Personal Data Protection

Coordinator **LDH** Ligue des droits de l'Homme

Partners **AEDH – EDRI – IURE - PANGEA**

France national report
LDH

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

CONTENTS

General synthesis

Methodology

To carry out its study of the four personal data protection topics selected at the February 2009 kick-off, LDH used the following:

- LDH's "ICT and Liberties" working group, made up of law agents, IT specialists, experts and concerned citizens. The group studies how the use of computers, the internet and ICT in general are a threat to civil rights and liberties;
- work carried out for the LDH conference of 1-2 June 2009, the theme of which was "Surveillance society: privacy and civil liberties;
- LDH's legal department;
- various campaigns in coordination with IRIS (**I**maginons un **r**éseau **i**nternet **s**olidaire – *The dream of a community-focused network*), unions (representing judges, lawyers, doctors, tax employees) to fight projects which attack individual freedoms;
- a Senate information report entitled "*La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information"* (Computer data storage and individual privacy: fostering confidence between citizens and the information society), released to the public on 3 June 2009;
- the annual report of the Forum des droits sur l'internet (the Internet Rights Forum);
- the Next Generation Internet Foundation's (FING) report;
- interviews with experts, including Alain Weber (lawyer), Dominique Cardon (sociologist) and Christophe Aguitton (researcher and union activist);
- a National Assembly information report entitled "Fichiers de police: les défis de la République" (Digital police data filing: national challenges).

Based on the pre-selected topics, subjects were chosen by a project monitoring committee. The factsheets were developed using interviews, information contained in the various documents, legal databases and information published online. Upon their completion, the factsheets were reviewed by the legal department.

Legislation and regulation regarding Privacy

Historical background

Protecting rights and freedoms is a longstanding tradition in France, where the 1789 Declaration of the Rights of Man appears in the preamble to the country's constitution.

In 1977, a project emerged to protect privacy and personal data through legislation and the creation of a new institution (the first independent authority of its kind). The **C**ommission **n**ationale de l'**i**nformatique et des **l**ibertés (CNIL) (French Data Protection Authority) was created under Act No.78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties. It is the culmination of a struggle initiated in 1974 against the creation of the GAMIN database (an automated database of children's medical files), which recorded the medical and social handicaps of children reported by children's medical services and made it possible to identify "high-risk categories". It was also in reaction to the creation of the SAFARI database, which linked all public files to create centralised profiles of individuals based on combined information from various government services. The idea of centralized profiling, already studied under the Vichy regime, was brought back to the table just when newly-emerging information technology was perceived as a precursor to Orwellian excesses.

Legislation

ACT NO. 78-17 OF 6 JANUARY 1978 ON DATA PROCESSING, DATA FILES AND INDIVIDUAL LIBERTIES (AMENDED IN 2004)

Although based on general, universal and timeless principles, the Act of 6 January 1978 could not have foreseen the spectacular expansion of information technology. As a result, the text has been amended a dozen times, most recently in August 2004, to ensure its conformity with the 24 October 1995 directive. Under the pretext of compliance, however, the new act eliminated the provision on pre-authorisation. Pre-authorisation gave the CNIL the right to reject the creation of police data files, for example. The new act also eased restrictions on the creation of databases containing sensitive data (biometric, genetic, social, etc.), bringing into question the independence of the CNIL and the true extent of its powers.

Articles 1 and 2 of the 6 January 1978 Act establish a framework for personal data protection. Article 7 deals with prior consent and Article 8 prohibits the collection and processing of personal data that reveals "*the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life*".

Article 1 defines the framework of the law:

Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy, or individual or public liberties.

Article 2 defines what personal data and processing fall under the scope of the law:

Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, storage, adaptation or alterations, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

In chapter II, Articles 6 and 7 set forth the general provisions applicable to personal data:

Intended purpose: data may only be processed for specified, explicit and legitimate purposes.

Relevancy and measure: data must be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Limited retention: data shall be stored for a period no longer than is necessary for the purpose for which they are obtained.

Information must only be shared with authorised recipients and third parties.

Security: The data controller shall take all useful precautions to preserve the security of the data.

Fairness and transparency: Every person shall be informed of the conditions in which data relating to him are used. He is entitled to access these data and to request that they be rectified or even deleted; he may also, under certain conditions, oppose the processing of data related to him.

Combinations: These amount to a new form of processing and call for the application of the principle of intended purpose (and are subject to authorisation).

The role of the CNIL is specified in chapter III (see "Data Protection Authority").

In addition to the 1978 Act, other texts exist which govern personal data protection:

PNR: ***ARTICLE 7 OF LAW 2006-64 OF 23 JANUARY 2006 ON THE FIGHT AGAINST TERRORISM*** authorises the French interior minister to automatically process personal data (PNRs/API) collected during international travel. Article 65 of the French Customs Code authorises customs offices to occasionally collect PNR data from certain flights.

The French Senate, in ***RESOLUTION No. 84 OF 30 MAY 2009*** on the proposal for a framework decision on the use of passenger name records (PNR) for law enforcement purposes (E 3697), voiced numerous reserves and recommended several protection provisions. In particular, it also called for the transposition of the directive to be controlled by law. (See Appendix xx)

Biometric passport: Decrees No. 2005-1726 of 30 December 2005 and No. 2008-426 of 30 April 2008, establishing electronic and biometric passports respectively, were challenged by LDH before the France's Conseil d'Etat (Council of State) on the basis that they violated the principle of measure set forth in the 1978 Data Processing and Individual Liberties Act. (See Appendix xx). Issuing of these passports began in June 2009, despite the case still being under examination.

LAW NO. 2004-575 OF 21 JUNE 2004 FOR CONFIDENCE IN THE DIGITAL ECONOMY (LCEN)

The law of 21 June 2004[1] transposes into French law the European directive of 8 June 2000. The text establishes French legislation on the internet and lays down rules for electronic commerce. Most importantly, the LCEN represents the first general law on the internet. In particular, it:

- defines internet communication by creating new legal categories;
- establishes a liability regime for parties using the internet.

LAW NO. 91-646 OF 10 JULY 1991 ON THE CONFIDENTIALITY OF CORRESPONDENCE VIA ELECTRONIC COMMUNICATIONS SYSTEMS

French law recognises the general principle that correspondence must be confidential. With respect to electronic communication, this principle is enshrined in the Law of 10 July 1991. Published in the Journal Officiel (Official Journal) on 13 July 1991, this law has since been amended several times through both administrative and legislative channels.

As the text points out, "*the confidentiality of correspondence via telecommunications systems is guaranteed by law*. *This confidentiality may only be breached by a public authority in the interest of public safety as defined by and within the limits of the law."* Furthermore, the law defines telecommunications as "*any transmission, emission or reception of signs, signals, writing, images, and sounds or of information of any nature by fibre optics, radio or other electronic systems*."

The text is very general and can therefore be interpreted to include electronic messaging where the correspondence is private in nature.

Developments in legislation

In the interest of enhancing security, there is a trend towards the increased use of ICT to monitor any and all aspects of individuals' lives. Surveillance and generalised suspicion are becoming common.
THE "CREATION AND INTERNET" LAW, KNOWN AS THE "HADOPI" LAW (THE HIGH AUTHORITY FOR THE DISTRIBUTION AND PROTECTION OF CREATIVE WORKS ON THE INTERNET) is designed to protect artists and the entertainment industry from illegal file sharing by internet users.
The law calls for the identification of "hackers" by private firms, copyright holders and producers, who would transmit the IP addresses of suspected hackers to the HADOPI. The HADOPI (the first independent administrative body created to **limit** rights and freedoms) will obtain hackers' addresses from internet service providers (ISPs) and, after a 3-strike procedure, can impose sanctions (denial of internet access, fines, etc.). In June 2009, France's Conseil constitutionnel (Constitutional Council) struck down the provision allowing sanctions to be imposed by an administrative authority, ruling that only a judge may do so.

[1] Source : JurisPedia - http://fr.jurispedia.org

In the new version of the law adopted in September 2009, a judge may suspend a person's access to the internet for a maximum of one year. HADOPI agents are authorised to identify infringements. Internet subscribers found guilty are deprived of their internet connection for one year and cannot subscribe to another provider. Attempts to do so are punishable by a fine of up to €30,000 and two years' imprisonment for violation of a criminal sentence. To claims that an internet subscriber is not necessarily the offender (insecure Wi-Fi access, etc.), the legislator has responded by creating a fine punishing the "blatant negligence" of a subscriber who allows his or her computer to be used for illegal file sharing...
Aside from the numerous technical problems and contradictory requirements posed by the law with respect to ISPs, it also raises issues over the idea of proportionality between privacy infringement (collection of IP addresses and internet access denial) and the protection of property (artistic copyright).

To limit illegal file sharing and protect the interests of a few companies, public authorities are establishing a system of generalised suspicion to monitor people, collect personal data and ultimately jeopardise the right to privacy. Even if it is deemed inapplicable, this law is a threat to the fundamental rights and freedoms of citizens. There is cause for concern that **such an instrument be used for purposes other than to protect creative works on the internet.**

LOPPSI 2, DRAFT LAW ON ORIENTATION AND PROGRAMMING FOR INTERNAL SECURITY

This law, under discussion in early 2010, takes citizen surveillance even further.

In particular, it authorizes the use of cookies by public authorities to access, collect, record, store and exchange computer data without the consent of those concerned and with no judicial control of the legality of these cookies.

The creation of a PERICLES database will bring together all judicial databases and combine available information to fight all forms of delinquency and child pornography in particular. To this end, the database will contain a wide variety of data.

LDH decided to alert public officials of the dangers of this proposal (11 February 2010):

The move towards total social control. The draft LOPSI law represents a significant leap in the construction of a big brother society characterised by suspicion and fear.

Despite being presented as an eclectic catch-all, the underlying logic is clear: the law aims to strengthen, incorporate and concentrate all available profiling, tracing and social control tools, which current governments are demanding on an ever-increasing basis.

The law represents the multiplication of video surveillance systems (even protests are now filmed), despite systematic proof in foreign studies that they are ineffective in most cases; the combination of police databases, despite these being full of errors according to evidence from the CNIL; police filtering of web sites and hunting down of web users, and the creation of a virtual justice system through the systematic use of video conferencing for the hearings of detainees and foreigners held in administrative custody.

Above all, it represents the legalisation of "electronic informers" (cookies) uploaded to personal computers without the knowledge of those being spied on. The PERICLES 'super' database will be able to combine all the information provided by these files, by telephone chips, online bills, identification card numbers, etc.

[…]

The Ligue des droits de l'Homme asks all parliamentary deputies to recognize their responsibilities with respect to the changes in society inherent in this proposal. It asks citizens to refuse to be treated as presumed delinquents subject to constant state surveillance of every corner of their lives.

Data protection authority

THE COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

For the CNIL, "*Information technology must respect the human identity, the human rights, privacy and liberties*".

The Commission National de l'Informatique et des Libertés (French national commission for data protection and civil liberties), or CNIL, was created in 1978 by the French Data Protection and Liberties Act. It is made up of 18 personalities, appointed for five years. Of these 18 personalities, there are four members of Parliament, eight senior officials and six qualified personalities appointed by the French Assemblée nationale (National Assembly), Sénat (Senate) and government. The current chairman is also a senator, which means that he can voice one opinion in the CNIL, criticising bills, and vote differently in the Senate. 120 agents carry out the CNIL's daily missions, constituting a team far too small given its responsibilities.

To meet the objectives set out in the law, namely preventing possible threats that information technology may present to civil liberties and protecting privacy and individual and public liberties, the CNIL may draw on its powers of decision and to impose penalties, as well as its supervisory and recommending powers. In 1978, these powers were used for six primary missions[2]:

- **To grant or refuse authorisation** prior to the creation of personal data processing files;
- **To inform** individuals of their rights and obligations with regard to privacy. The CNIL also provides information on the list of existing files and the processing for which they are declared;
- **To guarantee** the right to access police and military files, for individuals who so request;
- **To monitor** the security of information systems with regard to data processing, for example to ensure the accuracy of data and prevent disclosure to unauthorised persons. The CNIL can impose necessary measures, such as correcting or erasing inaccurate data;
- **To sanction** file managers who do not respect the law, by issuing warnings, formal notices, pecuniary sanctions and orders to stop processing, and even by informing the *Parquet* (public prosecutor) of any violations;
- **To regulate**. The CNIL establishes simplified standards so that the most common processing operations that endanger civil liberties the least are subject to reduced formalities.

But in 2004, when France was obliged to amend the 1978 law to comply with the European directive of 24 October 1995 on the protection of personal data, it modified the CNIL's powers. Consequently, the CNIL can no longer oppose the creation of police files, but merely provide an advisory opinion published in the Official Journal that does not influence whether or not the files are created. Furthermore, the law of 2004 created the *correspondant informatique et libertés* (Data Protection Correspondent), or CIL, profession; companies who appoint an employee to this position are entitled to be exempted from requiring the CNIL's authorisation to implement automated processing for personal data.

In theory, these simplified procedures are compensated for by the attribution of new powers to the CNIL, enabling them to carry out investigations and impose penalties. As a result, the CNIL can impose pecuniary sanctions of up to 300,000 Euros; its investigations, however, are rendered uncertain by a lack of resources.

In his 2008 report, the chairman of the CNIL observed that, from now on, no economic sector and no area of our individual or collective lives will be free from technological development and pressures.
In 2008, 71,990 files were declared, 4,244 complaints were filed, 218 inspections were carried out and 2,516 requests to access police files were received. This represents 116% more than in 2007; 3,500 requests could not be addressed!

Even though 12 jobs were created, the CNIL lacks the resources needed to address the problems posed by video surveillance, bills such as Hadopi, the LOPPSI law on police performance and orientation, social networks, recording personal data on students, implementation of unauthorised files, and police files that contain thousands of errors.

[2] Information based on http://wiki.univ-paris5.fr/wiki/CNIL (French only)

The CNIL believes that barely one-third of the French population is aware of the threats to individual liberties posed by the development of data recording technologies. **Young people make up a considerable majority of the remaining two-thirds of the population that is unaware.**

Citizens have had a reasonable amount of trust in the CNIL for a long time; however, since some of its powers were taken away in 2004, certain civil libertarians found it to be so ineffective that they occupied the building in December 2007.

Associations are requesting that its pluralistic and democratic nature be strengthened, in particular by choosing the six qualified personalities based on proposals from unions and human rights associations.

During its 2009 congress, with particular regard to monitoring citizens, the LDH called for the attribution of supervisory powers to authorities that are truly 'independent' based on their make-up, whose decisions must be made known to citizens and that must have both real legal powers (authorisation powers over government files, intervention and supervisory powers over police and gendarmerie files) and the resources needed to complete their tasks; **it requested specifically that the powers taken away from the CNIL in 2004 be restored to it.**

THE COMMISSION NATIONALE DE CONTROLE DES INTERCEPTIONS DE SECURITE (CNCIS)

The Commission nationale de contrôle des interceptions de sécurité (French national committee for security intercepts control), or CNCIS, is a personal data protection authority responsible for ensuring that the provisions of Title II (on security intercepts) of the law of 10 July 1991 on the confidentiality of correspondence via electronic communications systems, amended multiple times and in particular by the law of 23 January 2006, are respected.

The law of 10 July 1991 states that the confidentiality of correspondence via electronic communications systems is guaranteed, and that this right may not be infringed upon except by the public authority, and then only in the cases of public interest provided for in the law and within the limits established by this law.

Intercepts of correspondences via electronic communication systems are authorised for legal and security purposes.

Under Article 15 of this law, the CNCIS receives claims from private individuals, independently carries out the monitoring and investigation activities that it deems necessary to fulfil its mission, and develops all contacts that may be useful to it gaining information; it can, at any moment, recommend to the Prime Minister that an interception be cut short.

Furthermore, under Article 6 of law No. 2006-64 of 23 January 2006 on the fight against terrorism, the CNCIS is responsible for checking the data transmission requests set out in Article L.34-1-1 of the French postal and electronic communications code (CPCE).

http://lannuaire.service-public.fr/services_nationaux/autorite-administrative-independante_172128.html (French only)

Aside from these two independent authorities, the government has set up numerous bodies responsible for monitoring network security and informing the public on protection of their personal data. See the appendix (official organs involved in data protection), page 15.

Privacy awareness

In the summer of 2008, a massive movement took place in France, with 700 organisations and 250,000 individuals coming together against the creation, by decree, of a file named EDVIGE (**E**xploitation **D**ocumentaire et **V**alorisation de l'**I**nformation **GE**nérale, or documentary exploitation and utilisation of general information) that may infringe on privacy and liberties. The Conseil d'Etat censored part of the decree, based on the arguments put forth by the organisations and unions. Consequently, the government had to backtrack in part with regard to the file's purpose and content.

