

Foreword

Gusts of wind, rain showers and sunny spells...

Alex Türk, CNIL Chairman

The virtue of the climate metaphor resides in its ability to reflect the unpredictability of current events, their abruptness and brutality at times, as well as their precarious serenity. Gusts of western winds, firstly, blowing from the US Administration determined to impose an extraterritorial effect to its homeland security laws. Thus, in pursuance of an agreement signed by the European Union and the United States government in July 2007, personal data on all air passengers flying to the US on European airlines are now transferred over to more than a dozen US state agencies, in the name of the legitimate fight against terrorism. This transfer of Passenger Name Records (PNRs) occurs without any control by Europeans, the records are to be kept for a retention period of 15 years and may lead to a refusal by officials to allow any persons on board, who will then find it extremely difficult to get any explanation or much less to uphold their rights. Furthermore, the data transferred may “*if necessary*”, as assessed by fully sovereign US authorities, include “*sensitive*” data such as dietary preferences, health condition, political opinions and ethnic or racial origin. In spite of the staunch opposition from the European Parliament and European national data protection authorities, this EU-US agreement on PNRs was nevertheless signed. It leaves in its wake the bitter aftertaste of the failure of our model that intends to reconcile liberty with security, without sacrificing either.

Another gust of wind, from within our country this time, was the outcome of a commission charged with reviewing the reform of our national institutions, chaired by former Prime Minister Edouard Balladur, who recommended dismantling CNIL and replacing it with a “Defender of Fundamental Rights” gathering other authorities such as the Ombudsman of the Republic, the HALDE (High Authority against Discriminations and for Equality), the Defender of Children or the General Penitentiary Supervisor. This proposal was founded among other on the idea, though entirely erroneous today, that our Commission was intended as a mediation authority between citizens and public administrations. Yet, since the enactment of the Law of 6 August 2004, nearly 70% of the decisions adopted by CNIL address the private sector. CNIL has been endowed with powers of consultancy, in situ auditing and evidence verification, powers that the Commission intends to expand, in addition to a sanctioning power such that the Conseil d'Etat (or Council of State, administrative Supreme Court in France) recently qualified CNIL as a full-fledged “jurisdiction”. Hence, CNIL is no longer merely an authority in charge of issuing opinions on public records, but rather a genuine regulator, and a regulator of the private sector first and foremost. Thus, how could our citizens benefit, in term of protection of their liberties, from the disappearance of a collegial and jurisdictional body, to be replaced by a single person empowered with competences so broad that he/she could not reasonably be expected to exercise them adequately? It would be an understatement to say that I find the proposal questionable.

Then came the rain showers, the true genius of France! For several years now, the country has been questioning the efficiency of its republican integration model and addressing the necessity of combating discriminations. Yet, in order to fight discriminations, is it not indispensable to be first in a position to measure them? And to this purpose, is it not necessary to conduct a statistical analysis of differences, to assess our social, ethnic, religious, cultural or other diversity? But then, which criteria and which methods should be used to analyse this diversity? Who could or should do it? How can we reconcile the

necessity to gain better insights on our society with the French “Data Protection and Liberties Act” (Loi informatique et libertés) prohibiting the collection of data revealing “*directly or indirectly the racial or ethnic origin*” of people? This is a delicate issue that touches upon the very quintessence of our identity, our conception of the Republic, the way we perceive ourselves and are perceived by others.

Faced with such challenges, CNIL resolved to initiate a debate backed by a *ad hoc* committee. This working group conducted over sixty hearings on these issues and collected the views of all stakeholders: researchers, trade unions, representatives from the main religions, community associations, entrepreneurs, etc.

These proceedings ultimately led to the publication on 15 May 2007 of a series of 10 recommendations, one of which aimed at amending the data protection act in an attempt to facilitate research on assessing diversity, discrimination and integration, while both strengthening the protection of individuals and their personal data and enhancing the scientific quality of surveys. These recommendations were greeted with unanimous appreciation at the time. In turn, two Members of Parliament, who also sit on the Commission, proposed an amendment to the law during the Parliament session discussing a bill on “Controlling immigration, integration and asylum”. Alas, yesterday's truth was no longer true! What had emerged as a consensus proved, to our sad surprise, to turn into controversy. Commentaries closer to lampooning than real discussions prevailed over the deeper debate on the legal and technical substance of the issue, most likely too subtle for many to comprehend... In its decision of 15 November 2007, the Constitutional Council censored this amendment, judging it to be “*unrelated*” to the data protection act. The Council further considered that “*while data processing required to conduct research on the diversity of origins may look at objective data, it may however not rely on ethnic or racial origin, which would violate the principle stated in Article 1 of the Constitution*”. In its concern to fully comply with the ruling of the Constitutional Council, as required from any public authority, the Commission was however confronted with the helplessness of the scientist community faced with the complexity of this decision, while a number of renowned public agencies simply froze all research on the topic for fear of being in violation of the ruling. Educational efforts will therefore be needed and should be initiated forthwith to reassure the French research community and enable it to pursue its work in full serenity. I am very pleased to see that a recent addendum to the “Cahiers du Constitutionnel” (Issue No.23) is addressing the subject.

As for sunny spells, the first ray came shining from across the Atlantic, with the settlement of the SWIFT case. I shall not dwell, for lack of room here, on the questions raised by the issue of direct access by US authorities to numerous European banking data, such as contract amounts, beneficiaries, issuing companies, and all sorts of data that may have an indirect link with the combat against terrorism, but also contain a real risk of closer ties to industrial spying. Thanks to the joint efforts of national data protection authorities (DPAs) in the EU, the database of the Belgian-law company currently located in the USA will be repatriated to Europe, after which the US authorities will no longer be entitled to access its data related to intra-European transactions. This is a major victory in an issue close to the PNR topic, and emblematic of a certain American unilateralism.

