*" Users have to actively consent to these questions by ticking a box, if not they can't upload a given picture. Other guidelines are: "*Be yourself, don't give your password to others,…*" Also, you have to be at least 12 years old to be able to create an account on IRC-Galleria. They tried to check this by asking the national identity number of subscribers but the Finnish Data Protection Ombudsman told them to stop this since it was not proportionate to check the age of persons through the means of the national identity number, which discloses too sensitive information (even if they did not use that information). Now IRC-Galleria tries to find out what age subscribers have by means of the email used to create an account. In the future they would like to use electronic identity cards (provided by the Finnish government) to check the age when people want to log in and create an account. This way they would be able to better manage age-restricted content and be more flexible for adults. They still need to reflect on how to implement this in a matter that they only receive information of the electronic identity card on a need-to-know basis, i.e. age and not birthday date, let alone address etc. Other than that, IRC-Galleria has a good understanding with the Finnish Data Protection Ombudsman. For their work on media education, Sulake receives funding from the Minister of education. IRC-Galleria also cooperates with other organisations to educate young adults, but there are 2 main problems: parents don't think internet is important and teachers in schools don't know

	much about it, so there is a huge generational gap. IRC-Galleria thinks the best way to handle this is to introduce this kind of awareness raising as an obligatory course in the general education package, but then again, Sulake points out that there is also a generational gap with the minister of education. There are a lot of initiatives going on, but everything goes really slow.
Good practises	IRC-Galleria has 10 paid full-time administrators monitoring the site on inappropriate discussions, pictures, etc. For example, 1 in 1000 pictures is considered inappropriate and deleted, this can be on several grounds: alcohol and tobacco are prohibited to be included on a picture for minors, the same counts for too much nudity. Everybody can tip a given picture on these criteria. The administrators receive a message of this and evaluate whether this is the case. When they agree, they will delete the picture, inform the person involved and can even decide to sanction them by refusing access to their account for 7 days. Both users and administrators react really fast in cases where something is absolutely wrong (e.g. pictures concerning the shooting accident in a school). In cases of real threats, administrators also inform the police (this happened in the past 8 years 20 times). Also, there is a police unit active in IRC-Galleria which goal is to be easily accessible for young adults when they encounter problems online. It concerns a team of policemen in a station nearby the head quarter of IRC-Galleria that can be contacted online (for example in a case of stalking). It is very successful and the unit has already enlarged in personnel because of the amount of cases they receive. Both the police as IRC-Galleria are pleased with the cooperation. Before this cooperation started, the administrators had to solve all kinds of problems, for example bullying, but this wasn't always easy since these kind of problems usually go on in real life and off course policemen have more competences to treat such cases (for instance to visit a school and question the persons involved). Finally, IRC-Galleria (and Habbo; a site of Sulake for young children) also provides a platform to the project *Netari.fi*. This is a project launched by the City of Helsinki Youth Department since 2004 to carry out and develop national youth work performed over the Internet. The project's target is to make contact with that section of youth who spend a large part of their time in various Internet

	environments. Netari makes it possible for young people to have real-time conversations both with other youths and with trained youth work professionals. These youth work facilities are open six nights a week. Approximately 120,000 young people are estimated to have visited Netari during 2008. Through multi-professional cooperation, the project aims to lower the threshold for those youths using the facility to seek social and health services when necessary. The Internet seems to be a low barrier for shy Fins to talk about their problems since there is no judgement and a peer support network. The police will also contribute to this multi-professional environment.
Campaign to be led. On which themes?	/
Others	/
Conclusions	IRC-Galleria is at the moment the most popular social networking site in Finland. Overall, the company claims there are not much problems due to their policy and awareness raising. However, sometimes there are complaints about cyber bulling or stalking but for this reason IRC-Galleria works in close cooperation with the police. Next to this, there have been some problems with incitement to racism but this is covered by the Finnish blasphemy legislation. However, sometimes it is difficult to draw a line as of where law enforcement should be involved to actively prosecute things online.
Recommendations	