For more than thirty years in France, the rights and liberties of citizens with regard to information and communication technologies have been protected by the tools listed in the appendix of this document,

which support those implemented by the EU. Yet, existing provisions and tools are not sufficient for protecting our personal data and our privacy in a globalised world where political agendas are oriented towards greater surveillance of citizens, wanting to guarantee some sort of security to the detriment of liberties - the fight against terrorism being only a pretext - and where industrial and commercial stakeholders exploit advanced technologies and influence political decisions to their advantage when needed (e.g. biometrics, RFID, video surveillance).

As governmental projects are presented, there have been numerous mobilisations protesting, for example:

- the STIC file (Criminal Offences Processing System)
- INES (secure national electronic identity) electronic and biometric identity cards
- electronic passports becoming biometric passports
- the ELOI file (on persons subject to a removal order)
- SCONET and Base élèves premier degré (secondary and primary schools pupils database) files
- EDVIGE, CRISTINA (centralisation of internal intelligence for homeland security and national interests) and FNAEG (automated genetic fingerprint) files
- video surveillance (CCTV)
- the two new files that replace EDVIGE, on official inquiries related to public security and preventing threats to public security, created by decree on 16 October 2009 and published in the Official Journal of 18 October 2009[3].

MOBILISATIONS WITH VARYING RESULTS

There have been numerous campaigns against infringements on privacy and liberties, including:

- **Advertising video surveillance**

Late in 2008, the RATP (Parisian public transport operator) announced it was installing 400 "intelligent" advertising screens in the metro hallways, equipped with cameras that were technically capable of determining the gender of passers-by, as well as their age, skin colour and type of clothes, and of analysing their facial expression, all the while specifying what part of the ad they were looking at.

Following the mobilisation of various associations, including the ***R****ésistance à l'****a****gression* ***p****ublicitaire* (RAP; an association dedicated to fighting the negative effects of advertising), the RATP announced in July 2009 that it was not going to deploy the cameras designed to analyse the behaviour of people passing by the new advertising screens. The associations still insisted that the CNIL follow through with the detailed examination of this type of device and come to a conclusion as to whether they are illegal and unfounded or not.

- **ELOI file**

The ELOI file was created by a ministerial order from the Minister for the Interior to facilitate the removal of foreigners staying illegally on French territory. This text, published on 18 August 2006, was contested before the Conseil d'Etat by many associations. On 13 March 2007 the Conseil d'Etat decided to quash the order, reckoning that this sort of tool should give rise to a decree and be subject to the CNIL's approval.

Faced with this mobilisation, it seems the government was obliged to "fall back" on a number of points, in particular with regard to personal data recorded on people visiting foreigners held in detention centres. The second version of the ELOI file, created in a decree of 26 December 2007, eliminated these provisions. However, the points raised in the first petition remain. Consequently, the associations filed a new action for nullification with the Conseil d'Etat. The *rapporteur public* (public prosecutor) recommended rescinding specific parts of the decree:

- the second purpose of the file, i.e. establishing statistics on removal measures and the application of these measures;
- recording the AGDREF (application for managing files on foreign nationals in France) number in data on the person subject to a removal measure;
- the data retention period of three years from the date of actual removal, when the procedure is actually implemented.

[3] The new files state in particular that: personal data on minors aged 13 or older can be recorded; personal data can be recorded on people simply because they live in a certain geographical area; membership in a union, and political, religious or philosophic beliefs can in and of themselves be used to justify people not obtaining certain jobs (based on the "Non à EDVIGE" group's press kit, 4 December 2009).

The Conseil d'Etat did indeed rescind the two latter points on 30 December 2009.

- **Base élèves**

According to the Ministère de l'Education Nationale (ministry for national education), the IT application Base élèves premier degré is used for administrative and pedagogic management of students from kindergarten to the last year of elementary school (CM2, about 11 years old) in public and private schools. The base élèves has been experimental since 2005, in connection with the CNIL, and was being generally deployed in 2009 based on the content specified in the ministerial order of 20 October 2008.

A considerable volume of data was originally meant to be included in this file, on students' native culture, nationality and date of arrival in France, the language spoken at home, their entire educational path (e.g. repeating, absenteeism, support from a help network) and even information as personal as how they arrive at school (e.g. accompanied or alone).

At first very few parents reacted, most being unaware of this file. Then some of the directors in charge of recording these data decided to refuse to do so because of concerns about the mayors of *communes* and Académie inspectors having access to these data, as well as about the lack of security protecting such access. The movement grew with a petition and complaints lodged by parents. It was a success, as evidenced by the ministry modifying the file content. The ministry's site actually provides a list of what information is *not* included in the database (e.g. nationality and origin of the students and their legal guardians, family situation, parents' profession and social group, absenteeism, special educational needs, students' health condition, marks and learning achievements).

However, activists for the civil rights are still concerned by the attribution of pupils identifiers and the existence of a national database of these identifiers.

Recording personal data on children seemed sufficiently dangerous to the UN Committee on the Rights of the Child that, at the end of 2009, it informed the French government of its preoccupation with the deficiency of legal provisions for preventing interconnection between the *base élèves* and databases of other government bodies. The UN committee had two expectations: that parents have the right to correct and erase the file on their child(ren), and that access to the file be genuinely secure. These are the same demands that parents of the students and human rights defenders had been making for months.

The UN Committee on the Rights of the Child expressed many reservations with regard to the base élèves file, stating in an opinion of 11 June 2009 that it was preoccupied with the deficiency of legal provisions for preventing interconnection between the *base élèves* and databases of other departments.

While there have been some victories, the fact remains that a small minority of people were actively involved in these campaigns, which remain the product of militants who pay close attention not only to all draft laws, but also to all innovations designed to increase the 'security of citizens' and make daily life easier but that infringe nonetheless on the privacy of individuals.

NEW APPROACHES TO PRIVACY PROTECTION

The new stakes related to protecting privacy are no longer restricted to government bodies and their files (even though citizen monitoring by the government is always more intrusive), they also concern private companies. Not only is every individual deliberately put on file as employed, unemployed, a tax-payer, receiving social insurance, having a phone or Internet contract, but also as a customer of at least one chain store, a bank account holder, and a 'privileged' SNCF client, among other things. Privacy risks and concerns, with the multiplication of data that are circulating much more freely, are shifting from 'big files' to 'traces', and from government bodies to private operators.

The new forms of data collection and tracking (Internet, biometrics), along with the international dimension involved in collecting and transferring flows, the commercial value attributed to personal data and the power of search engines that enables cross-referencing, have changed the nature of both risks and the perception of risks considerably. And let us not forget the inflow of data from social networks, which must be considered as well as this collection of data by private companies.

Yet, there are practically no campaigns protesting the unfair use and sale of data by service providers and operators; only a few lawyers and experts try to draw these issues to the public's attention.

A major obstacle here is that the technologies available make life easier and increase the numbers of virtual contacts, while the price (entering personal information one time) seems like a bargain to

individuals who are poorly informed. The idea that they have nothing to hide leads them to believe they have nothing to fear.

It would seem that people are most active in movements against video surveillance, possibly because this technology is sometimes visible and is discussed in some official announcements.

THE TOPICS

The main problems identified in the themes studied are as follows:

Mobility and Transportation

The risks of tracking:

Users of the Navigo Pass are generally unaware that they are likely to 'disseminate' their personal data with the RFID chip of their travel card. They are also unaware of the lack of reliability of the RFID chips on which the data is stored and of the risk of tracking as their journeys can be recorded. The Paris city transport authority (RATP) has not promoted the "anonymous" version of the pass.

Geolocalisation leads to a very high risk of employee tracking which infringes on their privacy and also on labour laws.

Biological identity

The use of biometric data in passports poses the problem of the use of this technology for the purpose of identifying a person via their body parts. Furthermore, the database used to issue passports constitutes an ethnic and racial database which is made available (for example to police investigators), thus modifying the purpose initially declared.

The use of biometrics with children poses the problem of identification via body parts and of public authorities wishing to make children familiar with this type of checks.

Interpersonal communications

The problems caused by the use of electronic messaging systems are the results of either the sale or the non-protection of the registered user's contact details that go on to be used by marketing companies for sales purposes. Moreover, the data may be pirated and there is a risk of identity theft. When managed by an ISP, the e-mail account is subject to the retention of connection data and of other elements in the e-mails by the ISP, as part of the fight against terrorism. As concerns mobile telephones, there is the added risk of geolocalisation without the registered user's knowledge.

Social networks

The main problems identified are the infringement of privacy very often resulting from a lack of awareness of the configurations that enable users to protect their personal data, only making public certain details, and sharing other details with a limited number of contacts. The widespread media coverage of the problems experienced by some social network members or bloggers raised awareness among some enthusiasts who increasingly demand the right to delete the data concerning them.

In addition, American SNS stubbornly refuse to consider that European legislation is applicable for their activities in Europe.

CONCLUSION AND RECOMMENDATIONS

Through this study on the practices of teenagers and young adults, we have learned that it is not easy to obtain information on this target, with the exception of the use of telephones and social networks. Nevertheless, our work has led us to the conclusion that personal data protection procedures are generally lax, may represent an invasion of privacy and are potentially dangerous. These practices call for the need to inform and raise awareness:

- Among users of:
  - Transportation or other access with RFID smartcards,
  - Passports or other identification methods using biometrics,
  - Geolocalisation tools,
  - Internet messaging and mobile telephones,
  - Social networks.
- Among French public authorities regarding:
  - The increasing number of laws and regulations aimed at monitoring citizens as part of the fight against terrorism and organised crime, for enhanced security,
  - The implementation of these systems and the increasing number of tools favouring the industrial market of monitoring technologies to the detriment of human rights,
  - The increasing use of file profiling.
- Among European Union decision-making bodies, in particular using the powers entrusted to the Parliament since the entry into force of the Lisbon Treaty:
  - For compliance with the fundamental texts protecting privacy, in particular in all agreements with third-party countries and anti-terrorism and immigration measures,
  - So that the EU creates a Data Protection Authority with real powers,
  - So that they make American companies comply with European legislation.

The work to be launched or pursued is twofold: the demands to be made of public authorities and decision-makers, and information and awareness-raising campaigns to be launched.

Demands made of French public authorities:

- Comply with and enforce compliance with all the principles of the French data protection act (listed in the section on legislation), in particular as concerns biometric passports and their databases but also in the data collected in various fields (Navigo pass, messaging services, Internet Service Providers),
- Restore the French data protection authority (CNIL) all its powers, in particular those that were withdrawn in 2004 and the means to achieve real independence,
- Limit the number of State officials with access to databases and provide information and guarantees on the strict management of such access,
- Prohibit the sale of data collected by a public body to private organisations,
- Demonstrate transparency regarding the absence of links between the interests of monitoring technology manufacturers and the implementation of new legislation,
- Work for the respect of fundamental rights in all legislation, in particular that concerning the collection of personal data,
- Provide the means so that information campaigns can be conducted aimed at citizens and young people in particular on their rights, on the risk of self-exposure on the Internet and on social networks. Interesting campaigns have been launched by the CNIL and other bodies: they deserve wider media coverage and to be presented in all establishments welcoming young people of all school ages.

Information campaigns aimed at young people:

These campaigns could be launched after considering future changes in technology and also in mentalities. (For example, the argument of risks concerning exposure on the Internet as part of the search for a job sometimes leads to the argument: “in ten years’ time, if you do not have a blog or a profile, recruiters will find that suspicious”).

Some campaigns to be launched:

- Information on the anonymous Navigo Pass (see CNIL campaigns) and demands made to the RATP so that the advantages are equivalent to the standard Navigo Pass,
- Information on the Opt-in/Opt-out options of geolocalisation and of social networks,
- Information on the misuse of biometrics, on the collection of PNR data and its use,

- Information on the precautions to be made when posting on the Internet (messaging, blogs or social networks): check the configuration of profiles, bear in mind that the details may be read by more people than intended, and may also involve contacts who have not given their consent,
- Roll out campaigns to consider the options of data encryption, of browsing using anonymisation tools, of using pseudonyms, of ‘scrambling’ the message by posting contradictory information, the option of limiting information life spans, etc. All options that are restrictive and make the use of ICT more complex but for which technological advances may provide a solution.

Synthesis Appendices

OFFICIAL BODIES IN CONNECTION WITH DATA PROTECTION

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE (SGDN) [GENERAL SECRETARIAT FOR DEFENCE AND NATIONAL SECURITY]

One of its main assignments is to reinforce security on information systems and networks belonging to the government and public services. The SGDN works with major operators to identify and monitor the risks affecting information system security: network intrusions, malevolent interceptions of communications, proliferation of computer viruses, and manipulation of information. The SGDN conducts awareness-raising initiatives aimed at authorities on all the events and computer-related vulnerabilities it can identify.

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI) [FRENCH NETWORK AND INFORMATION SECURITY AGENCY]

Founded in July 2009, the ANSSI is attached to the SGDN and has national jurisdiction. The Agency has national authority as regards information system security for the implementation of the defence policy against cyber attacks.

In addition to its official website, the ANSSI has created a computer security portal: http://www.securite-informatique.gouv.fr. Set up in 2008, this portal provides practical information and advice for individuals and professionals. It includes: security alerts, a glossary on computer security, a guide and recommendations for passwords, information on the importance of security measures, etc. It also provides a number of links to bodies and organisations in connection with data protection.

CENTRE D'EXPERTISE GOUVERNEMENTAL DE REPONSE ET DE TRAITEMENT DES ATTAQUES INFORMATIQUES (CERTA) [GOVERNMENT CYBER ATTACK RESPONSE CENTRE)

This is a government website that posts a list of vulnerabilities notified by software publishers. The references are: http://www.certa.ssi.gouv.fr

AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES (ARCEP) [FRENCH TELECOMMUNICATIONS AND POSTS REGULATOR] - http://www.arcep.fr

The *Autorité de régulation des télécommunications* (ART) [telecommunications regulation authority] was created by a law enacted in 1996 to regulate the telecommunications sector. It is an independent administrative authority that was entrusted the regulation of postal activities in 2005. It is in charge of the adaptation of European Directives on electronic communications to national law.

OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITE LIEE AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (OCLCTIC) [CENTRAL OFFICE FOR THE FIGHT AGAINST INFORMATION TECHNOLOGY- AND COMMUNICATION- RELATED CRIME]

The central office was founded in 2000 within the French Ministry of the Interior, more specifically reporting to the economic and financial affairs sub-division of the criminal investigation central division (*police judiciaire*).

The fight against cyber-crime and credit card fraud includes the legal handling of criminal offences related to new technologies and of those for which the perpetration is facilitated or related to the use of these technologies. It also provides training and leads and coordinates the actions of the other departments with jurisdiction over offences related to information and communication technologies, as well as international cooperation - Europol, Interpol, G8.

DELEGATION AUX USAGES DE L'INTERNET (DUI) – [DELEGATION FOR INTERNET USE]

http://delegation.internet.gouv.fr

The DUI's role is to propose measures required for the development of an information society that benefits everyone everywhere. This includes in particular measures to reduce the digital divide. Founded in 2003, the DUI reports to the French Ministry for Higher Education and Research. It is in charge of developing universal Internet access, for example digital public spaces with the NetPublic label, of encouraging the security of Internet users in general and the protection of minors in particular – steering the European "Confiance" programme, Tour de France of schools, etc. – and of providing training and support with regard to information and communication technology – Internet support operation, multimedia Internet passport, etc.

WEBSITES UNDER STATE AUTHORITY

SERVICE PUBLIC http://vosdroits.service-public.fr/Fichiers, libertés, protection de la vie privée

This website explains how files containing personal data are accessed and provides information on principles and citizens' rights: rights of access, correction and opposition and also the limits of these rights – files excluded from data protection obligations with the CNIL authority, etc. There are links to fact sheets and models of letters proposed by the CNIL.

INTERNET SANS CRAINTE http://www.internetsanscrainte.fr/accueil

The national programme intended to raise young people's awareness of the correct use of Internet on a site. Created by the Délégation aux Usages de l'Internet (DUI) and Microsoft, this programme is supported by the European Union.
"*internetsanscrainte.fr*" is the official site for the prevention of Internet-related risks for children. The information provided is aimed at children aged between 7 and 12, young people aged between 12 and 16, and parents. There are also brochures, cartoons for children, quizzes and a hotline number to discuss concerns about the Internet.

PROTEGE TON ORDI http://www.protegetonordi.com/

This site is the fruit of a public-private partnership between public authorities (the DUI), Microsoft and a group of partners and proposes advice in various forms, in particular comic strips for adults or children on the theme "Working for a safer I*nternet! […] to help you learn the simple and essential ways of protecting your computer, your family and yourself* ".

"SURFEZ INTELLIGENT" http://www.ddm.gouv.fr/surfezintelligent/

Aim of the site: As in everyday life*, there are rules for using the Internet correctly and to make full use of it. With its partners –* ***public and private stakeholders*** *- the Junior Minister's Office in charge of forecasting and development of the digital economy provides a few landmarks and essential practices for hassle-free surfing*.
There is a charter for the promotion of authentication on the Internet in order to *familiarise Internet users with authentication*, tell the difference between authentication and identification, obtain information - recognise secure sites, *know what data some providers are entitled to request, data never to be provided, how to read contracts, legal and contractual obligations, access to data, etc*.-encourage Internet users to get into good habits - securing their computers*: use of protection tools, regular updates, management of authentication procedures, configuration of security applications, etc. […] not clicking on a link in a spam* -, and the 'Reciprocal commitments of professionals and public authorities'.