The second ray of sunshine emerged, and it should be highlighted, from the significant budgeting efforts allocated by the French government. Though, with 10 new jobs created in 2007 and 15 in 2008, the Commission is well engaged in increasing its staff, we still remain far behind our British, German or Spanish peers. Naturally, this momentum will continue, but it will need to involve a reorganisation of CNIL regional branches. With additional duties including advising enterprises and public administrations, coordination of a network of “Data Protection Correspondents”, investigation of complaints and auditing, an inter-regional decentralisation will be required in order to bring the Commission closer to the realities of business activities, to improve its responsiveness and facilitate its access to citizens.

Within a year, on two occasions, two politically antithetical organisations, the Baladur Commission and the “Alternative” movement who invaded the Commission offices last December 14, proposed to eliminate CNIL altogether. What lessons should we draw from this? I personally see three lessons to be learned. The first lesson is that such events attest at the very least to one important thing: namely the independence of our Commission. Indeed, there is nothing more irritating than an independent institution whose positions are never fully satisfactory for any one interest group, whatever it may be! The second lesson is that independence has its price, which may prove to be high at times, but should always be preserved. Last but not least, the independence of the Commission is also the fruit of its 30-year long experience. The 30th anniversary of CNIL's creation will be an ideal opportunity to pay tribute to it, on the occasion of the International Conference of Data Protection Commissioners scheduled in Strasbourg on 15 to 17 October 2008.

The conference will take place in the amphitheatre of the Council of Europe and will be jointly organised by CNIL and its German counterpart who will also celebrate its 30th anniversary. It will address the topic of *“How to protect privacy in a borderless world”* before 600 participants from all over the world. Representatives from enterprises, associations, data protection authorities and Governments will be debating, in this era of “Facebook” and of the convergence of technologies, of the anguish-generating question of whether the realm of privacy has become an endangered space. France who pioneered the debate on this subject back in 1978, was duty bound to raise these issues of privacy protection to a level of current relevance, namely the international level. See you all in Strasbourg!

Chapter 1 2007 Highlights

MEASURING DIVERSITY: TEN RECOMMENDATIONS BY CNIL

Everyone agrees on the necessity to combat discriminations. Yet, in order to fight discriminations, it is indispensable to be first in a position to identify and measure them. And to this purpose, which criteria and statistical analysis should be used? Who could or should do it? This is a complex and delicate issue.

Complex because, as observed by the Commission, such a “measurement of diversity” has given rise to a genuine “methodological bloom”, with researchers and statisticians demonstrating great imagination on the subject, while not necessarily agreeing on the tools to be used.

Delicate because it touches upon the very quintessence of our identity, our conception of the Republic, the way we perceive ourselves and are perceived by others. Delicate as well because it should not be allowed to challenge the fact that the concept of race has no scientific value whatsoever.

Following the publications of initial recommendations on the subject in July 2005, CNIL investigated the issue in greater depth by conducting over sixty hearings of scientists, statisticians, trade unions, representatives from the main religions, community associations, qualified experts, entrepreneurs and other stakeholders.

These hearings revealed a broad diversity of views, including divergences of opinions, and highlighted the difficulty of reaching a consensus on the subject.

One key finding nevertheless emerged for CNIL: France needs to upgrade its statistical apparatus, and solutions can already be proposed to advance our knowledge of our society, thereby improving the fight against discriminations.

To this purpose, CNIL published in May 2007 a list of ten recommendations greeted favourably for their pragmatism, balance and bold fairness.

DID YOU KNOW THAT...

Sensitive data: What does the law say?

Under the terms of Article 8 of the French Data Protection & Liberties Act (Loi informatique et libertés), the following data are regarded as sensitive and subject to special protection measures: **“...personal data revealing directly or indirectly the racial or ethnic origin, political, philosophical or religious opinions, trade union affiliation, or related to the health or sexual life of individuals”**.

Processing of such data is prohibited, except under exceptions provided by the law, e.g. if:
— statistical processing is conducted by INSEE (national statistics agency) or by a Ministry's statistics department, and authorised by CNIL,

- express consent has been secured from the individuals concerned, and a declaration issued to CNIL,
- the survey presents a character of public interest and has been authorised by CNIL.

What types of data are considered by CNIL as not covered under Article 8 of the Act?

Address, nationality and birth place are not regarded by CNIL as “sensitive data” within the meaning of Article 8 of the Law.

Data concerning the birth place of an individual belong to the Civil Registry and are regarded as “objective data”.

The Commission nevertheless keeps a close watch on processing of data related to nationality and birthplace in records, and the relevance of such data collection must be duly grounded on a case per case basis by the data controllers.