SOME ORGANISATIONS THAT MONITOR SECURITY

OBSERVATOIRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX (OSSIR) [FRENCH INFORMATION SYSTEM AND NETWORK SECURITY OBSERVATORY] -http://www.ossir.org

The OSSIR is an association of users interested in information system and network security that organises the annual *Journée Sécurité des Systèmes d'Information (*information system security day*)*. This annual event brings together experts, professionals in all aspects – technical and legislative – of information system security. In 2008, the theme was: *Anonymity, privacy and identity management* with a presentation of the concept of a "blank identity card ", on the theme "*Principles and technologies to protect privacy on the Internet*".

FING - FONDATION INTERNET NOUVELLE GÉNÉRATION [NEW GENERATION INTERNET FOUNDATION]

http://fing.org/

Launched in 2000, the foundation's members include experts, major companies, start-ups, research laboratories, universities, local authorities and administrations. It monitors technologies, at the crossroads between society, the economy and technology. It works in three fields: intelligence and foresight, think/do tank, and open innovation. Its objectives are:

- Play a pivotal role in the emergence of innovative ideas and projects,
- Mobilise stakeholders around the future technological cycles,
- Take part in emerging ethical and societal debates,
- Facilitate bottom-up innovation.

The foundation works on the theme of Active identities: Digital identity is the pivoting, federative element of most of the new services and practices that emerge today on the Internet (on blogs, social networks, "*web 2.0*", identity federation, portfolios, multi-service cards, composite services, communities, virtual universes, etc.). The question of anonymity or "pseudonymity" is analysed and discussed on the site's blog.
It is working on the question of setting up a **"data protection act 2.0"**, attempting to answer the question: "apart from changes (only normal over a thirty-year period) in the data protection field defined thirty years ago, or the difficulties arising from application – *are there factors that radically change the context in comparison to 1978: new practices (individual, group, corporate or administrative) that cannot be reduced to those we know? Techniques that change the background? Scales so different to those in 1978 that they change the very nature of the phenomena concerned?... "*

***LE FORUM DES DROITS SUR L'INTERNET [FORUM OF INTERNET RIGHTS]* - http://www.foruminternet.org/**

Defined as the link between the public and private spheres, the Forum is an original answer to the question of regulating a constantly changing universe". The Forum has around 70 registered members divided into two colleges, economic players and users, made up of legal entities, public authorities and people from civil society.
It posts advice for Internet users, teenagers, parents, bloggers, etc., in various forms: comic strips, factsheets, guides etc.
The Forum also publishes recommendations drawn up by various working groups, notes and case law on various subjects related to the Internet.

IMAGINONS UN RESEAU INTERNET SOLIDAIRE [IMAGINE A SUPPORTIVE INTERNET] - IRIS

http://www.iris.sgdg.org/

Founded on 4 October 1997, the IRIS association's aim, as defined by IRIS itself, is to "work towards a development of the Internet with more equality, sharing and solidarity".
Its main areas of consideration and action are as follows:

- To work for the development of a public service infrastructure providing access for all with permanent connectivity,
- To enable everyone to produce content and communicate it publicly, without using intermediaries,
- To fight for the long-term continuation of non-market sectors on the Internet.

In France, IRIS is member of the ***DELIS COLLECTIF (DROITS ET LIBERTÉS FACE À L'INFORMATISATION DE LA SOCIÉTÉ) [RIGHTS AND FREEDOM AGAINST THE BACKDROP OF THE COMPUTERISATION OF SOCIETY]***: www.delis.sgdg.org.

On a European scale, IRIS is a founding member of the EDRI Foundation (**E**uropean **D**igital **Ri**ghts): www.edri.org.

On an international scale, IRIS is a member of the GILC coalition (**G**lobal **i**nternet **l**iberty **c**ampaign): www.gilc.org.

The association works on a national scale by conducting institutional consultations and hearings. It raises awareness in the field of associations and unions of the political and social stakes related to the Internet. IRIS also publishes reports and analyses, and organises conferences and debates. On a European level, IRIS takes part in European Commission working groups on illegal and offensive content on the Internet and on cyber-crime. Lastly, on an international level, the association works with the Council of Europe and Unesco, in particular as part of the GILC.

Mobility and transportation

NAVIGO PASS

TOPIC	**The NAVIGO pass, a travel card in the form of a smart card for use on public transport in the Ile-de-France area.**
Technologies used	Radio Frequency Identification (RFID) and file for storing collected data. This technology makes it possible to identify objects, track them and determine their features remotely thanks to a label that emits radio waves and is attached to or embedded in the object. RFID technology can read these labels without contact and can penetrate thin layers of material such as paint or snow. The label comprises a microchip and an antenna embedded in a medium, in this case a plastic card. A reader scans, captures and transmits the data stored on the microchip. There are three types of RFID labels: * Single-read labels; * Multiple-read labels; * Read and re-write labels. And two major groups of RFID labels: * Active labels, connected to an on-board energy source (e.g. electronic toll systems on motorway networks). * Passive labels, that use energy from an emitter. These less costly labels are usually smaller and have an almost unlimited lifespan. The RFID label type of Navigo pass is a passive one of CALYPSO technology answering standards ISO 7816-1, 2, 3, 4 and CEN on 1545. It passes on the information which it contains but cannot receive from it. How it works: When going to use public transportation, the passholder presents the Navigo pass to a reader that authorises or refuses access (for certain trips this pass also has to be validated on the way out). The machine reads data from the contactless RFID chip: first and last name, age, mailing address and information regarding the type of service subscription and its validity period. The Navigo pass only makes it possible to know at which station a user entered, and possibly exited, the metro system. It is not possible to know what route was taken. These data can only be retained for a maximum of two days (at the request of the French national commission for information technology and civil liberties, or CNIL) and only for the purpose of detecting fraud.
Country/zone where used	France/Ile-de-France public transport.
Target population	Whole population, no age restriction or requirement. However, the groups most concerned are: - employees commuting daily to work; - Schoolchildren and students travelling to school or college/university. As of 31 January 2009, there were 4,536,000 Navigo clients (source: ratp.fr), broken down according to the following service subscriptions: • 2,498,000 monthly or weekly Orange cards: These are travel cards that allow holders to make unlimited trips for a week or a month within the Ile-de-France zones specified in the contract.

	• 870,000 annual passes: This is a travel card purchased under a long-term service subscription that allows the holder to make unlimited trips within the Ile-de-France zones specified in the contract. • 779,000 "Imagine R" passes: This is a travel card for young students between the ages of 12-25 in the Ile-de-France area. It is valid for one year, and allows access to the various public transport means in the region. On weekdays, the passholder is allowed unlimited travel within the zones specified in the contract. On weekends, bank holidays and school holidays, the card is "de-zoned" and can be used to travel anywhere in the Ile-de-France region. • 389,000 Navigo *Découverte* (Discovery) passes: This Navigo pass has been available to all public transport users since 2007, whether or not they live in the Ile-de-France area, and was created at the request of the CNIL, which demanded an anonymous version of the Navigo pass to comply with the principle that coming and going freely is one of the fundamental freedoms of our democracies. It contains no personal data. It also comes as a contactless RFID chip card, associated with a personal transport card with the holder's photo and handwritten first and last names. It is used to load short-term Orange card access. If the card is lost or stolen, however, neither the card nor the access remaining on it are reimbursed as no personal data can be used to verify who purchased the service subscription.
% of use among the target population and young people	No reliable figures on the ratio use/user age.
Trends	No reliable statistics. See GIE Comutitres site (French only).
Known/potential dangers of this technology/risks	RFID presents a threat in terms of tracking and profiling individuals. This new technology, accused of invading the privacy of citizens/consumers, worries consumer protection and fundamental rights organisations that see it as a way of collecting information on consumers without their consent. Furthermore, anyone with an adapted reader can read the contents of an RFID chip without the holder knowing. In the case of the Navigo pass, which contains personal data that can be used to remotely identify the holder, individuals can be tracked in all of their daily activities. In France, the CNIL has already classified RFID labels as a technology that endangers individual liberties, deeming they constitute personal data under the definition in the French Data Protection and Liberties Act of 1978. Source: http://www.cite-sciences.fr/francais/ala_cite/science_actualites/sitesactu/question_actu.php?langue=an&sommaire=1&id_article=2803
Files created and their purpose	Source: General conditions of use Deliberation 2008-161 of 3 June 2008 granting unique authorisation for implementing automated processing of personal data with regard to ticket application management by public transport operators and organising authorities (unique authorisation decision No. AU- 015) - (JORF No. 0153 of 2 July 2008), available in the appendix. The data collected undergo automated processing with a view to managing Orange card service subscriptions and Navigo pass applications.

Associated file and date of creation	Reference unknown, created in 2003.
Purpose of file	Managing, issuing and using travel cards: - managing service subscriptions and issuing full fare, reduced fare and even free tickets; - managing after-sales service operations and customer complaints. Managing and monitoring commercial relations. Managing fraud: - detecting technological fraud and counterfeit, and investigating cases; - managing cards cancelled due to loss, theft or a payment issue; - managing cards cancelled due to misuse (e.g. detection of several dozen entries/exits made using the same card). Carrying out statistical analyses on network use: - traffic; - types of travel cards issued; - clients; - use by type of travel card. Assessing quality of system operation: - analysing technical problems with cards or validating machines; detecting operational abnormalities in the information system.
Content, data types	- Identity (marital status, sex, first and last names); - Date and place of birth; - Mailing address; - Telephone numbers (home and mobile) and email address (optional); - ID picture.
Who retains the data, who has access? Risks	Data are intended for GIE Comutitres (an economic interest grouping that manages shared travel cards and tickets in Ile-de-France), its service providers, Ile-de-France transport undertakings, institutional financiers and the Organising Authority for Public Transport in Ile-de-France (STIF). In 2006 an Internet user accessed the files of Navigo users, as the Internet address for each form included part of the client number of the user in question. By modifying these numbers in the browser, the hacker succeeded in accessing 1,400 applications containing client pictures, first and last names, mailing addresses, email addresses and telephone numbers.
Retention period	**For management:** All customer data is retained throughout contract relationships and for a period of two years afterwards for commercial and statistical purposes related to customers and prospective clients. **For daily travel:** Validation data containing information on the movements of individuals, linked to the card or holder number, both of which refer indirectly to the identity of the user, can be retained for a maximum of 48 hours and for the sole purpose of fighting technological fraud.
Right of inspection and	Access and rectification rights as defined in section V of the modified law of 6 January 1978 can be exercised by contacting the service(s) designated by the

rectification	processing manager.
Hidden purpose of file and wrongful use/risks	**The CNIL believes that preserving details of the journeys of an identified individual for 48 hours, purportedly to fight fraud, runs counter to democratic values. Consequently, it called for users to be offered the possibility of travelling anonymously without incurring any additional cost as compared with a personal pass.** **This requirement has been met in part because the Navigo Découverte pass is available in some RATP and SNCF stations for 5 Euros.** The police are entitled to access the recorded data. In an opinion of 8 April 2004, the CNIL demanded that the STIF create an anonymous form of the Navigo pass, emphasising that users should have the possibility of accessing public transport services in an anonymous manner without incurring any additional cost as compared with using a personal pass. The STIF reacted by creating the anonymous Navigo Découverte pass on 1 September 2007. The CNIL declared it was satisfied, though disappointed by both the delay in introducing this anonymous card and the associated cost (5 Euros). To offset the cost, the card is valid for 10 years. On 6 January 2009, following various consumer complaints and field-testing operations, the CNIL judged that exercising the right to travel anonymously is not guaranteed for users, and that the conditions for the provision of information on, and for obtaining, the Navigo Découverte pass were mediocre and even acted as a deterrent. **A lack of awareness regarding the availability of this pass can indeed be observed in personnel; the regular absence of related commercial documentation and the difficulties in actually purchasing this pass at sales windows are also noticeable.**
Legislation currently in force	
Legislation	The French Data Protection and Liberties Act of 6 January 1978, amended on 6 August 2004, is applicable in cases where RFID devices are used to directly or indirectly a private individual. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20090723 (official text) http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (CNIL translation)
Threats to liberties despite the legal framework in place	Tracking, registration and profiling of individuals.
Compliance with European law (e.g. Charter of Fundamental Rights, directives)	There is currently no European legislation on the use of RFID technology. See the European Commission's recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Like CCTV surveillance, the Navigo pass circumvents the Universal Declaration of Human Rights which states in Article 12 that "No one shall be subjected to arbitrary interference with his privacy...", and in Article 13 that "Everyone has the right to freedom of movement...".
If regulations are revised: grounds? Outcome: data	

protection improved or weakened?	
These tools, young people and young adults	
Extent to which they are concerned, or importance of use	Adolescents and young adults, whether students or employees, are exposed to the possibility of registration, tracking and profiling, just like all individuals.
Awareness of problems and risks	They are not properly informed about the threats to liberty posed by these systems; they do not see beyond the comfort and convenience they offer and are unaware of the inherent dangers.
Campaigns to run, aspects to be covered	Awareness-raising campaigns based on the Navigo pass. RFID technology is developing very swiftly without the public being informed of the potential dangers of tracking and profiling by the government and the business sector. It is urgent that the public be informed on this topic. Communicate with Imagine R cardholders (no anonymous pass options, strong targeted marketing incentives by the RATP).
Conclusions	
Recommendations	Tracking risks should be publicised in the media and denounced. Risks regarding access to personal information stored on RFID chips could be reduced by using high technology chips. File managers should be encouraged to secure access to these data (e.g. provide for penalties in case of access by unauthorised people?).

PNR

TOPIC	PASSENGER NAME RECORD (PNR)
Technology used	**Database.**
Country/zone where used	Europe ⇔ United States. The EU also has agreements with Canada and Australia.
Context	This is an agreement between Europe and the United States. As part of the fight against terrorism, for every flight to the United States, every transit flight or overflight, European air carriers must allow US authorities (US Customs and Border Protection) to access their databases containing personal passenger data related to their entire trip. These data are collected from clients at the time of reservation by travel agencies or the air carriers, and stored in the reservation systems shared by multiple air carriers or agencies such as Amadeus. They serve to identify the passenger's itinerary, flights involved, ground contact (telephone number), fares negotiated, bank card number and in-flight services requested such as specific dietary requirements (e.g. vegetarian, Asian, kosher) or services related to the state of health of the passenger, as well as services booked for the stay, such as hotel and car rental. See the list in the file content section. US authorities require access to the databases 72 hours before each flight to the United States. They also receive Advance Passenger Information (API) data, completed during check-in and transmitted when the flight departs. These data include information such as marital status and passport number. Data is collected to create a file of persons, based on profiling, to compare against the no-fly and selectee lists. The **no-fly list** contains the names of passengers who, for certain reasons, are not allowed to fly. Passengers on this list are refused boarding passes. The **selectee list** contains the names of passengers who present a higher risk than normal and must therefore be subjected to additional security screening (person and luggage). Similar agreements have been signed with Canada and Australia. The United Kingdom has implemented a monitoring system with European countries.
Target population	All ages. No mention of age restrictions. According to Eurostat, the number of passengers flying between Europe (25 Member States) and the United States increased by 12% between 2003 and 2004, the equivalent of 45 million passengers (on 215,000 flights). This upward trend has continued.
Files created and their purpose	The US government has not provided any information on this subject. Apparently there are three files: - No-fly list: banned from US territory; - Selectee list: files to be checked prior to a decision; - Files containing data collected (PNR). These PNR files are not transparent. The data collected are held for at least 15 years with no guarantee they will be destroyed thereafter. PNRs can be created in various ways: 1) Through computerised reservation systems (GDS): The travel agent creates a PNR on a client using the computerised reservation, which is a gateway to numerous stakeholders in the tourism industry. It offers the possibility of reserving seats with many air carriers, and reserving hotels and car rentals.