Key points of CNIL recommendations

- It is indispensable to allow researchers to gain an easier access to staff records, administrative files and public statistics databases, in full respect naturally for data protection.
- In order to assess the reality of discriminations experienced, it is also necessary to conduct questionnaire-based surveys with the relevant individuals. It should be possible to ask questions about nationality and birthplace of individuals and their parents, provided that answers are optional, based on self-declaration and kept confidential. It is also important for individuals who feel they were victims of discrimination, to indicate on which criteria they believe such discrimination is based (e.g. physical aspect, language, name, etc.).
- In addition, an analysis of first names and surnames may prove useful to detect any discriminatory practices under certain conditions, i.e. provided that it does not lead to a classification by ethnic or racial categories.
- In this respect, CNIL retains many reservations on the creation of an “ethnic-racial” master record. A majority of the individuals interviewed during the hearings remain hostile to such a classification. The current reluctance may be explained by numerous reasons, i.e. risk of comforting stereotypes, of stigmatisation, of classification filled with uncertainties or being non-scientific, reductive or approximate, all grounds motivating extreme reservations on the issue. The Commission feels in particular that any decision to be adopted on the principle of creating such a classification, should its use become compulsory for purposes of public statistics or population census for instance, would fall under the competence of lawmakers under the control of the Constitutional Council.
- Lastly, it is necessary to amend the Data Protection Act in order to improve the protection of personal privacy and sensitive personal data, by guaranteeing the scientific nature of research on the subject and by bolstering CNIL's control over the research records for which mere prior individual consent should not be regarded as sufficient.

Sequels to CNIL's recommendations

Michèle Tabarot, MP from Alpes Maritimes, and Sébastien Huyghe, MP from the Nord county, and both CNIL members, proposed an amendment to a bill under discussion at the Parliament on immigration,

integration and asylum control, drafted to implement one CNIL's ten recommendations. This amendment was intended to call for CNIL's authorisation to any processing of data revealing directly or indirectly the racial or ethnic origin of individuals for purposes of research designed to “*assess diversity of individual origins, discriminations and integration*”. In an effort to guarantee the scientific quality of such research, the amendment planned for CNIL to have the option of referring cases to a scientific committee to be appointed by decree. In order to avoid creating yet another body, it considered the possibility of referral to the existing scientific council of the Consultation Committee on Data in Human and Social Sciences created for the purpose of advising the Ministries of Economy, Employment, National Education and Research.

This latter provision was the subject of heated debates and controversies, at times far remote from the actual subject matter of the amendment, but was nevertheless voted by the Parliament, although it was later appealed before the Constitutional Council.

In its decision issued on 15 November 2007, the Constitutional Council ruled the amendment in violation of the Constitution, judging that this provision was “*unrelated*” to a bill dealing with the control of entry and residence of foreigners in France.

Regarding the substance of the amendment, the Council further considered that “*...while data processing required to conduct research on the diversity of origins, discrimination and integration may look at objective data, it may however not rely on ethnic or racial origin, which would violate the principle stated in Article 1 of the Constitution*”.

While this ruling appears to definitely prohibit the creation of any ethnic/racial master record in France, which is in line with the wishes of CNIL, it however keeps open the question of what type of research can be carried out today in order to assess and measure diversity, discrimination and integration. A response to this open question would be of utmost interest to the research community.

We can only hope that 2008 will be a year of appeasement, providing for opportunities to examine, in full serenity, research projects intended for no other purpose than to improve insights and knowledge on our society and support the fight against discriminations.

CNIL's 10 Recommendations on Diversity

- provide broader researchers' access to statistical data bases and administrative records,
- use “objective data” related to the ancestry of individuals (nationality and/or birth place of parents) in surveys to assess diversity,
- do not incorporate data on personal ancestry in corporate or administration records (staff and users/customers),
- conduct research on “perceived” discriminations, including the collection of data on the physical aspect of individuals,
- accept, under certain conditions, that first names and surnames be analysed in order to detect any potential discriminatory practices,
- amend the Data Protection & Liberties Act (Loi informatique et libertés) to improve the protection of sensitive data, by guaranteeing the scientific nature of research and harmonising control procedures on research files,
- oppose the creation of a national “ethnic and racial master record”,
- resort to trusted expert third parties to conduct research on diversity assessment,

- guarantee confidentiality and anonymity via the use of anonymisation techniques,
- guarantee the effective enforcement of the rights granted under the Data Protection & Liberties Act by ensuring full disclosure.

ADVICE FROM CNIL

In order to ensure both the protection of privacy and the scientific rigour of research assessing diversity or discrimination, CNIL recommends that institutions wishing to conduct such studies call on the expertise of independent consultants (e.g. research institutions) who are also “trusted third parties” in a position to guarantee full data confidentiality and anonymity of individuals when the results are published. In this respect, CNIL believes that public authorities should encourage a more systematic recourse to encryption and anonymisation technologies.

Individuals surveyed should be perfectly informed of the goals and conditions of the survey, of the optional nature of responding to the survey, as well as of their rights of opposition, access and rectification. Such prior information, though essential, is too often neglected. Yet, on issues as sensitive as assessing diversity or combating discriminations, it constitutes a key factor to secure the acceptance, trust and unqualified participation of everyone.

Likewise, in the event of surveys conducted on labour issues, consultation of personnel representation bodies is highly recommended. More generally, it is advisable to announce publicly the launch of national surveys in order to raise the population's awareness on these topics.

FOR ADDITIONAL INFORMATION ON THE COLLECTION OF ETHNIC DATA IN EUROPE, see research report on “*Ethnic Statistics and Data Protection in the Council of Europe Countries*” authored by P. Simon (INED) and published by the Council of Europe's European Commission against Racism and Intolerance (ECRI) - October 2007, accessible at www.coe.int/ecri.

CNIL reports and recommendations are accessible at www.cnil.fr.

MANAGEMENT OF CENTRAL RECORDS ON CREDIT AND HOUSING

Central credit record or “positive” record

What is it?

All data on the financial status of individuals, whether or not they have outstanding debts, are retained in a central credit record, commonly called “positive record” by opposition to the “negative record” containing only credit-related payment incidents.

The creation of data files enabling all players in a given business sector, whether credit institutions or professional lenders, to obtain information on risks linked to personal solvency and credit worthiness is followed up by CNIL with sharp vigilance in view of the obvious risks of social exclusion for the individuals concerned.

The question of the legitimacy and proportionality of introducing a “centralised positive credit record” addresses both the issues of breach of privacy and of cost and efficiency. The Commission has always refused to recognise any legitimacy to the implementation of such centralised records in the absence of any specific legal framework (see Report on “Centrales Positives” of January 2005; Activity Report 2005). It considers that the lawmaker alone has competence to decide on the social usefulness of a “positive record” as related to credit issues, and to define the purposes and contents of such a database. In line with this stance, CNIL refused to authorise the creation of a centralised credit record requested by Experian (Decision of 8 March 2007).

What about the legal right to housing?

CNIL further refused to authorise the company Infobail to process two databases intended for information to real estate professionals, related to inventories of tenants with unpaid rents and of tenants meeting their rent payment obligations. The Commission considered that such data records could violate the “legally enforceable right to housing” voted by lawmakers who have sole competence to decide on the compilation of both “negative” and “positive” records in housing matters (Decision of 10 July 2007).

Questions to Philippe Nogrix:

Senator of Ille-et-Vilaine

Commissioner in charge of the “Currency and Credit” sector

Why did you refuse to authorise the Experian centralised credit record?

The rejection was based on three grounds:

- data covered under a legally protected confidentiality, i.e. the banking secrecy, would have been massively transferred, without any legal protection framework, to a service provider not bound by banking law and whose business is not bound by the rule of banking secrecy,
- clients would not have been informed under satisfactory conditions of the consequences of signing a release clause waiving the banking secrecy,
- the transmission, to the centralised record member institutions, of data relative to an individual for purposes of processing a loan application, to be supplied in the form of a highly detailed report listing outstanding loans or loans repaid within at least the past three years, would have enabled the economic profiling of the private individuals concerned. Such data are liable to be retained in the computer files of the recipient credit institutions and could therefore end up being used for reasons other than processing a loan application, in particular for commercial purposes.

Yet, CNIL has authorised data exchanges within banking groups. How is that different from the Experian case?

CNIL has indeed authorised several subsidiaries of banking groups, specialised in consumer credit (Crédit Agricole in 2005 with Finaref and Sofinco; BNP Paribas in 2006 with Cetelem and Cofinoga) to share data on their borrowers for purposes of bad debt prevention, based on five criteria, with which Experian was unable to fully comply:

- legitimacy of purpose: i.e. prevention of fraud and bad debts;

- occasional and restricted nature of data exchanges between the credit institutions: no centralised database is created. Client records kept by the institutions cannot be fuelled with any data transferred via the query system;
- quality of institutions granted authorisation to exchange data: all are consumer credit specialist companies, hence all bound by the banking secrecy;
- existence of a shared financial risk between these institutions, reflected in an effective control by certain companies over others, or in third-party risk management;
- explicit authorisation given by the client to share data covered by the banking secrecy, requiring among other that the client be clearly informed of the purposes and recipients of the shared data.

Last minute

At a hearing before the Commission of Economic Affairs at the French Parliament on 16 January 2008, Alex Türk testified on the growing importance of CNIL's economic regulation power. He reviewed the major issues emerging in this sector, and stressed that the technologies used raise significant challenges to privacy protection. Thus, techniques of biometric tracking, video-surveillance and geo-location raise the question of respect for workers' rights.

The cases of Discovery (transfer of data contained on hard disks belonging to French employees to the US), Swift (transmission of banking data to the US) and PNRs (transmission of data on airline passengers to US security agencies) highlight deeply diverging views between Europeans and Americans regarding the level of data protection. The mechanisms set up in the United States to reinforce the fight against terrorism raise fundamental questions on issues of data protection or even on the economic sovereignty of the states.

As regards centralised credit records, the Commission feels that it has exhausted all possible investigation avenues and that it is now up to lawmakers to decide on whether to create such a system.

REGULATING BIOMETRICS

Biometrics

What is it?

The term of biometrics designates all computerized technologies enabling the automatic recognition of an individual based on physical, biological or even behavioural features. Biometric data are regarded as personal data since they enable the identification of an individual. Most of them share the characteristic of being **unique and permanent** (DNA, fingerprints, etc.).

Key figures 2007: a boom in the number of requests

In 2007, a total of 515 biometric devices were submitted for authorisation to CNIL, i.e. an increase of over 43% versus 2006.

Among them, 449 requests were subject to an “undertaking” with the biometric guidelines adopted by CNIL in 2006 in order to frame its utilisation and simplify the notification process for some biometric devices (unique authorisations):

- 90 devices use hand geometry for access control, working time management and food catering at the work place;
- 275 use fingerprints recorded exclusively on an individual device for access control to the work place;
- 84 use hand geometry for access to the school cafeteria.

The Commission also reviewed 66 requests not covered under the scope of application of the above-mentioned single authorisations: **the application was denied for 21 devices**, while 45 others were authorised.

In addition, over 120 applications for authorisation are still currently under investigation by the Commission.

As a reminder:

- in 2005, CNIL authorised the use of 34 biometric systems and rejected 5
- in 2006, 351 were authorised and 9 rejected
- in 2007, 494 were authorised and 21 rejected

Biometric IDs

Biometric visa or VISABIO

On 10 July 2007, CNIL issued an opinion (Decision No.2007-195) on a draft decree referred by the Ministry of Home Affairs, relative to the creation of a master record of foreign nationals applying for a visa.