	Depending on the GDS, there are many possibilities. The travel agent books an entire trip and all information on this trip is stored in the PNR. Each PNR is identified by a 6-character alphanumeric record locator. Once the PNR is created, the information is sent to all concerned parties. 2) Directly by the air carrier: The PNR contains information on a single flight. There are as many PNRs as there are reservations; a single PNR can cover multiple passengers travelling together. Each person travelling to the United States must fill in a form on the American embassy's website. Upon arrival in the United States, each person must go through immigration, at which time the passenger's picture is taken, as are their digital fingerprints.
File content	The full PNR data list is posted on the CNIL's website (www.cnil.fr). PNR files contain the following data (list not exhaustive): - passenger's first and last name; - place of residence; - telephone numbers; - email address; - method of payment (credit card number, billing address, ticket price); - APIS information, such as passport number; - date of birth and nationality; - OSI data (free input zone: list of requests made by passenger, such as provision of a wheelchair on arrival, SSI/SSR data – request for special services based on meal preferences, state of health or age, e.g.: vegetarian, diabetic, salt-free, no pork, medical care; - general observations regarding incidents that occurred on previous flights such as arguments or excessive alcohol consumption; - passenger status, e.g. economy, business class, frequent flyer, miles flown); - date journey booked; - scheduled date of travel; - date ticket issued; - full passenger routing; - passenger without a reservation; - passenger recorded as a no show (absent at boarding despite having a reservation); - travel agent and agency that sold the ticket; - information on seat occupied (left-hand/right-hand side, front/rear of the aircraft); - record of changes to the PNR file.
Retention period/risks	GDS PNR data are retained for one month after the flight, and archived for three months. Data collected by US authorities are retained for 15 years without any guarantee that they will be destroyed.
Who retains the data, who has access?	Travel agencies, air carriers and GDSs. The US authorities
Right of inspection and rectification	- All PNR data benefit from administrative protections, irrespective of the interested party's nationality or country of residence. - Furthermore, a system is available providing redress for persons seeking information about or correction of their PNR. - Persons wishing to access their PNR are entitled to do so under the Freedom of Information Act; requests may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW Washington, DC 20229

Purpose of file	The official goal is security. It is apparently a tool for fighting terrorism and serious crime. As such, although this system was introduced before 11 September 2001, the US authorities subsequently tightened their requirements. However, terrorism and serious crime have not been defined.
Dangers	➢ *Article 29 Working Party opinion - 2007* In November 2007, shortly after the European Union and the United States signed an agreement on the transfer of PNR data, the European Commission filed an umbrella project for a new directive. The Article 29 Working Party, which brings together the European data protection authorities, published a report on this framework decision in December 2007, criticising, in particular, the lack of provisions designed to guarantee the security of personal data with regard to privacy. It highlights that "the present draft foresees the collection of a vast amount of personal data of all passengers flying into or out of the EU regardless of whether they are under suspicion or innocent travellers. These data will then be stored for possible later use for a period of 13 years to allow for profiling. The proposal comes in addition to the fingerprinting of all citizens when applying for their passports as well as the retention of all telecommunications traffic data in the EU... An EU PNR regime must not lead to general surveillance of all travellers." The Article 29 Working Party also specified that the United States "has never conclusively proven that the vast amount of passenger data it collects is indeed necessary in the fight against terrorism and serious crime... The only substantiated available information to this end indicates that primarily API rather than PNR data are used". Consequently, the Article 29 Working Party observes that it does not see the need for countries to record, on top of the API and PNR data, a biometric database on applicants for Schengen visas (especially since the EU already has a Schengen Information System, or SIS, and is working on a European Visa Identification System). With regard to exchanging information with third countries, the group is concerned about the consequences of automatic reciprocity with third countries using a PNR system. According to the Article 29 Working Party, the fact of an existing European PNR regime might lead to PNR demands on the basis of reciprocity by undemocratic or corrupt regimes. The repercussions of such reciprocity do not appear to have been sufficiently examined (e.g. retention of credit card information by a civil servant in a country incapable of eliminating corruption could have dire consequences) It should also be noted that the interpretation of the wording "fight against terrorism" in some countries might differ significantly from the European view. As a result, reciprocity could enable a dictatorship to carry out a risk analysis on dissidents based on PNR data. ➢ *PNR agreement between the United States and the European Union* Following the events of 11 September 2001, the United States' Department of Homeland Security (DHS) tried to obtain access to EU Member States' PNR data. Congress passed two laws requiring these data, the Aviation and Transportation Security Act of 19 November 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002. Washington also negotiated an agreement with the European Union in May 2004, the EU/USA PNR Agreement.

	However, the European Court of Justice, on application of the European Parliament, invalidated this agreement on 31 May 2006 in a *Euractiv* ruling founded solely on the agreement's legal basis and not on its substance. The US and the EU signed a new PNR Agreement in July 2007. The new agreement puts an end to the period of uncertainty that followed the European Court of Justice's ruling that terminated the previous agreement. Nonetheless, according to the European data protection authorities, the European Parliament and the European Data Protection Supervisor (EDPS) believe that the level of protection for transmitted PNR data provided in this agreement is far from adequate. Another criticism of the agreement pertains to the lack of clear provisions, that are both precise and proportionate, on the sharing of information, retention, additional data transmissions and supervision by data protection authorities. Another potential concern lies in the fact that numerous provisions may be implemented at the discretion of the United States. ➢ In November 2006, the Electronic Frontier Foundation, a civil liberties group, filed a complaint against the DHS to make the use of PNRs (also used for domestic flights) more transparent. ➢ Potential for espionage and economic intelligence: all fares granted for a given flight can be known. ➢ Potential for selective entry into the United States based on criteria other than the risk of terrorism.
Legislation	*France:* Article 7 of law No. 2006-64 of 23 January 2006 on the fight against terrorism. This article authorises the collection and use of PNR and APIS data. The Minister of the Interior is authorised to introduce automated processing of personal data collected in connection with international travel. Article 65 of the Customs Code. This article provides for the compulsory production of all kinds of documents related to operations of interest to the customs authorities. They are also entitled to explicitly request the PNR data of specific flights on occasion. Executive order NOR IOCC0830651A of 28 January 2009. This order sets up, on an experimental basis, automated processing of the personal data of passengers recorded in airline departure and control systems. Senate resolution No° 84 of 30 May 2009 on the proposal for a framework decision relating to the use of PNR data for enforcement purposes. *European Union:* In the European Union, access to PNRs is regulated by different texts on the protection of data. 1980 OECD Guidelines on the Protection of Privacy/1995 European Data Protection Directive. *PNRs can only be transmitted to countries implementing similar guidelines on the protection of privacy.* Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, adopted without the opinion of the European Parliament, based on the Schengen Agreement, also regulates the exchange of PNR data with the official goal of fighting terrorism and illegal immigration by

	authorising "their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (ordre public) and national security" (Art. 12). 2007 Agreement between the European Commission and the US authorities. This agreement includes the following provisions: • The number of US authorities authorised to access PNR data on US territory has been expanded; • The purposes for which PNR data are used can be changed through a unilateral amendment to US law; • Any decision to transfer European PNR data to third countries shall be taken unilaterally by the US without prior consultation of the European authorities; • Henceforth, "in case of need" the US authorities can access so called "sensitive" data , i.e. data that may reveal individuals' racial and ethnic origin, political opinions, or state of health, despite the filtering rule initially agreed to; • Data shall be held for 15 years, actively for 7 and passively for 8, without any guarantee that files not consulted will be definitively destroyed; • The move from allowing US authorities direct mode access (pull) to the data held by airlines to the airline release mode (push), whereby direct access is no longer possible, will only occur if the United States is satisfied with the attendant technical conditions; • Evaluation of the implementation of the "review" agreement no longer has to be conducted annually. Only the European Commissioner of the Directorate-General for Justice, Freedom and Security shall conduct this inspection, without national data protection authorities being clearly associated; • The US authorities shall have the faculty to decide unilaterally to accede to European passengers' request to access and rectify data on them held by the US authorities.
Campaigns	As of 2003, the French league for human rights (LDH) has taken up the AEDH's message, denouncing the invasion of privacy and threats to democracy represented by the PNR agreement, just like IRIS within the Trans Atlantic Consumer Dialogue (TACD). During its 2009 congress, the LDH highlighted the dangers of these exchanges, stating that the exchange of personal data organised between European Union Member States (especially due to the extension in 2007 of the provisions laid out in the Prüm Treaty), or even between the EU and third countries (in particular, the PNR Agreement signed with the United States relative to passengers of transatlantic flights), significantly amplifies the threats that these monitoring techniques pose for privacy and liberties by increasing the area in which "sensitive" data are collected and transmitted, including by private companies, without anywhere near sufficient control. Young people, like the majority of the population, do not seem to be aware of these dangers.
Recommendations	Associations for the defence of liberties and human rights should, based on the aforementioned opinion of the Article 29 Working Party and the EDPS (see EDPS-PNR in appendix), and using the new powers conferred to the European Parliament by the Treaty of Lisbon, act to: • Ensure that the principle of proportionality and the rule of necessity of the agreement terms are respected; • Create a secure legal framework; • Obtain a summary of the concrete results stemming from use of such an arrangement;

	• Exclude any use of sensitive data related to racial or ethnic origin, religious beliefs, political opinions, membership in a union, state of health or sexual orientation; • Encourage use of the "push" system for transferring data to be included in this new agreement; • Revise the total period of data retention, currently disproportionate, to a more reasonable retention period; • Inform passengers on how their personal data is used.

GEOLOCALISATION AT WORK

TOPIC	Geolocalisation
Technologies used	A GPS (Global Positioning System) geolocalisation system based on processing data emitted by satellites paired with the use of a GSM (Global System for Mobile communications) electronic communications network.
Country/zone where used	Europe ↔France.
Context	According to the CNIL's definition: "geolocalisation" devices enabling private and public employers to ascertain knowledge on the geographical position, at a point in time or continuously, of employees by locating objects they use (e.g. badges, mobile phones) or the vehicles entrusted to them.
Target population and age	Employees.
% of use among the target population and young people	Unknown.
Trends (measured/presumed)	The development of technologies and control-related needs (e.g. quality, security) indicate that the number of employees being tracked is in a growth trend.
Known/potential dangers of the technology/risks	**Tracking** a car must be proportionate to the intended purpose, and permanently monitoring where employees travel to is disproportionate when this can be verified through other means
Other	
Files created and their purpose	
Associated file and date of creation	Recorded data processing file. This file must be declared in advance to the CNIL unless a CNIL agent has been designated.
Grounds for inclusion in this file/risks	Inclusion in the following circumstances: - the security or safety of an employee, or of the goods or vehicle they are in charge of (e.g. employees working alone, cash transportation); - improved allocation of resources for services to be performed in scattered locations (e.g. emergency operations, taxi drivers, breakdown fleets); - the follow-up and invoicing for transportation of persons or goods, or for provision of services directly linked to the use of a vehicle (e.g. school buses, cleaning verges, snow clearance, motorway service patrols); - monitoring working times, when no other means are available. In contrast, tracking systems cannot be justified when employees are allowed some freedom in the organisation of their movements (e.g. medical representatives, sales representatives). The CNIL emphasises that tracking devices should not give rise to continuous monitoring of the employees. Furthermore, the processing manager must not collect data on the location of an employee outside his working hours. That is why the CNIL recommends that, where these vehicles are available for private use, employees be given the option of switching the tracking function of their vehicles off at the end of

	their shift. Employees who hold trade union or elected offices must not be subject to tracking operations when on business pertaining thereto. Source: CNIL, deliberation No. 2006-066 of 16 March 2006 adopting a recommendation related to the implementation of devices designed to track motor vehicles used by employees of public or private entities. (French only.)
Purpose of file/content, types of data/risks	The purposes of this device can include managing customer operations in real time and fighting theft. The data collected are: - name of employee; - vehicle registration number; - kilometres covered; - stopping times; - average speed; - geolocalisation data. Risk of diversion from purpose; for example, employers using tracking devices to check on the activity of their employees while the purported purpose is fighting theft. See: CNIL employee tracking guide on the rights and obligations of employees with regard to GSM/GPS tracking. (French only).
Who retains the data? Risks	Employer.
Who has access? File sharing? Access restrictions/risks	Access to tracking data must be restricted solely to those individuals who may legitimately need those data to perform their duties which relate to the purpose of the device (e.g. persons in charge of coordinating, planning or monitoring operations, persons in charge of the security of goods carried, human resources officers). The processing manager must then take every precaution to preserve the security of the data and prevent access by unauthorised staff, in particular by instituting identity checks. Individuals must access tracking data using a personal PIN and password, frequently changed, or by some other means of authentication.
Retention period/risks	1 – Tracking data on employees cannot be held longer than is relevant for the purpose that warranted the tracking operation in the first place. The CNIL believes that two months is a proportionate time to retain the data. 2 – Tracking data can be held for a period exceeding two months should this prove necessary either to constitute a record of movements so as to optimise rounds, or as evidence that operations have been carried out where no other form of proof exists. In these cases, the retention period is one year. 3 – As regards monitoring working time, only data relating to hours worked can be held for a period of five years.
Right of inspection and rectification	The processing manager must, according to the provisions laid down in the labour code and the legislation applying to the three civil services, inform and consult staff representatives before introducing an employee tracking device. Every employee must be able to gain access to the data related to him or her generated by the tracking device by addressing a previously designated person.
Hidden purpose of file and wrongful use/risks	Recording of movement data can be used to monitor employees.
Other	Where employees object to personal information on themselves being processed, the processing manager, in this case the employer, will weigh the legitimacy of the reasons given. In case of disagreement, the competent courts must settle the dispute.
Legislation currently in force	
Law/regulation/other	Geolocalisation operations, in that they can locate an employee using a

	vehicle in real time, deal with personal data, and are subject to the provisions of the amended law of 6 January 1978 (Article 6-2). According to the CNIL, in accordance with Article 32 of the Law of 6 January 1978, amended in August 2004, and Article 34-1 IV of the postal service and electronic communications code, employees must be informed, individually, on the following before any such system can be implemented: • the purpose(s) of the tracking system; • categories of tracking data processed; • period for which tracking data related to them shall be held; • recipients or categories of recipients of these data; • the existence of the rights of access, rectification and objection, and how to exercise these rights; • as required, transfers of personal data envisaged to a third country. **Furthermore, it is absolutely necessary that each employee concerned by such measures sign a contract amendment, or that these provisions be included in the company's employment regulations.** Geolocalisation is subject to the French employment code **(Art. L.432-2-1**) which states that prior to implementing this sort of system, the employer must inform and consult the elected works council or, failing that, the employee representatives, on the automated processing to be implemented, as well as on any modifications to this processing.
Threats to freedom despite the legal framework in place	Employee monitoring by employer, invasion of privacy.
Other	In a deliberation of 17 November 2005, the CNIL opposed a project to personalise insurance premiums based on how vehicles are actually used. The insurer proposed reducing the premium in exchange for installing a tracking device in the vehicles so that it could verify, if required, that contractual commitments were being respected. In particular, tracking was going to be used to confirm that drivers respected the authorised speed limits. The CNIL opposed this scheme, citing many principles from the amended law of 6 January 1978. For example, Article 9 of this law does not allow a person governed by private law to perform operations related to speed violations. Therefore, an insurer cannot record when its clients speed.
If regulations are revised: grounds? Outcome: data protection improved or weakened?	Need for a more detailed analysis of current and future uses so as to assess which restrictions should to be brought in. Specific regulations reduce the risks of invasion of privacy and liberties.
Compliance with European law	Directive 95/46/EC of 24 October 1995 on the protection of individuals in terms of personal data processing and the free movement of data. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
Application or not of the legislation/risks	
Other	Article 29 Working Group opinion of May 2008 on the use of tracking data for the provision of value-added services. 2005 opinion: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf
These tools, young	

people and young adults	
Extent to which they are concerned, or importance of use	Unknown.
Awareness of problems and risks	Unknown.
Indifference or response	In 2008, the CNIL received 70 complaints regarding problems using geolocalisation to monitor employees' working hours.
Awareness-raising campaigns/impact	None
Good practices	Recommend that, where these vehicles are available for private use, employees be given the option of switching the vehicle-tracking function off at the end of their workday.
Campaigns to lead, aspects to cover	Inform employees of their rights through trade unions and works councils who must be consulted: prior information, limits on monitoring.
Other	
Conclusions	
Recommendations	Insofar as these practices predominantly concern employees, associations should target unions when leading awareness campaigns for application of the law and especially for: - respect of the purpose principle each time data is processed; - informing the employees concerned by these measures; - systematic de-personalisation of the data.