The new biometric visa system called VISABIO, implementing the experiments conducted since 2004 under the BODEV pilot project, should concern over two million foreign nationals from countries subject to visa obligations each year. The system under consideration provides for the collection and retention of biometric data in a centralised base (digitised facial photos and ten fingerprint scans), combined with identity data previously collected during the visa application procedure.

While noting that the use of biometric data may offer strong benefits to check the identity of ID card holders and authenticate IDs, the Commission felt however that the system should be framed by strict guarantees. CNIL regretted in particular that no consideration was given to the possibility for card holders to simply retain their own biometric data on their personal ID card, an option that would raise fewer problems from the personal data protection point of view, since in this case, only the data subjects own the device onto which their personal data are recorded.

The Commission also stressed that the collection of fingerprints of minors from the age of 6 could not be regarded as a mere technical measure and that its very principle deserved to be broadly debated.

Biometric passport

The issue of biometric passports was referred by the Ministry of Home Affairs to CNIL for review in the autumn of 2007 and the Commission issued its opinion on the draft decree on 11 December 2007 (Decision No.2007-365).

The decree intends for France to be in a position, prior to 28 June 2009, to issue passports fitted with an electronic component containing not only the digitised facial picture but also images of two fingerprints, in compliance with the provisions of the European Council Regulation of 13 December 2004.

Concurrently, it provides for the retention of the passport applicant's digitised facial and eight-fingerprint images in the existing passport management record called "DELPHINE", which would lead to significant changes to this database.

The Commission expressed a number of reservations about this project, finding that the system under consideration would lead to the implementation of the first centralised bank of biometric data on French nationals for administrative purposes.

CNIL reminded in particular that processing of such data, in an automated and centralised form, would be acceptable only to the extent that it may be justified by a compelling necessity linked to national security or public order.

In this respect, the Commission considered that the purposes claimed, however legitimate, i.e. improving the procedures for issuance and renewal of passports along with combating ID fraud, failed to justify the national-scale retention of biometric data such as fingerprints, and that the type of data processing involved would cause excessive prejudice to individual liberties.

Furthermore, the retention of digitised facial and fingerprint images in a central database appears disproportional with the purposes, in spite of assurances from the Ministry of Home Affairs who stressed that it would be impossible to conduct any identification searches from the digitised fingerprint images (i.e. it would not be possible to retrieve civil registry data on individuals based on their fingerprints) and that the system contained no facial recognition device based on the digitised photos (i.e. it would not be possible to retrieve civil registry data on individuals based on their facial image).

Lastly, CNIL regretted that this new procedure framework was to be defined via a regulatory rather than legislative process (i.e. Government decree versus law voted by Parliament), since the changes introduced by this draft decree are much more substantial than actually required by France's European commitments. The scope of this reform and the significance of the issues at stake would undoubtedly have justified a law to be proposed before Parliament, enabling a broad public debate on the subject.

Did you know that...

The very first biometric passport in France should be issued in October 2008. As of 28 June 2009, all passports issued by French authorities will need to comply with the requirements of the European Council Regulation of 13 December 2004.

Research programmes

On 18 January and 4 October 2007, CNIL authorised for the first time three research programmes in the field of biometrics. The first 2 approvals concern public research projects submitted by the University of

Evry Val d'Essonne and the Groupement des Ecoles de Télécommunications (GET). These programmes address the following topics:

- assessment of biometric recognition processes;
- compilation of “multimodal” biometric databases, i.e. combining the use of several biometric techniques (2D and 3D facial images, iris, fingerprints, hand geometry).

The third authorisation was granted to a European project coordinated by Sagem Défense Sécurité in a consortium with 12 partners. The purpose of this research project is to improve 3D facial recognition systems and the security of biometric data.

These research programmes, relying on volunteer participation, are of major importance since they provide CNIL with sources of reliable assessments on state of the art techniques. The reports published on research findings will be made available to the Commission.

Voice recognition and vein pattern recognition

In 2007, CNIL also investigated its very first request for installation of a voice recognition system, designed to secure and facilitate the management and resetting of passwords used to access the IT system at Michelin. The process can generate and reset the passwords automatically, in particular in the event of forgotten passwords. The Commission reviewed the system to ensure that adequate information was supplied to the personnel and that all efforts were made to guarantee data security and prevent any risks of identify theft.

Similarly on 8 November 2007, CNIL reviewed for the first time five devices based on finger vein pattern recognition (VPR) designed to control access to premises or IT systems. Following an in-depth technical expertise of the vein recognition technology, the Commission reached the conclusion that, in view of the current state of the art, vein pattern recognition **is a traceless biometric process** generating data that can be recorded in a database without any particular risks in terms of data protection.

Traceless or traceable biometrics

What is it?

Among all biometric data used currently, some data present the possibility of being captured and used unbeknownst to the data subjects. Such is the case for instance of genetic prints, since each of us involuntarily leaves behind traces, sometimes even minute, of our body, from which DNA can be extracted. This is also the case for fingerprints whose traces we leave behind us in our daily life and can be exploited with variable ease.

Conversely, other biometric data do not show this same characteristic, at least not at the current state of the art of this technology: this is the case for instance for finger vein pattern or hand geometry recognition, since such biometric data leave very few traces or even none in our daily life.

Traceable biometrics therefore requires close vigilance to ensure the protection of the data subjects.

An analytical scale for the use of fingerprints

CNIL issued its very first opinion in 1997 regarding a device based on fingerprint recognition. A decade later, the Commission felt it was necessary to clarify its position on the subject.

A document was therefore published recently, presenting the major criteria grounding the Commission's decisions to authorise or reject the use of systems based on **fingerprint recognition with recording of data in a scanning/matching device or on a server.**

The analytical scale derives from the following observations:

- fingerprinting is a traceable biometric process. Each person leaves traces of fingerprints in most circumstances of daily life (e.g. on a drinking glass, a door handle, etc.), which can be exploited with variable ease;
- **such “traces” may be captured unbeknownst to data subjects and may be used among other** for purposes of identity theft (a copy of the fingerprint can be used to fraudulently deceive a fingerprinting recognition device).

Consideration for these characteristics and for their related risks has led CNIL to differentiate between the various devices based on the fingerprint storage method:

- Storage on an data subject device (e.g. chip card or USB key) = limited risk since **the data subjects keep full control over their biometric data** which cannot be used for identification purposes without their knowledge.
- Storage in a scanning/matching device or on a server = higher risk, since data subjects lose control over their data held by a third party. In the event of intrusion into the system, all fingerprint data can be accessed.

Accordingly, the Commission does not authorise the use of devices based on fingerprint recognition with data recording in a database, unless the use of such devices **is duly justified by compelling necessity of security and fulfils the following four prerequisites:**

- **the purpose** of the device must be **restricted to access control for a limited number of persons to a specifically delimited area** constituting or containing a **major concern over and above the basic interests of the organisation, such as protection of physical integrity of persons, property and facilities, or integrity of certain data.**
- **proportionality:** it is important to know **whether the proposed system is the most suitable for the previously defined purpose** with regards to any risks it may involve for personal data protection and as compared with other potentially usable systems;
- **security:** the device must enable both a reliable authentication and/or identification of data subjects and offer all guarantees of security to prevent any data disclosure;
- **information of data subjects :** it should be conducted in full compliance with the Data Protection Act and, as appropriate, with the Labour Code.

[Cross perspectives on the analytical scale](#)

[François Giquel](#)

Vice-President, Honorary Legal Counsellor to the Cour des Comptes

Commissioner in charge of the Justice sector

[Didier Gasse](#)

Legal Counsellor to the Cour des Comptes

Commissioner in charge of Telecommunications & Networks and European & International Affairs sectors

What were the triggering factors that drove the Commission to clarify its doctrine on fingerprint databases?

F. Giquel: In view of technological breakthroughs in biometrics and of the diversity of circumstances, it was felt essential to clarify, as a reminder, the main criteria used by CNIL to investigate applications for authorisation.

It was also necessary to help companies, public administrations or local authorities considering the installation of such systems to ask themselves the relevant "Data Protection"-related questions prior to the decision making and application filing processes.

What justifies such special attention from the Commission to this type of devices?

D. Gasse: Unlike any other identity-related data or any other personal data, biometric data are not assigned by any third party or chosen by the data subject: they are generated by the human body itself, they designate or represent the human body as unique and immutable, unlike any other. Such data therefore belong to the person who generated them.

Hence, it is easy to understand that any possibility of misuse or misappropriation of these data would engender a major risk for that person's identity. Entrusting a third party with your biometric data and allowing that third party to retain them is therefore never a trivial or inconsequential matter, particularly since fingerprints are traceable biometrics that can be captured and used without the person's knowledge.

What are the criteria selected by the Commission to evaluate the proportional nature of a system based on the recording of fingerprints in a database?

F. Giquel: As a general rule, the purposes of fingerprint storage in a database can always be achieved via a different technology based on fingerprint storage on an individual device (e.g. smart card). Nevertheless, a centralised database may be of benefit whenever access must be provided at any time and immediately, or to respond to emergency situations requiring a timely intervention.

D. Gasse: It should also be noted that, whenever we deal with situations where security is the key issue, we also look at the relevance, adequacy and non-excessive nature of fingerprint database systems, as compared with the number of data subjects: the more restricted the area and the smaller the number of data subjects, the more limited are the drawbacks of fingerprint databases.

Investigations

Over **25 investigations on the spot** were conducted in 2007 to assess the implementation of biometric recognition devices from the standpoint of compliance with the French Data Protection Act (Loi informatique et libertés). Several lessons may be learned from the investigation findings.

First of all, it appears that fingerprint recognition systems rely too frequently on a centralised biometric database even in the absence of any compelling necessity for security that would justify such a choice. This may derive from a lack of knowledge about CNIL recommendations by the data controller, or from improper parameterising of the software, leading to this situation unbeknownst to the users.

Secondly, the investigations have established that information to data subjects was obviously insufficient, primarily as regards the purposes of the process and individual rights of access and opposition.

Lastly, it was found that biometric recognition systems are installed without the necessary security measures being implemented: access control software and biometric databases are not sufficiently protected.

Whenever serious cases of non-compliance were recorded during the investigations, e.g. absence of authorisation from the Commission, the matter was referred to CNIL restricted committee who has competence to order sanctions, in order to ensure that the organisation investigated would remedy its processing accordingly.

In addition, discussions are currently under way between the Commission and companies selling biometric devices, in an attempt to secure from them commitments to inform their customers on the need to apply for the Commission's authorisation prior to any installation of biometric processes, to raise the awareness of their sales staff to the requirements of the Data Protection Act, and to remove from their advertising material any misleading statement that would deceptively let anyone presume that CNIL may have granted any kind of seal of approval to their biometric systems (for the time being, the Commission has not yet used its labelling powers).

THE SWIFT CASE: TOWARDS AN END TO THE CRISIS

SWIFT (*Society for Worldwide Interbank Financial Telecommunication*)

What is it?