GEOLOCALISATION BY MOBILE PHONE

TOPIC	Geolocalisation by mobile phone
Technologies used	• Global Positioning System (GPS); • Global System for Mobile communications (GSM); • Personal Digital Assistant (PDA); • Computer IP address.
Country/zone where used	France (Europe, world).
Use	• Tracking of employees and/or company vehicles; • Tracking of people (especially children and elderly persons) and/or objects (by private individuals); • Commercial purposes: supplying services or advertising based on the individual's location. The GPS system makes it possible to know where a person or object is at any moment. It relies on a satellite network, and can retransmit this information to a centralised system. The GSM system is the digital standard for mobile telephony. It relies on widespread ground antenna coverage. The number of antennas depends on population density and landforms in the area. With the Universal Mobile Telecommunications System (UMTS) standard, it is possible to switch from the terrestrial to the satellite system. (e.g. iPhone, with integrated 3G technology). Tracking is very fast, less than 5 seconds, but not entirely precise, with a margin of error of 100-700 metres in urban areas and almost 10 kilometres in rural areas. PDAs are also increasingly used for geolocalisation, mapping and driving navigation when paired with a GPS device. High-performance integrated GPS systems are now available at a low cost, making it possible to navigate while driving with the assistance of a map that continuously indicates the vehicle's position and speed on a visual representation of the road (sometimes in 3-D), and instructions provided on the screen and read by a programmed voice. Software used to locate IP addresses – http://www.geolocalise-ip.com/ (French only) – or location based on longitude and latitude – http://www.maxmind.com/app/lookup_city
Target population and age	All ages. There is, however, a geolocalisation system dedicated specifically to children. This service, called OOTAY, is provided by the company ilico.net, and tracks children using their mobile phone (in France Orange or Bouygues mobile phones). This "geo-parental control" system is very simple. To begin, the adult signs up for the service online, and registers the child's name and phone number(s). To locate the child, the adult access their secure space (with a login ID and password) over the Internet or using a mobile phone compatible with WAP or iMode. When the adult clicks on the child's name, a request to locate the phone is sent to Orange's mobile phone network. In response, the parent receives a map indicating the geographic perimeter in which the mobile is located. This perimeter is indicated by

	a coloured circle. The service works throughout France, and is precise to within 50-150 metres in urban areas and 0.15-3 kilometres in rural areas. The CNIL validated ilico.net's file. Other tracking services also exist for private individuals: Google Latitude (now available on iPhone), and Google Maps (available on computers).
Files created	Telephony operators' files.
Contents	Subscriber management data + geolocalisation data.
Retention period	Unknown.
Who retains the data and who has access?	Operator, service provider.
Right of inspection and rectification	The operator must obtain permission from the subscriber before recording and storing data. The operator must also provide its client with a simple technical means of objecting at any time, during any connection, to the recording of tracking data pertaining to that client. Finally, the operator must provide the client with clear and complete information on the conditions related to use of this data (e.g. communication to third parties, retention period) before commencing the service.
Purpose of file	
Dangers	Geolocalisation can be misused in numerous ways, and can undermine privacy. In general, the operator uses an opt-in system, which means the user must sign up for the service and give consent or be alerted to each tracking operation. The user must also be able to easily change their mind without incurring additional costs. The opposite of the opt-in system, the opt-out, does not require the user's consent.
Other	Presented as a comfort, geolocalisation is becoming a universal application that is creeping into our everyday lives, and movement tracking is becoming a constraint to which we are growing accustomed. The potential dangers are numerous, including infringement on: The right to privacy; Liberties; The freedom to come and go anonymously.
Legislation	
	The tracking data that are transmitted from a mobile telephone to the operator, who then uses and stores them, are defined under French and European law as "personal data" because they contain information on private individuals that can be used to identify them. Consequently, the collection, use and retention of such data are subject to the French Data Protection and Liberties Act of 1978, amended by the law of 6 August 2004.
Other	

Campaigns	Information and awareness-raising campaigns on the implications of geolocalisation on infringement of liberties. Spread information on the opt-in/opt-out systems.
Recommendations	Demand that operators respect the law with regard to obtaining users' prior permission and make their terms and conditions of use sufficiently explicit. Alert the privacy protection authorities (+ France's ombudsman for children) to growing number of tools available for parent/child/elderly persons monitoring.

Biological identity

BIOMETRIC PASSPORT

TOPIC	BIOMETRIC PASSPORT
Technologies	Radio frequency identification, biometrics and databases
Technologies used	Use of three technologies: 1) RADIO FREQUENCY IDENTIFICATION - RFID (see the information sheet on the *passe Navigo*). According to Gemalto, the company that manufactures the microchips: "the data on the chip belonging to compulsory data groups 1 and 2 (zone read by an optical reader and passport's facial image) confirm the printed information. Yet the facial image recorded on the chip is of a higher resolution than the printed photograph: when it is viewed on the police check screen, it provides more accurate identification of the person." 2) Biometric data: biometrics is a technique used to verify the identity of a person by measuring one of his/her physical characteristics. The two biometric techniques are: fingerprints (eight prints) and a digital photograph of the face. Fingerprints (finger scan): the basic data verified is the impression made by the curves and grooves of the epidermis. 3) Creation of databases.
Country/zone where used	France
Use	Official document used as proof of identity required for travel to other countries (outside the EU).
Target population and age	The entire population with French nationality is concerned regardless of age. Fingerprints are not collected for children under six years of age.
Danger	RFID leads to a risk of the tracing and profiling of people. It is claimed that RFID is an invasion of citizens' privacy. (See *Passe Navigo* information sheet). Contents of the microchip: digital identity photo, digitalized prints of two fingers and all the civil status data found on the first page of the passport itself. Any other microchip reader that receives a signal from the chip could recover biometric data without the knowledge of the person concerned. Biometric data contained in the microchip and database: fingerprints: these are examples of biometric data that may change (accidents, working with chemicals etc.); and the traces of fingerprints left on various objects (door handles, windows, etc.) could be recorded without the person's knowledge and reproduced. Also, the number of distinctive points (minutiae) recorded is insufficient to prevent mistaken identifications and erroneous rejections when RFID chips are read. The databases created may be used to characterize one part of a population with great ease (risk of discrimination). (See Appendices). Biometrics is not "a miracle and universal solution".
Fichier généré	Creation of an automated personal data processing system (central file called TES), the first centralised biometric database for administrative use concerning French nationals, including the photographs of passport applicants and eight of their fingerprints, which goes beyond the provisions of European legislation. (See the French Data Protection Agency's opinion in the appendix.)
Qu'est ce qui motive	All passport applications for French nationals.

l'inscription dans le fichier ?	
Finalité du fichier/ contenu, types de données/ Risques ?	The purpose of the file is to implement procedures regarding the creation, issuing, renewal, replacement and collection of passports and to prevent, detect and curb their falsification and forgery. The personal data recorded in the automated processing system includes: a) Data concerning the passport holder: - surname, first names and, if the applicant so wishes, a name recognised by French law, the date and place of birth, and gender; - eye colour, height; - home address or place of residence, or where necessary, the municipality of the applicant or the address of the reception centre he/she lives in; - where necessary, the decision certifying the applicant's legal capacity; b) – eight fingerprints. c) – a digital photograph. d) Information on: - the application number and fiscal stamp series number of the passport; - type of passport; - stamp duty rate; - date and place of issue; - issuing authority; - expiry date; - comment, with the date, on the loss, theft, destruction, cancellation or collection; - comments on the identity papers supporting the application; - technical data regarding the creation of the passport; - information regarding the passport application: application number, place of application, application receipt date, date the passport is sent to the centre where the application was submitted, reasons for non-issue; e) Data concerning the maker of the passport and the officials issuing the passport: - id of the official registering the passport application; - id of the passport maker; - references of the officials stated under article 20 of French Order No. 2005-1726 (see § on law).
Qui le détient / Risques	The French Ministry of the Interior
Qui y a accès / Partage de fichier / Restrictions d'accès / Risques	Access: The recipients of personal data recorded in the automated processing system provided for in article 18 and in the electronic component provided for in article 2 are officials working for the French Ministry of the Interior specially appointed in the department implementing said system, and only the officials and staff specially appointed to study passport issue applications, listed hereafter: - officials in charge of the application of regulations concerning the passport at the French Ministry of the Interior and the French Ministry for Foreign Affairs, individually authorised by the Minister of the Interior or the Minister for Foreign Affairs or by officials designated by these Ministers for this purpose; - officials in the prefectures and sub-prefectures in charge of issuing the documents cited in articles 4 and 15, individually authorised by the prefect or the sub-prefect; - diplomatic and consular officials in charge of issuing the documents cited in articles 4 and 15, individually authorised by the ambassador or consul; - officials in charge of issuing official passports at the French Ministry of the Interior, individually authorised by the Minister of the Interior or by officials designated by the Minister for this purpose. For exclusive use in their assignments, staff in charge of personal identity searches and checks and passport validity and authenticity checks within the

	departments of the French police force, constabulary and customs services may access the personal data stored in the electronic component of the passport provided for in article 2 and recorded in the automated processing system provided for in article 18. Risks: Is the specific and individual authorisation procedure granting access to data recorded in the file to officials stringent enough to block access by other, unauthorised, officials? Another risk: checks of the authenticity of the documents required when applying for a biometric passport (full birth certificate, etc.) are not provided for, which prevents it from being effective against identity theft. Profiling: The automated processing system provided for under article 18 of French Order No. 2005-1726 (see § on law) is subject to data profiling with Schengen and INTERPOL information systems. This profiling concerns the data on the numbers of lost or stolen passports and on the issuing country, type and blank or personalised character of the document. Risk of profiling in future with other files, in particular those containing biometric data.
Durée de conservation	The retention period for personal data recorded in the automated processing system provided for in article 18 is fifteen years if the passport is issued to an adult and ten years when issued to a minor.
Droit de regard ou de rectification	Passports are handed over with a paper copy of the personal data recorded in the electronic component. The holder is entitled to correct the data by contacting the issuing authority. The right to access and correct personal data via the issuing authority is subject to the conditions cited in articles 39 and 40 of the French Act dated 6 January 1978 modified in 2004.
Finalité cachée du fichier et détournements/ Risques	Creation of a centralised database of fingerprints and digital photographs of all French nationals... a compulsory biometric identity card may follow.
Legislation en application	
Loi	French Order No. 2005-1726 dated 30 December 2005 concerning electronic passports. See appendix. French Order No. 2008-426 dated 30 April 2008 modifying Order No. 2005-1726 dated 30 December 2005 concerning electronic passports. See appendix. In 2008, the Ligue des droits de l'Homme filed a request with the French *Conseil d'Etat* (Council of State) aimed at the annulment of Order No. 2008-426 dated 30 April 2008 modifying Order No. 2005-1726 dated 30 December 2005 concerning biometric passports, as this Order violates the principle of proportionality provided for under article 6, 3° of the Law dated 6 January 1978. See appendix. The request is still under consideration.
Conformité avec le droit européen	Taking eight fingerprints goes beyond the provisions of European legislation, and certain EU member states (Germany for example) have implemented biometric passports without creating central fingerprint databases. In the opinion dated 26 March 2008, the European Data Protection Supervisor recommends " the Commission to propose further harmonisation measures in order to implement only the use of decentralised storage (in the wireless chip of the passport) regarding biometric data collected for EU Member States' passports"

	The appearance of new processing purposes provided for by EC Regulation n°2252/2004. The French Ministry of the Interior is now authorised to create a centralised database called TES to prevent and detect the falsification and forgery of passports (article 7 of the French Order dated 30 April 2008), in addition to the creation, issue, renewal and collection of passports. See the aforementioned request.
Autres	
Ces outils et le public jeunes et jeunes adultes	
Niveau auquel ils sont concernés ou importance de l'utilisation	Teenagers and young people are concerned, as is the entire population, when they apply for a passport.
Conclusions	
Recommendations	Associations defending rights and freedom should raise awareness among citizens and elected representatives so that: • The biometric data collected for passports is only stored on the RFID chip of the passport (as in Germany) (see EDPS). This would mean that the TES database could no longer be used to record ethno-racial data. • The government is working to improve the security of the application process as the main conveyor of identity paper fraud is the production of false supporting documents, the civil status document should be paperless and computerised so that it can be sent directly from the authority in possession of the document (town halls) to the biometric passport issuing authority. • Guarantees are given on the authorisation procedure for persons with access to the database. In addition, they should make known the fact that the relationships individuals have with the State are changed through the use of biometrics: these relationships are no longer based on identity declarations (born on:… in:… son of:… etc.) but on the individual's body.

TOPIC	BIOMETRICS
Technologies used	Fingerprint or palm print readers. 1) **Fingerprints:** each fingerprint is different. There is only one chance in 17 billion of finding two fingerprints with 17 similar minutiae. Fingerprints are read by either a sensor (live scan) or by a scan of an ink-based fingerprint image. 2) **Palm prints:** this involves capturing a 3D image of the hand, extracting several dozen minutia points and taking into consideration the length, width and shape of fingers, etc.
Country/zone where used	France
Use	Access to schools and/or school canteens. Access to companies and/or corporate canteens. Even though this chiefly concerns school and corporate canteens, the system is also being developed for school transport and libraries.
Legislation	• French data protection act dated 6 January 1978 modified on 6 August 2004. • **Directive No. 95/46/EC dated 24 October 1995** of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (http://europa.eu.int/smartapi/cgi/sga.doc?smartapi!celuxplus!prod!DocNumber&lg=fr&type.doc=Directive&an.doc=95&nu.doc=46) • **Convention No. 108 dated 28 January 1981** for the Protection of Individuals with regard to the Automatic Processing of Personal Data. French law complies with European legislation.
Target population and age	Adults employed in some companies. Young people from age six upwards. Fingerprints are not measurable before this age as they are still developing.
Retention period	Retention periods vary according to the use of the data collected. The period is defined by CNIL authorisation.
File content Purpose of file	Links with: Employee files in companies with access rights Pupil files in schools
Who retains the data, Who has access?	Access to school canteens: after rejecting the proposal in 2000, the French data protection agency (CNIL) has authorised the use of a biometric application with hand geometry and contour landmark technologies to manage access to the canteen of the Joliot-Curie lower secondary school in Carqueiranne. Access to school buildings: the French data protection agency (CNIL) published a decision dated 26 June 2008 rejecting the use of a system based on fingerprints to control access to school buildings and the presence of pupils. The agency stated that fingerprints, unlike hand geometry, leave a trace. These 'traces' may be captured without people's knowledge and used in cases of

	identity theft.
Right of inspection and rectification	These systems are subject to prior authorisation from the French data protection agency (CNIL), with the exception of the following three systems which are subject to specific authorisations: 1) Hand geometry to control access to school canteens – authorisation No. AU-009. 2) Hand geometry to control access and manage working hours and canteens in the workplace – authorisation No. AU-008. 3) Fingerprints exclusively recorded in an individual device in the possession of the individual concerned to control access to professional premises - authorisation No. AU-007. The French data protection agency (CNIL) insists that the individuals concerned be informed prior to such checks. The individuals concerned, in this case the parents acting on behalf of their children, must be clearly notified of the conditions of use, whether such checks are compulsory or optional, of who has access to the data and how to oppose, access and correct said data. As concerns employees: On 19 April 2005, the Paris regional court (*TGI*) prohibited a subsidiary of the French rail company SNCF from using fingerprints as a clocking system. The judges stated that fingerprints are morphological biometric data used to identify specific physical characteristics that are unique and permanent in each individual and that their use is an invasion of privacy. This judgment is based on the European Directive and article L. 120-2 of the French labour code.
Dangers	• Files being created without people's knowledge. • Use of the files for other purposes than those originally envisaged. • Possible tracking or profiling. • Risk of identity theft. The proposal paper (*Livre bleu*) published by GIXEL[4] (the French association for electronic component systems and smart card industries) reads as follows: Security is very often seen in our democratic societies as an invasion of privacy. Our task is therefore to help the population to accept the technologies used, including biometrics, CCTV and checks. Several methods should be developed by both public authorities and industrial players to ensure that biometric technology is accepted. These methods should go hand in hand with efforts to make the technology user-friendly, increasing recognition and adding attractive functions: children should be taught how to use this technology as early as nursery school to enter and leave the school building, eat at the canteen, and parents should have to identify themselves when they pick up their children from school. http://bigbrotherawards.eu.org/IMG/pdf/Livre_bleu.pdf (in French)
Campagnes **Communication**	Awareness of the risks: As regards biometrics in schools, the headteacher of a secondary school equipped with this system states that:

[4] Groupement des industries de l'interconnexion des composants et des sous ensembles électroniques

	1) “Parents have unanimously approved the system.” 2) “The day pupils find the hand recognition system quite fun.” This system is presented as easy, convenient and time- and money-saving: no more lost canteen or library cards. However, people who disagree are trying to make their voices heard: In November 2005, campaigners entered the upper secondary school in Gif-sur-Yvette to protest against and raise public awareness of the installation of terminals in the canteen. Their sentencing for damage to a biometric terminal encouraged reactions but proved to be a deterrent to other protests. Louis Joinet, former director of the French data protection agency (Cnil), and independent expert on human rights at the United Nations, speaks up against biometric terminals installed in schools: “*because they are trying to make three year-olds accept tracking. Because they want to tell them that it is normal that their bodies are used for checks, like animals”.* Parents and unions (teachers’ unions such as FSU, magistrates’ unions) condemn these biometric checks and denounce the dangers, shortcomings and costs, and “*reject this system because it gets children used to being checked using part of their bodies*.” *(*FCPE 34*)*. The French data protection agency (CNIL) wishes to continue working on the issue of using biometric technology with children. It plans to organise meetings with parents, headteachers and representatives of the French Ministry for Education.
Recommendations	Lean on protests from unions and parents’ associations to: Raise awareness among national and European personal data protection authorities of the dangers of using biometrics to identify people. Denounce the financial interests of industrial players, coupled with the political interests of checking citizens.

Interpersonal communications

GMAIL ACCOUNTS

TOPIC	**INTERPERSONAL COMMUNICATIONS:** **Free e-mail accounts – example: Gmail (service "offered" by Google)** Free email service offered by Google. Messages received through the Gmail account can be read using an email client (thanks to its compatibility with POP3 and IMAP protocols) or web browser. Several service features are only accessible via web browser, however.
Technologies used	Sending/retrieving electronic messages Protocols used to send e-mails: SMTP (Simple Mail Transfer Protocol) Protocols used to send/retrieve e-mails: POP and IMAP
Use	Country : France and worldwide E-mailing, document sharing, file attachments (text, sound and image) between different parties (between individuals, individuals ➔businesses, ➔public authorities, etc.). Personal computers at home or in private or public spaces (schools, universities, internet cafes etc.), businesses; laptops in Wi-Fi equipped spaces, cell phones (smart phones) ; Includes an instant messaging (chat) option. Google began "offering" this service in 2006; in "exchange", advertising is displayed which matches keywords found in message exchanges. Requirements for opening a Gmail account are minimal: users provide their first and last name and choose a user name and password. There is no verification of the name used, which could be pseudonym. Users need to read the terms and conditions to find out that "Residual copies of your messages may remain in our system, even after you erase them from your inbox or close your account".
Legislation	Google adheres to the US Safe Harbor privacy principles. According to the CNIL, Google currently refuses to adhere to European legislation on data protection for the following reasons: • considers that it is not subject to European data protection laws, despite having servers and establishments in Europe; • would like to store the personal data of internet users longer than the 6-month maximum requested by the G29, without any justification; • has made no improvements to its anonymity mechanisms despite these being insufficient; • considers that IP addresses are confidential but not personal data and can thus avoid giving its users certain rights; • shows no intention of improving and providing clarification about how it obtains user consent.
Statistics	Population profile: According to ComsCore Media Metrix, **3.6 million unique users** connected to Gmail in December 2008 (excluding public and telephone connections). 149 million internet users used this email service in 2009. It should be noted that a significant proportion of young people who do not have an internet subscription with a regular ISP have a Gmail account, accessible from any internet access point.
File content	<u>The motive behind information filing?</u> Improving service quality

Purpose of file	Google says it uses cookies “and other technologies” to “…learn about how you use Google services in order to improve the quality”. Information of a personal nature provided to create an account is stored by Google and can be combined with other information provided for other Google or third-party services to “provide a better user experience”. Google servers automatically record information when you visit our website or use some of our products, including the URL, IP address, browser type and language, and the date and time of your request. <u>Purpose of file:</u> As a favor to you, according to Google. Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail. Google computers process the information in our messages for various purposes: to format and display information, to relay advertising and related links, to prevent spam and to store our messages, as well as for other purposes linked to the Gmail service. <u>Content in the file:</u> Gmail’s Privacy Notice states: “When you use Gmail, Google's servers automatically record certain information (your messages, address book and other account information) about your use of Gmail. Similar to other web services, Google records information such as account activity (including storage usage, number of log-ins), data displayed or clicked on (including UI elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL)”.
Retention period	Initially, Google: Intended to store information for two years, then 18 months. Eventually, the period was reduced to nine months.
Who retains the data, **Who has access**?	Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information on a server outside your own country. This implies that for Google, US legislation applies As a result, Google or authorized third parties have access to this data. (Google’s) Terms of Service state that: When we entrust the processing of your personal information to third parties, we ensure that the latter do so in compliance with our privacy policy and any other appropriate confidentiality and security measures. We may also disclose certain information to third parties in limited circumstances, notably in the case of legal proceedings, fraud prevention, protection against an imminent threat, and to ensure the security of our network and services. Google only processes personal information for the purposes described in this Privacy Policy and/or the supplementary privacy notices for specific services. In addition to the above, such purposes include: ▪ Providing our services, including the display of customized content and advertising ▪ Auditing, research and analysis in order to maintain, protect and improve our services ▪ Ensuring the technical functioning of our network ▪ Protecting the rights or property of Google or our users

	▪ Developing new services Gmail is configured for information sharing and onward transfer: • When you send email, Google includes information such as your email address and the email itself as part of that email. • Google provides advertisers only aggregated non-personal information such as the number of times one of their ads was clicked. We do not sell, rent or otherwise share your personal information with any third parties except in the limited circumstances described in the Google Privacy Policy, such as when we believe we are required to do so by law. Information security: Google takes all necessary security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data. Access to personal information is restricted to only Google employees, contractors and agents who need to know that information in order to operate, develop or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations. Sharing of information with third parties: Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances: • Google has your consent. Google requires opt-in consent for the sharing of any sensitive personal information. • Google provides such information to its subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. Google requires that these parties agree to process such information based on its instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures. • Google has a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to satisfy any applicable law, regulation, legal process or enforceable governmental request, enforce applicable Terms of Service, including investigation of potential violations thereof, detect, prevent, or otherwise address fraud, security or technical issues, or protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law. If Google becomes involved in a merger, acquisition, or any form of sale of some or all of its assets, it will ensure the confidentiality of any personal information involved in such transactions and provide notice before personal information is transferred and becomes subject to a different privacy policy.
Right of inspection and rectification	Gmail users can modify the data provided to create an account. Except from the Gmail Policy Notice: You may (…) terminate your account through the Google Account section of Gmail settings. Such deletions or terminations will take immediate effect in your account view. Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems. Excerpt from Google's "Privacy Overview". We make good faith efforts to provide you access to your personal information upon request and to let you correct such data if it is inaccurate and delete it, when reasonably

	possible.
Risks	• **Direct marketing** • **Spam** • **Phishing** • **Hacking** - In October 2008 a researcher showed that he could intercept the content of a web application session such as Gmail or Facebook, read and write messages, erase or modify the legitimate user's address book, or even change his or her password. - In June 2009, 38 international experts wrote to the head of Google about Gmail's security weaknesses (+*Docs, Calendar, other free Google services*) and asked him to fix the problem. The default secured connection system (where "https" appears in the address bar) is only activated when logging on – the connection is not secured after that. The option for a secured connection is disabled by default, users are not informed, and access to choose it remains difficult (it is the last of 13 settings). Google argues that it slows down the e-mail service. Possible consequences of hacking: **Identity theft**
Awareness of risks/ communication	E-mail accounts in general According to a Senate report, a Eurobarometer survey among youth aged 15 to 24 shows that only 33% of them are aware of their rights regarding personal data; 18% know of the existence of national data protection supervisory authorities. Furthermore, only 20% of these young people consider it safe to transfer personal data over the Internet. Despite mistrust due to a lack of information, young people today are those most familiar with Internet and new technologies. Best practices: a) Since it is not mandatory, do not provide your real identity when creating a Gmail account: b) Use an anti-virus and anti-spam program ; c) Do not give personal information (e-mail address, mailing address, telephone number, family address, etc.) when signing up. Do not publish your e-mail address online (if this is necessary, certain 'tricks' can be used such as writing 'at' instead of the @ symbol, which a robot will not recognize); d) Use one specific e-mail account for online Internet services and another for e-mail exchanges with family, friends and others ; e) Change your (specific) e-mail address if you receive too much spam; f) Never reply to spam, even to complain – this reveals that the address is valid; g) Read the Terms of Service. When creating an account and choosing a password, Gmail suggests a question/answer prompt to identify a user who has forgotten their password. In the list, select the "write my own question" option; this way, 'secret question' hacking (by trying to answer stored questions) will be much more difficult (hackers must guess both the question and the answer!). To avoid 'total profiling', use another free e-mail solution, particularly if Google's search engine is used frequently.

	Only use a Gmail account for non-sensitive data. **Action campaigns:** Demand that Google produce Terms of Service that are short, legible and understandable for every user, for every application, particularly Gmail. As it stands, the Terms of Service require the reader to go back and forth between links. https://secure.eff.org/site/Advocacy?cmd=display&page=UserAction&id=433
Other	The French government, through the *Secrétariat général de la Défense Nationale* and the *Agence nationale de la sécurité des systèmes d'information* publishes advice and very detailed technical information on Internet security. Internet users should visit the following site: **http://www.securite-informatique.gouv. fr/gp_article74.html**
Recommendations	Lobby (national and European) governments and personal data protection agencies to demand that Google be subject to European law.

ISP EMAIL[5]

TOPIC	INTERPERSONAL COMMUNICATIONS: ISP Email (e.g. SFR)
Technology used	An Internet service provider is an organisation, usually a company that provides a connection to the Internet network. Use: Internet connection - network - high- or low-speed modem – WiFi. Possibilities: electronic mail (email), transfer of texts and attached files (text, sound, pictures) between different parties (e.g. individuals ➔ individuals, ➔companies, ➔government). Protocol used to send emails: SMTP (Simple Mail Transfer Protocol). Technology. Protocols used to receive emails: POP and IMAP. POP, the post office protocol, is used to retrieve email from a server. IMAP, the Internet Message Access Protocol, synchronises the contents of the inbox stored on a server with the email software every time it connects. (Unlike POP, IMAP makes it possible to connect and read emails from different computers and/or mobile phones and to still find the same folders and archived emails.) The sender and receivers are identified by their email address. The provider can be accessed from personal computers, in private or public places (e.g. schools, universities and Internet cafes), in companies, from laptop computers in WiFi hotspots, and from mobile phones (smart phones).
Country/zone where used	France/world.
Legislation	• Act No. 78-17 of 6 January 1978 on data processing, data files and individual liberties. • Act No. 2004-575 of 21 June 2004 on confidence in the digital economy (French only). • Act No. 2007-297 of 5 March 2007 on crime prevention (French only). • Act No. 2008-3 of 3 January 2008 on promoting competition for the benefit of consumers (French only). • Economic Modernisation Act No. 2008-776 of 4 August 2008 (French only). • Law on internal security orientation and programming (LOPSI): • The new Article 222-16-1 of the French penal code punishes malicious use, in electronic communications, of someone else's identity or any other personal data, with the aim of disturbing the peace of others or prejudicing their honour or reputation. It sanctions these behaviours as it does malicious telephone calls, with one year's imprisonment and a fine of €15 000. Compliance with European Law: • Directive 95/46/EC on the protection of data; • E-Privacy directive of 1997 modified by directive 2002/58/ce.
Target population and age	According to the *Observatoire des Usages Internet*, an analysis of Internet use in France published by French market research company **Médiamétrie**, in 2009, 25.9 million people used email regularly.

[5] ISP: Internet service provider

	SFR counted 3.8 million users at the end of 2008. Other source: nearly 32 million Internet users in France in July 2008 (http://www.journaldunet.com/cc/01_internautes/inter_nbr_fr.shtmlFrench only) According to Médiamétrie, young adults aged 18-24 make up 1/5 of all Internet users (Internet in general - no numbers available for email). In **1999**: 3 million Internet users in France were older than 18. In **2009**: 29 million.
Files created **Associated files**	• Commercial management file created by a private company, recording of client registration information. • Electronic communications data file that ISPs are required to keep.
Retention period	It should be noted that ISPs must retain their clients' connection data for one year. This includes: • personally identifying data; • data related to the connection terminals used; • technical characteristics and the date and time of communication; • data on supplementary services requested or used, and their suppliers; • Data identifying the recipient(s) of the communication (e.g. message headings, recipients' email addresses, subject). No information available on the destruction of these data at the end of the retention period.
Who retains the data, who has access?	Number of people that have access to these data is unknown. The ISP has access.
Right of inspection and rectification	Provided for in the French Data Protection and Liberties Act. Example: SFR terms and conditions of use. **Rulings:** Example: The CNIL recently announced its decision of 12 June 2008 to fine Neuf-Ci, formerly Club Internet, 7000 Euros. (CNIL, decision No. 2008-163, 12 June 2008.) A Club Internet user asked to access all data related to her that the ISP had retained. After being refused access she finally received some information (name, address, bank coordinates), but nothing more (namely data recorded during her calls). As authorised by the law, she went to the CNIL. After making numerous requests with no reply, the CNIL sent a letter of formal notice within a month. Club Internet announced that it was setting up a charter on personal data; one year later the charter was still at the proposition stage. As for the letter of formal notice, the CNIL received scant answers. Following these events, the pecuniary sanction of 7000 Euros was pronounced against Neuf-Ci on 12 June 2008.
Dangers	• Spam; • Marketing solicitations; • Phishing; • Identity theft; • The ISP retaining connection data as part of the fight against terrorism. • It should be noted that using company email for private purposes risks challenging the status of "private correspondence". • Art. 1 of French Act no. 91-646 of 10 July 1991 guarantees the confidentiality of correspondence sent through

	telecommunications (violation of this confidentiality falls under Art. 226-15 of the French penal code). However, the employer must have access to the resources provided to the employee and, as such, to the email system used. • Disclosure of personal data to legal authorities, with every Internet user becoming a potential suspect. Awareness of dangers According to a report by the French Senate, a **Eurobarometer** survey carried out amongst 15-24 year-olds showed that **only 33%** knew their rights with regard to **personal data**; 18% were aware of the existence of national data protection authorities. It should be noted that only 20% of these respondents believe that sending data over the Internet is safe. Despite this distrust that comes from a lack of information, young users are currently the most familiar with the Internet and new technologies.
Campaigns	Campaigns led: There are campaigns to inform young users on dangers of the Internet in general, launched by the CNIL, the *Education Nationale* and the *Forum des droits sur l'Internet* (an independent organisation for Internet co-regulation): the practical guide "*Internet et moi*" (Internet and Me) was compiled by the *Forum des droits sur l'Internet* and Okapi (a children's magazine), with the support of Microsoft, the inter-ministerial delegation for the family, and the *Collectif Interassociatif Enfance et Media* (CIEM; a federation of associations involved in childhood and the media). The guide offers a wealth of advice on the most common ways in which teenagers use the Internet and includes a 10-question quiz. "*Internet et moi*" is in conformity with the law as it stood the day of publication (25 April 2007). **"*L'Internet plus sûr, on se mobilise !*"** ('The safer Internet, mobilise yourself!'), a group composed of Microsoft, other private companies, and government agencies dedicated to the Internet, launched a campaign for the protection of privacy. Their site http://www.protegetonordi.com/ (French only) contains lots of advice, games and comics for all audiences: children, teenagers, parents and teachers. The impact of these campaigns is unknown.
Other	At the end of May 2004, Rampell Software, an American company, launched a new email service called DidTheyReadIt? This subscription service allows users to know: the date and time when an email was opened; the geographical location of the person who opened it; how many times and for how long it was opened; if the person transferred the email to other people and from which email server. It also lets users know which browser and operating system the recipient uses. The entire process takes place without the recipient(s) of the email knowing. In contrast to acknowledgement-of-receipt services provided by "classic" email programs, the recipient cannot choose to accept or refuse to send this information to the DidTheyReadIt? subscriber. The recipient is not even informed. In principle, the CNIL can only express the strongest reservations about such a process. In effect, it constitutes collecting personal information because the information recorded and transmitted concern the email recipient's "behaviour". Collecting this sort of information without the person's knowledge violates data protection rules, more specifically Article 25 of the French data protection and liberties act of 6 January 1978, which prohibits the collection of personal data through any fraudulent, unfair or illegal means.

	The CNIL stresses that violation of these provisions is punishable by five years' imprisonment and a fine of €300 000 (Article 226-18 of the penal code). As such, the CNIL points out to French companies, public services and the general public that by subscribing to DidTheyReadIt?" any person based in France is liable to prosecution.
Recommendations	Campaigns to lead: • Fight against spam, phishing and the use of data for marketing campaigns; • Motivate users to read the terms and conditions of use, and demand that the conditions be accessible to everyone (comprehensible to everyone). Advocacy campaigns: Demand to know how data retention files are processed. *Good practices* • Use an anti-virus and an anti-spam tool. • Do not communicate personal data (e.g. email, home address, phone number, family address) to "friends" on the Internet. • Do not publish any email address on the Internet. • Use one specific email address for online services and another for communicating with friends and family. • Change the "services" email address if it receives too much spam. • Never reply to spam email, even to protest: this will only confirm the validity of the address. Read the ISP's terms and conditions of use.

TWITTER

TOPIC	SOCIAL NETWORKS/Interpersonal communications
Technology used **File content**	**TWITTER** is a social networking and microblogging tool that allows users to send short messages (140 characters maximum, roughly one or two sentences) called "tweets" for free over the Internet, instant messaging or by SMS. Twitter was created in San Francisco, in the start-up Odeo, Inc. founded by Noah Glass and Evan Williams. Odeo offered a platform for hosting, distributing and recording podcasts. The initial idea was to allow users to describe what they were doing via SMS. When it opened to the public on 13 July 2006, the first version was called Stat.us and then twittr, alluding to the picture-sharing site Flickr, and finally Twitter, its current name. As opposed to a normal blog, Twitter does not allow readers to comment on the messages posted. The initial slogan was "What are you doing?", inviting users to tell what they were doing while they were doing it. Twitter then replaced this slogan with "What's happening", giving an opportunity to exchange information and links. Once connected to Twitter as a registered member, it is possible to access the tweets posted by the people the member has chosen to follow, the member's "following". For example, if user Elsa follows user Pierre, we say that Elsa is a follower of Pierre, whereas Pierre is part of Elsa's following. Twitter is an "asymmetric" social network, differing from Facebook in this sense in that users can choose to follow as many or as few of their followers as desired. Someone who wants to keep their messages relatively private can choose to make them private, in which case they can only be viewed by users whose request to be added to the list of followers has been approved. Over 50% of users update their profile either from their mobile or from tools other than Twitter ('related tools', e.g. Firefox offers a tool to publish information on Twitter) (according to Sysomos – see below). Users can communicate directly with "friends" and decide whether messages can be read by everyone (public mode) or only by other users in their networks (private mode). To create a Twitter account, users are only asked to give their name, a user name, a password and an email address. Twitter recommends that users give their real name and place of residence so that friends can find them, but this is not mandatory. Users can modify their profile or create it with these parameters: By checking the box "Protect my tweets": Only let people whom I approve follow my tweets. If this box is checked: you WILL NOT be on the public timeline Tweets posted previously may still be publicly visible in some places.
Country/zone where used	France/world.
Legislation	Twitter is governed by American law. Consequently, no protection is afforded under the French law in force. Article 5, para. 2 of the Terms of Service.