Swift is a Belgian-law cooperative company founded in 1973, providing a series of services to banks, including a secured electronic messaging system. A large proportion of international bank transfers are processed by Swift, whose services have become a must for the banking community.

In June 2006, the US press disclosed the existence of a surveillance project on international banking transactions set up by the CIA shortly after the 9/11 terrorist attacks. Media sources revealed that the CIA and the US Treasury Department had had access for several years to millions of data processed via SWIFT, the main international e-messaging network used in the banking sector (see Annual Report 2006).

This access, established in the name of combating terrorist financing, enables the surveillance of financial transfers to the United States but also of any other types of transactions handled by SWIFT, including within the European Union. The data disclosed include the transaction amount, the currency, value date, name of payee, name of the payer requesting the transaction and client's banking institution. Officially, the purpose of this programme is to identify individuals presumed to be linked with the financing of terrorism. However, fear that the data may be used for other purposes, less security-minded and more economically oriented, cannot be neglected.

The Article 29 Working Party coordinating the European data protection authorities at EU level (known as G29) concluded, in its opinion issued in November 2006, that SWIFT had failed to comply with European regulations on data protection, in particular by assisting the US authorities in implementing the banking and financial data surveillance programme. The G29 Working Party further considered that financial institutions bear part of the responsibility in this matter.

One year later, we now see this crisis coming to an end. The G29 issued a press release on 11 October 2007 expressing its satisfaction for the substantial progress made by SWIFT to comply with principles of data protection.

Completion of EU-US negotiations

In the spring 2007, the European Commission and Council negotiated a number of guarantees with the US government, in order to define rules on the use by US authorities of the data stored in the SWIFT database in the US. These guarantees include limitations of such use for counter-terrorism purposes, compliance with the principle of necessity, maximum retention time of 5 years, and the appointment of an "eminent European personality" with powers to verify the proper operation of the surveillance programme (Mr. Jean-Louis Bruguière).

This political agreement was covered in a series of letters published by the European Commission.

SWIFT reengineering its system

The SWIFT architecture currently relies on the principle of a systematic copy ("mirroring") of all messages stored in two operating centres, one located in the Netherlands, the other in the US, regardless of the origin or destination of messages, which are currently retained for 148 days in the US operating site.

By late 2009, this architecture will be fully reengineered with the installation of a new operating centre in Switzerland. Messages issued by clients of European banks will be systematically duplicated in both European sites (Switzerland and Netherlands), but will no longer transit through the US server. Surveillance by US authorities will therefore no longer be possible on messages related to intra-EU transfers. Messages from or to the United States will be systematically stored at the US operating site.

[Questions to Georges de La Loyère](#)

Member of the Economic & Social Council

Commissioner in charge of European & International Affairs sector

What makes you believe that the Swift case is now behind us?

A lot of progress remains to be made by SWIFT under its reengineering programme to reach compliance with the demands of the G29 opinion of November 2006. One year later, the following results deserve mentioning:

- completion of procedures for compliance of the US subsidiary of SWIFT with Safe Harbour privacy principles,
- revision of SWIFT contractual documents,
- definition of a new data protection charter called "Privacy Policies",
- substantial reengineering of the network architecture, based on a "regionalisation" principle. It is undeniable that the reengineering of the SWIFT network architecture enables us to speak of an end to this crisis.

What conclusions are you drawing from this case?

The existence of such surveillance programmes should prompt CNIL, along with its European counterparts as well as European governments and EU institutions to stay extremely vigilant on issues of any technically motivated centralisation of massive and sometimes sensitive data on the territory of foreign states, and in particular in the United States.

Know your rights!

Back in the spring of 2007, the European Commission issued a firm reminder to G29 member authorities about the importance of ensuring that banks duly inform their SWIFT user clients about the existence of potential data transfers to the US authorities for counter-terrorism purposes. Since it was felt unrealistic to draft standard information notices applicable across the entire EU, the European DPAs opted to work jointly on the subject with their respective national banking federations. Thus, CNIL cooperated on the issue with the FBF (French Banking Federation) and several banking networks in France. Consequently, you should now always be informed by your banker about such data transfers.

VIDEOSURVEILLANCE UNDER CNIL'S WATCHFUL EYE

Growing number of declarations and complaints referred to CNIL

The Commission has recorded a steadily growing number of notification procedures on video-surveillance filed over the past five years, with sharp increases in 2004 (4 times more than in 2003) and 2006 (3 times more than in 2005, i.e. 20 times more cases filed than in 2003). And this increase has continued in 2007.

Thus in 2007, CNIL registered **1317 notifications for video-surveillance systems, for a total of 2980 notifications over the 2002-2007 period. In most cases, each notification is filed for several CCTV cameras.**

The number of complaints filed about video-surveillance also increased from 114 in 2006 to 121 in 2007.

Typology of video-surveillance related complaints in 2007:

- 70 complaints concerning the Labour sector,
- 20 complaints in the Housing sector (problems of joint property ownership or neighbourhood relations),
- 13 complaints related to local authorities and municipal police forces,
- 3 complaints related to the National Education sector,
- the remaining 15 complaints addressed various other sectors.

In 2007, the investigation department inspected video-surveillance devices on site in 8 organisations.

Necessary clarification of video-surveillance regulations

During the 22 November 2007 hearing of Mrs. Michèle Alliot-Marie, Minister of Home Affairs, Overseas Territories & Local Authorities, CNIL reminded the Minister that increasing numbers of CCTV cases were referred to CNIL for review. Accordingly, it would appear necessary to clarify the applicable statutory texts and most of all to harmonise, if not unify, the various systems of formalities (between CNIL and the local authorities' video-surveillance commissions). The Law of 21 January 1995 was adopted in an era where video-surveillance was done primarily with analog recordings on magnetic tape, and it should therefore be reviewed today to take into account the CCTV technology changes.