	Copyright protection.
Target population and age	France, June 2009: 10,000-12,000 registered members according to Sysomos (a Canadian social media analytics company) This figure, though still very low, should increase by 190% for Paris. According to Sysomos, the majority of Twitter users belong to the following age groups: • 31% are 15-24 years old • 35% are 20-24 years old • 15% are 25-29 years old The number of Twitter users is growing very quickly because it is so easy to use, can be connected to in various ways (e.g. Internet, telephone) and is easily enriched. If the site existed in French it is conceivable that the number of French users would increase very quickly. http://www.sysomos.com/docs/Inside-Twitter-BySysomos.pdf
Retention period	Unknown.
Who retains the data, who has access?	Twitter's terms of services provide that: • "We engage certain trusted third parties to perform functions and provide services to us, including, without limitation, hosting and maintenance, customer relationship, database storage and management, and direct marketing campaigns. We will share your personally identifiable information with these third parties, but only to the extent necessary to perform these functions and provide such services, and only pursuant to binding contractual obligations requiring such third parties to maintain the privacy and security of your data." • "Twitter cooperates with government and law enforcement officials or private parties to enforce and comply with the law. We may disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims, legal process (including subpoenas), to protect the property and rights of Twitter or a third party, the safety of the public or any person, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with the law." • "We reserve the right to alter these Terms of Use at any time. If the alterations constitute a material change to the Terms of Use, we will notify you via internet mail according to the preference expressed on your account. What constitutes a "material change" will be determined at our sole discretion, in good faith and using common sense and reasonable judgement."
Right of inspection and rectification	Profiles can be modified or deleted at any time. Twitter indicates that data indexed by search engines are no longer its responsibility. Registered users of Twitter can access, update or correct information provided by sending an email to privacy@twitterdot.com. A warning is given when data or a profile are about to be deleted These actions are final. Before deleting information, then, it is important to know that: • This action is final, and it is not possible to reactivate an account; • It is not necessary to delete your account to change the username; it can be changed in account settings;

	• Deleted accounts may remain visible on Twitter.com for a few days; • To be able to create a new account and use the same user name, phone number or email address associated with the other account, these fields have to be modified in the first account before deleting that account; otherwise, these details will no longer be valid and become unusable; • Twitter has no control over information cached in search engines such as Google.
Dangers	Twitter collects personal data on its users and shares them with third parties. Twitter considers these data as an asset, and reserves the right to sell them if the company changes hands. The privacy policy and terms of service provide that: "We reserve the right to modify or terminate the Twitter.com service for any reason, without notice at any time." "Twitter may sell, transfer or otherwise share some or all of its assets, including your personally identifiable information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. You will have the opportunity to opt out of any such transfer if the new entity's planned processing of your information differs materially from that set forth in this Privacy Policy." Due to non-stop publication of tweets, Twitter is well referenced by search engines; consequently, personal data are highlighted by search engines (unless the box "Protect my tweets" is checked). It should also be noted that it is very, almost too, easy to defame people as there are no real-time monitoring measures in place.
Campaigns	Occasional alerts when "incidents" occur, these campaigns are driven by Internet watchdogs rather than by users.
Recommendations	• Maintain the personal character of shared data. • Make user profiles inaccessible to search engines by default. • Lobby public authorities (national and European) and data protection authorities to make Google subject to European law.

TELEPHONY

TOPIC	INTERPERSONAL COMMUNICATIONS **Mobile Telephony**
Technology used	**GSM-GPRS-3G-UMTS** Exchanging different types of messages (e.g. voice, text, images) between individuals, from mobile/land phones and/or computers. This sort of communication is possible from anywhere, as long as the subscriber has access to their provider's phone network, or the network of an associated provider (especially in a foreign country). This includes: • Telephone connection (voice); • Video conferencing; • SMS (Short Message Service): short text message (160 characters); • MMS (Multimedia message service): SMS messages to which photos, sound or video can be added; • GPS; • Mobile Internet; • Email; • Television. The purpose of this type of file: • Allow operators to retain data as part of a commercial relationship with its clients, and to transmit these data to third parties directly involved in invoicing and collection; • Ensure the security of networks and installations; • Provide information to legal authorities (judicial request); • Invoicing; • Correct operation of network; • Detection and prosecution of criminal offences (Art. R.10-13 of the CPCE). In all of the above cases, the information retained is: • Personally identifying data; • Data related to the communication terminals used; • Technical characteristics, date, time and length of each communication; • Data on supplementary services requested or used, and their suppliers; • Data identifying the recipient(s) of the communication; • Data identifying the origin and location of each communication.
Country/zone where used	France/world.
Legislation	French law: • French postal and electronic communications code (CPCE; French only): Book II (legislative part, Council of State decrees, simple decrees). Current trends show generalised suspicion through the Hadopi and LOPSI II (law on internal security orientation and programming) laws. Once

	adopted, these laws will strengthen legal surveillance instruments; consequently, a decrease in the protection of privacy and personal data in general, and in telephony in particular, can be expected. • 2004 law on the protection of data. Compliance with European Law: • E-Privacy directive of 1995; • Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002/58/EC.
Target population and age	Potentially the entire population. According to a study published by the French Research Centre for the Study and Monitoring of Living Standards (Credoc; "La diffusion des technologies de l'information et de la communication dans la société française (2008)", in French only), in June 2008 78% of the French population over 18 years old, and 99% of 18-24 year olds, were equipped with mobile telephony. In June 2008, 69% of users sent SMS messages using their mobile phone, mainly students and people younger than 25. Percentage of population owning mobile phones (Credoc): • November 2001: 55% (84% of the under-25 demographic); • June 2008: 78% (99% of the under-25 demographic).
Files created and their purpose **Associated files**	Source: Guide juridique pour les opérateurs locaux et les collectivités (Legal guide for local operators and governments; French only) published 15 March 2007 by The French Telecommunications and Posts Regulator (ARCEP). Associated files: • Commercial management file created by a private company (in this case, the mobile telephone operator), recording of client registration information (see Annex 1 Art. R.10-14(I) and (II) of the CPCE); • File making it possible to ensure the security of the network and installations (see Annex 1, Art. R.10-14(IV) of the CPCE); • Electronic communications data file that mobile telephone operators are required to keep.
Retention period	One year.
Who retains the data, who has access?	Data may be retained by the operator or outsourced to external service providers. • Employees of the company that retains the data. • Legal authorities, upon judicial request. • With regard to preventing acts of terrorism, Art. L.34-1-1 of the CPCE allows for administrative requisition allowing authorised law enforcement authorities and national gendarmerie officers to obtain these data from operators and other parties mentioned above.
Right of inspection and rectification	The operator is responsible for maintaining the security of the information it retains and processes. As such, it must prevent them from being distorted or damaged, or accessed by unauthorised third parties. The provisions of the CPCE stress that it is prohibited to process personal data other than for the explicit and legitimate purposes determined, which allow, especially in the domain of electronic communications, fulfilment of

	a contract involving the person whose data is being processed. Clients' right to access and modify their identifying data processed by the operator is guaranteed. In this regard, operators also ensure that their clients benefit from rights related to directory and information services. In particular, this relates to the right to not figure on subscriber lists, not list a complete address, forbid market research based on the list and prevent reverse searching.
Dangers	• Spam; • Marketing solicitations; • Geolocalisation; • Retention of communication data; • Misuse of data for purposes other than those intended. Awareness of dangers According to the Credoc study, and with regard to **geolocalisation**, in 2008, 80% of 18-24 year olds and 53% of 12-17 year olds wanted to be able to prevent data related to their location from being communicated to companies. 20% of 18-24 year olds, and 43% of 12-17 year olds, did not want this option.
Campaigns	Existing: unknown. To lead: • Campaign on geolocalisation (and related advertising, especially during trips abroad); • Campaign on data stored by operators or their principals. What happens to them? • Campaign on the right to access and modify data. Good practices: • Turn off the telephone when it is not in use. • Carefully read the terms and conditions of use. • Do not send personal information by SMS (e.g. name, address, telephone number, credit card number). • Do not reply to an SMS from an unknown source. • Do not follow a link sent by SMS unless the source is known. With regard to SMS messages, the ARCEP has set up a special number to combat spam (site available in French only): **http://www.telecom-infoconso.fr/je-m-informe-sur/mobile/sms-indesirables.html** **Vous recevez un SMS indésirable : que faire ?** (You've received a spam SMS: what should you do?) (updated 16 December 2008) On 15 November 2008, operators in France introduced a tool to fight against spam SMS messages: 33 700. If you receive a spam SMS that tries to get you to dial a surcharged number that provides no service, forward it to 33 700. For more information (site available in French only): www.fftelecom.org/files/CPtelecom.pdf
Recommendations	Demand that operators make their terms and conditions of use accessible, readable and complete (e.g. the anti-spam number set up by ARCEP is not mentioned in terms and conditions).

Social networks and new gate keepers of communications

FACEBOOK

TOPIC	SOCIAL NETWORKS
Technologies used	FACEBOOK: Facebook is a social networking website, created in 2004 by Mark Zuckerberg and aimed at bringing together people who know each other as well as strangers.
Country/zone where used	France / World The French version of Facebook was launched in March 2008. Membership was initially reserved solely for Harvard university students. The site gradually expanded to other universities. In 2005, Facebook expanded again to high school networks. It has been accessible to the entire world since September 2006.
Legislation applicable et conformité avec le droit européen	The Terms of Use specify that the site is governed by the law of the State of Delaware. The user accepts these terms upon registration on the site. As regards European legislation: The US Department of Commerce, and in particular the National Information Agency, rapidly confirmed that the US wishes, at least in the private sector, ensure sufficient protection not through legislation but via codes of conduct and other selfregulation instruments. An initial text entitled "*Elements of Effective selfregulation for privacy Protection"* was published in 1998. Following the breakdown of negotiations since 1998 between the European Commission and the USA, the American position has changed significantly. The US Department of Commerce has published various versions of the *Safe Harbor Principles*, which are international principles in the field of security concerning the protection of privacy. These principles aim to ensure the protection of personal data transferred from a European Union Member State to the United States of America. The latest version was published on 17 March. There is, in addition, a "FAQ" section, published by the US Department of Commerce, providing guidelines on how to implement the principles. However, the site is still governed by the law in Delaware which provides less protection than French law.
Statistiques	The site currently boasts 250 million users • 11,124,780 French nationals are members (France is the 5th largest country in terms of membership numbers) • 3,665,000 are aged between 18 and 24 (32.7% of members). • 207,000 are under 13 • 1,850,000 are aged between 14 and 17 • 3,180,000 are aged between 25 and 34 Between 600,000 and 700,000 new accounts are created every day across the globe. 52% of French nationals who have a Facebook account log on at least once a week (25% log on daily). Gender distribution is relatively balanced (52.2% women and 47.8% men). Facebook's popularity has also increased as 68% of French people have heard of Facebook, a 30% jump in 2008 compared to 2007.
Cadre d'utilisation **Contenu**	Facebook is a means of communication. Users contact other users free of charge. Reasons:

Intérêt d'avoir un compte Facebook	• To widen the user's circle of "friends", • To keep in touch and communicate with friends and family, • To share videos, music and photos, • Chats via instant and private messaging. Users can enter personal data and interact with other users. Data likely to be made available on the network concerns civil status, studies and interests. Such data enables users to find or meet other users with the same interests. Together they can create groups and invite other users. The contents of the file vary according to the user. Each user chooses which information is shared with other users. Compulsory data is as follows: name, which may be a pseudonym, gender, date of birth, which may be wrong, and email address. Other information may be added: religion, political views, professional training, interests and employers. Each user has a profile page that displays the latest news concerning their "friends", and a "wall", which displays the user's news and on which friends may leave messages. Facebook offers its users optional functionalities called "applications". Users can choose which applications are displayed and can add applications after consulting the catalogue. Users can display the following on their profile page: • A list of their friends • A list of mutual friends with other users • A list of the networks that the user and his/her friends have joined • A list of the groups that the user has joined • A window to access photos related to the user's account • A mini-feed summing up the latest events concerning the user or his/her friends Facebook's terms of use provide that users grant a licence to Facebook on all user content: profile including name and photo, messages, text, information, photos, films, etc.). Facebook can also collect data from other sources.
Retention period	- The French data protection agency (CNIL) investigated the retention period of the data collected by Facebook, the latter stating that data will be stored "for a reasonable period". - Facebook stores all personal data shared on the site (as stated in the terms of use). If a member ***"chooses to remove User Content, the license granted will automatically expire"***. However, Facebook specifies that although it does not own the content, it ***"acknowledges that the Company may retain archived copies of User Content"***. Facebook justifies this by arguing that it makes the process easier should members who have left the site wish to re-register, as they do not have to re-enter their data at the time of re-registration. Members who wish to permanently delete their accounts must fill in a form.
Détention des données **Right of inspection and rectification**	As previously stated, each user can choose the content shared with others. Facebook users can configure who can view their profile, their contact details and applications in the "Privacy settings" tab. This is now easier for French users since the site has been translated into French. It is also possible to block people or groups. Users can also partially or totally block their profiles so as not to be listed in

	search engine results or even in Facebook searches (thus entering the user's name on Facebook does not display a result). There is no right to erasure of data as the details deleted are stored by Facebook. The right to correct data is only superficial as Facebook stores all the data posted on the site and it is relatively easy to retrieve even data that has been deleted. The form required to delete a Facebook account is not easy to find on the website. More often than not, users only deactivate their account.
% /de la population concernée globalement et chez les jeunes	
Tendance (mesurée / supposée)	Launched in 2004 for Harvard students, the site gradually expanded to other universities. In mid-2005, Facebook expanded again to high school networks. It has been accessible to the entire world since September 2006. Today (July 2009), the site boasts 250 million users (between 600,000 and 700,000 new accounts are created every day on Facebook).
Dangers	Facebook has given rise to controversy over the respect of user privacy. Personal information posted on Facebook may be read and used by people who were not initially intended to read it. Some companies use Facebook to collect information on their employees and recruiters use it when selecting applicants. Also, some parents use Facebook to watch over their children's private lives. The software can also use personal information posted on-line by users in order to introduce advertising adapted to their profile and may sell such data to private companies as stated in the privacy charter. This charter states that Facebook may collect information on members from external sources such as journals, blogs or other Internet sources. Similarly, the information on users collected by Facebook in order to improve its databases and enable its customers to better target their advertising by providing knowledge on the consumer behaviour and habits of each user. Therefore, third-party sites can use data collected by Facebook to send advertising targeted according to users' various profiles. The Beacon controversy: Beacon is Facebook's latest advertising software, enabling websites with a Facebook script to send information on the actions on their sites of a Facebook member to the member's friends, in their newsfeed or by placing the information on the member's profile page. This type of marketing is considered to be very effective as it uses social networks instead of directly addressing advertising at people. In response to the reactions caused by this new advertising system and to the threats its represents, Facebook's creator has apologized to users and has stated that the case-by-case opt-out system (at each new intrusion, Facebook users had to inform each company working with *Beacon that* they did not want to be part of the system), will now be replaced by an opt-in system which would apply when a user decides whether or not to be part of the system. Also, personal data may be used as part of legal investigations. To view a user's private profile or IP address (used to locate the user), investigators must act via legal requisition of the site's hoster **(**the accounts of 100,000 Facebook and MySpace users have already been erased due to

	suspicions of sex offences)[4]. There are several reasons why a Facebook account may be deleted. Firstly, Facebook may wish to avoid SPAM (therefore if it is ascertained that the same message is sent several times to various users, the account may be deleted) or because there is too much activity on Facebook (messages, photos etc). Facebook may also delete a user's account if it has reason to doubt the real identity of the user or the school or membership organisation and if the user has written provocative content. In this situation, the account is deleted unilaterally without any explanation given.
Communications	Campaigns: There are no campaigns specifically targeting Facebook in France, yet some campaigns focus on the Internet in general. There is a campaign called Internet enemies launched by "Reporters Without Borders". The general public is not aware of these campaigns, which consequently have no significant impact. Young people are generally aware of the problems related to Facebook. There is a general trend of configuring profiles to block access by strangers. There has been quite widespread reaction to denounce the dangers of Facebook recording information. A movement has been created on Facebook called "*Pas besoin d'Edvige, il y a déjà Facebook*" (no need for Edvige, we already have Facebook) in reference to the so-called French government "Edvige" personal information file which was subject to controversy. However, many NGOs working to defend human rights and privacy, such as the *Electronic Frontier Foundation* and *Privacy International,* are concerned about this new way of gathering information on users of such sites and the use of the information. It is considered even more harmful as it is developed and carried out with the assent and cooperation of Facebook users who are not necessarily aware of the dangers of such methods. Facebook employees allegedly have access to the pages of all users. At the end of November 2007, a network launched by *MoveOn* put the pressure on to defend the privacy of Facebook users and launched an on-line petition demanding that the Beacon system be deleted. As a result, a number of groups have been created on Facebook, denouncing this violation of privacy affecting the site's users. Facebook's increasing popularity is inevitable as despite the threat to certain fundamental freedoms, this social network remains very attractive and practical for most of its users.
Recommendations	Conduct campaigns aimed at national and European public authorities and data protection authorities to make Facebook subject to European legislation. In addition, request that Facebook users are able to: • permanently close their accounts, including the deletion of all shared personal data. • make user profiles inaccessible to search engines by default.

COPAINS D'AVANT

TOPIC	SOCIAL NETWORKS: COPAINS D'AVANT
Technologies used	Copains d'avant is a French social networking site owned by the Benchmark Group. It was created in 2001 and enables users to find former classmates as well as people they worked with, or with whom they were involved in associative or leisure activities. Registration on the Copains d'avant site enables users to consult member profiles. It involves filling in a form with the identity of the person and the various institutions attended. When registering on l'Internaute Copains d'avant, you enter personal data on the site's various forms. This data, such as email address or education, is necessary for the site to operate properly, but is above all personal and therefore precious. The site has an internal e-mail system and photos can be shared among members. The site's messaging system is free and only a few marginal options must be paid for such as the extension of storage space to 1 Gb for photos and 2 Gb for videos, and the option of posting unlimited searches and sending messages to several members at the same time. In 2008, the site added new free functionalities inspired by those offered by Facebook and MySpace. It is now possible for each member to display cultural interests and see which other members have similar interests.
L'utilisation	France The aim is to keep in touch with / locate former classmates.
Legislation	• Websites are subject to the French press act, the French audiovisual communication act and the French law on trust in digital economy. • The French data protection act is applicable but the sites are exempt from declarations with the French data protection agency (CNIL) when they contain personal data (however, to publish personal data, authorisation is often requested for children under 12). • The law dated 21 June 2004 which defines the online log-in system is applicable, therefore anonymity and pseudonyms are authorised as long as the hoster knows the identity of the person and can pass this information on to legal authorities. Case law is shifting towards hoster responsibility as they offer platforms that are increasingly adapted to content. Copains d'avant is governed by French law and consequently by European legislation. Application of European Directives.
Statistiques concernant la population	Ten million members were registered in 2008, making it the leading social networking site in France. According to an IFOP study published in Les Echos in 2009, Copains d'avant is still ahead of Facebook in terms of the number of registered members among the French population of Internet users.
Retention period	No information.
Qui détient ?	The French data protection agency (CNIL).

Who has access?	Access to personal data can be restricted. Profiles can be viewed by other members (unless restricted) and searches can be made using keywords (school name, town, etc.) The files are shared with third-party sites. Personal data is used for targeted advertising.
Right of inspection and rectification	Users can restrict their profiles or delete certain details.
Dangers	As Copains d'avant users are slightly older than the users of other social networks, they are a little more aware of the problems related to posting personal data. A user does not use this platform for as long as other social networks (after friends have been found, users use the site less). Anxious to protect member privacy, Benchmark Group, publisher of Copains d'avant, provides a number of tools: • E-mail addresses are never displayed on the site • If users do not want their entire information file to be viewed by all, they can control who is authorised to access it and which information is public • It is possible to limit access to photo albums • It is possible to filter some messages • Users can notify misuse if they are aware of reprehensible behaviour on the site • Users can opt that search engines cannot reference their page • Users can opt not to appear on JDN Réseau (a professional networking site) • Users can delete their accounts • Lastly, Copains d'avant files are declared with the French data protection agency (CNIL).
Communications	No campaigns
Recommendations	

MYSPACE

TOPIC	SOCIAL NETWORKS: MYSPACE
Technologies used	MySpace is a social networking website created in the United States, offering members a free personalised web space that can be used to present various types of personal data and to create a blog. The site also has a messaging system and photos can be uploaded. Launched in 2003 by Tom Anderson and Chris DeWolf, MySpace was bought out by Rupert Murdoch's group, News Corp, in July 2005. The French version of the site is on-line since mid-July. Even though MySpace can be used to meet and keep in touch with people, it is above all a music social network that is used to promote talent or share music. Users are able to contact other users free of charge (friends and groups made up of members in a region, school or university, company or with similar interests defined by the user) and share various multimedia documents with them (films, photos, texts, etc.).
Country	France / World
Legislation	• US Federal Law. • Myspace is a member of the SafeHarbor system based on a European Directive • Websites such as MySpace cannot be held responsible for the contents posted or for any criminal action committed by individuals visiting their sites. • MySpace **Terms of use:** http://www.myspace.com/index.cfm?fuseaction=misc.privacy • A bill in the United States, the "Deleting Online Predators Act" (DOPA), was submitted to Congress in 2006. It aims to limit the access children have to social networks in schools and libraries. However, this type of initiative is not a sure-fire way of solving the problem as children have many other ways of accessing these sites. • **Myspace Suicide Case** pronounced by a US Federal Court in November 2008. Lori Drew, 49 years old, was found guilty of having violated the Myspace terms of use by pretending to be a sixteen year-old boy. The site requires the information entered to be true. The case had significant impact as it has extended the 1986 Computer Fraud and Abuse Act to social networks while it was originally passed to prosecute hackers. It was the **first case of prosecution of "cyber-bullying"** which led to the suicide of a young girl.
Statistiques concernant la population	16-35 years of age. Minors represent 12% whereas one year ago they represented 25%. The 34-54 age range represents 41% as against 32% one year ago. These sites are attracting an increasingly wide audience. Launched in 2003, its popularity among young people took off in 2005.

	33% of users log on at least once a week.
Contenu du fichier	Myspace is part of the Data Availability initiative which enables users to share the data in their Myspace accounts with other sites of their choice. Myspace members can share the details of their profile, their friend list and photos and videos they post online. For the moment, Myspace limits this experiment to a handful of major sites (Yahoo, Ebay, the image sharing site Photobucket and the micro-blogging site Twitter).
Retention period	No information. However, there is a general trend of reducing the retention period of personal data. Google and Microsoft have cut this period to 9 and 6 months respectively.
Qui détient les données? **Who has access?**	Myspace judges the files and can share users' personal data with other sites. MySpace plans to offer a free parental notification application so that the parents of young Internet users surfing on MySpace can use a software program called **Zephyr** to determine which name, age and place of residence their children enter on their MySpace accounts.
Right of inspection and rectification	• Ability to block access to profiles. If the profile is not blocked, it can be accessed by everyone (with no geographical restrictions for example). • E-mail addresses can only be viewed by the administrators. • Users can post photos, add songs/videos. • Ability to block certain people.
Dangers	• Advertising: there is an opt-out option but it is so well hidden that it is difficult to find. • The sale and use of personal data is not authorised (only targeted advertising is authorised). • Relatively high exposure as there seems to be a race to have the most contacts (no real selection in contacts). • Intelligence and investigations. • Sex offences: several cases have already involved use of Myspace. • Right of publicity and right to privacy.
Campagne	No campaigns specifically targeting MySpace in France, however a study has been conducted by Reporters Without Borders called "Internet enemies". The general public is not aware of these campaigns, which consequently have no significant impact on the populations concerned. Reaction to denounce Myspace recording information on its users. In particular via press articles or dissatisfied groups on the site itself.
Recommendations	Conduct campaigns aimed at national and European public authorities and data protection authorities to make MySpace subject to European legislation.

FLIKR

TOPIC	SOCIAL NETWORKS
Technologies used	Flickr is a free photo- and video-sharing website including some functionalities at a cost. Flickr is not only popular among users that share their personal photos, it is also often used by professional photographers. Flickr was launched in 2004 by a Vancouver-based Canadian company founded in 2002 by Stewart Butterfield and Caterina Fake. Flickr was initially a set of tools intended for a multi-user Internet game called *Game Neverending.* The game was finally shelved but the Flick project continued. The first versions of Flickr were based on a Chatroom to share photos. Subsequently, Flickr focused more on uploading and filing photos. Yahoo! acquired Flickr in 2005. Only available in English for a long time, Flickr has been available in seven other languages since 2007. The main purpose is to share photos and videos. It has also become a blogging platform. Opening an account requires registering with Yahoo! Mail (which involves providing all sorts of details). Members' profiles are also subject to targeted advertising. The details entered when registering and when uploading photos (tags) are used by Yahoo! to target ads. There is a photo censorship system that could lead to controversy. The site provides both public and private storage. Users uploading an image onto the site can decide who has access to it by configuring the access controls. Images can be flagged as private, for friends and family or public. It is also possible to configure private viewing for an entire group. However, most users flag their photos as public, so they can be viewed by all, creating a huge database of photos filed by category. As a default setting, other users can leave comments on any image they are authorised to view and can sometimes add keywords for the image. As concerns the actual use of Flickr, photos are tagged so that they can be found easily with keyword searches. Similarly, photos can be organised into groups for easier searches. There is a guest pass system that enables people who do not have a Flickr account to share images.
L'utilisation	United States/World
Legislation	Data is transferred to Yahoo! Inc. on its servers in the United States or in other countries for processing or storage when the services offered on Yahoo! sites other than the Yahoo! France site are used. Users expressly consent to this when they validate their Yahoo! account registration. The transfer of personal data to the United States follows an agreement between Yahoo! Inc. and Yahoo! France to ensure the protection of user

	data. The database made up of data entered during Yahoo! account creation has been submitted to the French data protection agency (CNIL). As these details are protected by professional secrecy regulations, Yahoo! can only provide them under requisition by an authorised legal or administrative body in France, or such an authority in the State in which the details are processed and/or stored.
Statistiques concernant la population	• 20% of users own 82% of the photos on the site and the 3.7% of users with Pro accounts (not free) upload 59.5% of images. • 62% of people have no photos. • 65% have no contacts. • 87% have never posted a comment. • 84% have never received a comment. • 93% have never selected a “favourite”. • 92% have never been part of a group. • In short, only 3% of users use all Flickr functions. Even with Pro accounts, some functions are only used by a minority, such as favourites (56% have never selected a favourite) and groups (49% of pros take part). No statistics available specifically concerning France.
Retention period	No information
Who retains the data, Who has access?	Yahoo! declares the collection and processing of personal data with the French data protection agency (CNIL).
Right of inspection and rectification	In accordance with the French law dated 6 January 1978 modified, known as the data protection act, Internet users have a right to consult, modify and remove all personal data collected by Yahoo!
Finalité du fichier	Sharing photos and videos.
Dangers	The dangers chiefly involve right of publicity and the risk of finding photos online without the consent of the person photographed. As we have said, users can choose to flag their photos as public or to keep them private. Very often users flag their photos as public, creating a huge database and an even greater threat to privacy. There is also a risk of intelligence, and of false use of photos. Most users are not aware of such problems as a large number of photos are shared and users do not feel they are revealing information about themselves as much as on other social networks as the emphasis is not on personal data such as schools, universities or places of residence.
Campagnes	No awareness-raising campaigns. We must raise young people’s awareness of the future consequences of posting photos on the Internet without the consent of the people photographed. An increasing number of employers google the names of job applicants and may therefore find details on social networks.
Les bonnes pratiques	It is possible to configure profiles to avoid exposure to strangers. There is a licence to protect one’s photos, Creative commons (service at a cost). Access to justice for right of publicity problems is often difficult and expensive.
Recommendations	Conduct awareness-raising campaigns.

SKYROCK BLOG

TOPIC	SOCIAL NETWORKS: SKYROCK BLOG
Technologies used	Skyrock Blog is a social networking site offering a free personalised web space to members. The site was launched on 17 December 2002 by the French radio station Skyrock. It is also possible to create a blog, add a profile and exchange messages with other members. The site is used to create blogs devoted to members' musical compositions and has a specific space for these creations. Each blog may be personalized and it is possible to incorporate videos, but only from Youtube, Dailymotion, Veoh, Metacafe, Google Video or from the member's webcam. Since 2006 (after the arrival of Myspace and Facebook), Skyrock Blog created a system of friends and contact lists that is displayed on the blog and can be used to create reciprocal links between members. Launch of Skyblog Music which enables bloggers to post music based on the model of Myspace. There is a conversation platform called SkyMessager, and a platform to manage e-mails, Skymail. These improvements made to the Skyblog system help to compete with the major American social networks and to keep users on the site.
Use	France / Europe
Legislation	Skyrock blog is subject to French legislation and therefore European legislation. Application of European Directives. The blogs form an online communication service and are therefore subject to the same legislation as websites (the French press act, the audiovisual communication act, the French law on trust in digital economy). The French data protection act is applicable but the blogs are exempt from declarations with the French data protection agency (CNIL) when they contain personal data. However, to publish personal data, authorisation is often requested for children under 12. The law dated 21 June 2004 which defines the online log-in system is applicable, therefore anonymity and pseudonyms are authorised as long as the hoster knows the identity of the person and can pass this information on to legal authorities. It is always difficult to know whether to condemn the author or the hoster, who may be of different nationality. This may lead to difficulties in relation to applicable legislation. Case law is shifting towards hoster responsibility as they offer platforms that are increasingly adapted to content.
Statistiques concernant la	The site ranks 17th in the world, ahead of Wikipedia and Amazon. It represents 27% of French blogs.

population	The target population is the 12-24 age group. Very popular with secondary school pupils due to its user-friendliness (15 million blogs were listed in April 2008). On 7 March 2009 the Skyblog platform contained 23,000,000 blogs and 637,600,000 articles.
Retention period	No information.
Qui détient les données ? **Who has access?**	The files are shared with third-party sites. Personal data is used for targeted advertising. Ads are contextualised in relation to the Skyblog page's content. Advertising is therefore more effective as it is better "targeted".
Right of inspection and rectification	In accordance with the provisions of the French data protection act No. 78-17 dated 6 January 1978, the Skyblog site submitted a declaration to the French data protection agency (CNIL), under No. 895721 on 23 January 2004. As a consequence, users have the right to access, modify, correct or delete the data concerning them (art. 34 of the French data protection act dated 6 January 1978).
Dangers	• Intelligence and sex offences. • Use of information contained in blogs as part of legal investigations. • A Skyrock Blog sometimes contains elements that are protected by copyright without the consent of assignees. Some skybloggers have even gone as far as slander with regard to certain people: several lower secondary schools have had to deal with problems concerning pupils using the platform to malign staff, leading to exclusions and warnings issued to pupils and parents on a wide scale. • The tribunal dealing with disputes in the French public sector in Clermont-Ferrand annulled the exclusion of a pupil by teaching staff after he insulted one of his teachers on his blog. School and blogs are both private spheres, in that activities taking place in them are not meant for a wider public but for those who have reason to be part of these spheres. Therefore blogging, which is a sphere undergoing institutionalisation, must be independent from the academic sphere.
Communication	<u>Awareness of dangers:</u> • It would seem that skybloggers and in particular younger bloggers are unaware of both the dangers of slander (whatever the form) and the external criticism from a certain community of computer enthusiasts and bloggers (using platforms considered more serious and powerful such as the freeware DotClear) towards Skyrock Blogs. • Reaction of parents and the press in general. Users do not react as much as those on other networks such as Myspace or Facebook.
Campagnes	There are no campaigns specifically directed at Skyrock Blog.
Recommendations	Young people must be made aware of the risks of publishing image and texts without consent or posting slanderous content. In addition, the settings to configure a profile are not as effective as

	on other social networks. When illicit content is found on a blog, it is often difficult to make a distinction between civil and criminal law as the expressions used are not always clear. Users are not always sufficiently aware of the consequences of their actions and of the dangers of sharing personal data on too wide a scale.

Appendices List of documents

ACT N°78-17 OF 6 JANUARY 1978 ON DATA PROCESSING, DATA FILES AND INDIVIDUAL LIBERTIES (Act78-17VA-loi-INFOR&LIBERTES-ver-EN.pdf)

PASSEPORT ELECTRONIQUE 2005-2008-FR.doc (French)

IRIS et LDH passeport bio requete + mémoire Conseil Etat.doc (French)

PNR - Résolution du Sénat n° 84 du 30 mai 2009.pdf (French)

PNR - EDPS.pdf (EN)

Resolution-Societe-de-surveillance-congres-2009.pdf (French)