In addition, the co-existence of two different legal systems for CCTVs installed in public or in private facilities, causes confusion and misunderstandings. It would prove beneficial to consider endowing CNIL with sole oversight powers on video-surveillance systems installed both in public and private facilities, in the context of a revision of existing statutes relative to the subject. The Commission would however require a substantial increase of its resources in order to fulfil such duties.

Questions to Jean-Marie Cotteret

University Professor Emeritus

Commissioner in charge of Home Affairs and Defense sector

What is your outlook on the growth of video-surveillance in our society?

The issue of video-surveillance is emblematic of the much broader issues confronting data protection authorities. The expansion of video-surveillance devices responds to growing demands for collective security expressed by our fellow citizens - don't we also speak of "video-protection"? (a term used by

Minister Michèle Alliot-Marie at her November 2007 hearing) - and may also be explained by a boom in available technologies. Yet, it should not lead to any generalised surveillance, which may in turn deprive citizens of their liberties.

Recent government announcements on the subject have further intensified the necessity for investigating the resources allocated to institutions responsible for controlling these devices (planned installation of nearly 90,000 CCTV cameras in public areas, planned interconnection between the video-surveillance networks of RATP and SNCF, installation of cameras in places of worship, enterprises and department stores).

From a technology standpoint, IP video-surveillance, enabling the transmission and remote viewing of images via internet or a mobile device, has become increasingly common. Likewise, intelligent image analysis software (used to detect "suspicious behaviours" or abandoned objects, count passer-bys, monitor individuals in a crowd, etc.) have become a reality.

What role can CNIL actually play in this context?

While our society can perhaps hope to gain a higher level of collective security, we must however ensure the legitimacy of these developments and also guarantee the protection of our liberties. Several prerequisites must prevail to this purpose. Firstly, the goal pursued must be clearly defined, along with the means and resources planned to reach it. We also need to ensure that our Commission is endowed with the necessary means of investigation in order to protect individual rights. Lastly, we must make sure that an evaluation system is implemented in order to objectively assess the process after a certain development time. Only if these prerequisites are fulfilled, will our fellow citizens accept measures designed to enhance collective security and be reassured about respect for their fundamental right to personal data protection.

Facial recognition

What is it?

Based on a bank of pre-recorded pictures connected to a video-surveillance device and to an automatic facial recognition system, it is now technically possible to identify an individual within a crowd. While this technology still remains embryonic, it is essential to understand its increasingly intrusive nature, since our freedom to move around anonymously could be seriously challenged.

RFID (Radio Frequency Identification)

What is it?

RFID devices enable the presence detection and identification of objects or persons. They consist of a microchip (also called tag) and an antenna communicating via radio waves with an electronic reader over distances ranging from a few centimetres to several dozen metres. For applications in the retail industry, their cost is approximately 5 eurocents per unit.

Other types of communicating chips, smarter or smaller, have been emerging with the advent of the globalised "object-oriented internet". Some prototypes are virtually invisible (0.15 mm square and 7.5 micron thick), while others have a storage capacity of 512 KB (kilobytes) for a size of 2 mm² and can exchange data at a rate of 10Mbps (megabits per second).

NFC (Near-Field Communication) technology, a communication standard developed in 2002, enables communication and inter-operation between various types of RFID chips. The transmission distance is 10 cm at a maximum throughput rate of 424 Kbps.

How are these chips being used?

Contactless chips have been invading our daily life little by little. They rely on various technologies, such as RFID (Radio Frequency Identification) or NFC (Near Field Communications).

They can already be found in urban transit passes (e.g. Navigo subway pass or Velib bicycle rental cards), in electronic passports, building access badges (e.g. Vigik), electronic purses, car keys, in logistics applications for luggage handling systems at airports or inventory control in retail stores.

The radio-identification technology (RFID) has concurrently become a major economic stake, particularly for applications in the retail and transportation industries.

Yet, the future promises to add ever more diversified applications. Chips will most likely be used to instantly detect the contents of our supermarket shopping cart. They will have the ability to analyse the items we purchase; luxury goods will be tagged to prevent counterfeiting; payments will be contactless once NFC readers are imbedded into our mobile phones; medicines and blood pouches will also be tagged to enhance their traceability.

Experiments are currently under way to fit newborn infants in maternity wards with RFID bracelets to prevent kidnapping. What about chips implanted under the skin? It's already being done in Spain, where RFID tags are injected under the skin as a means of payment in some nightclubs, a purpose totally disproportionate with real needs!

What are the challenges for data protection and privacy?

These technologies raise new challenges for personal data protection and privacy, first and foremost the issue of their invisibility or quasi-invisibility. How can compliance with the law be guaranteed in the presence of invisible technologies?

Furthermore, anyone equipped with the appropriate reader can access the contents of the RFID tag. And a chip can contain personal data (or data that can become personal via interconnections with a database) that enable a remote identification of its bearer. **If all the objects of our daily life** (transport cards, clothes, telephone, car, bracelet, etc.) are tagged in this manner, **it will then become possible to track individuals in every single act of their daily life...**

It is true that today RFID devices still do not allow for continuous monitoring of individuals. For instance, the use of a Navigo pass only provides information on which subway station the passenger entered and possibly exited the Paris subway. It is still not possible to find out the passenger's detailed ride, particularly since CNIL has restricted the data retention time to 2 days, and only for fraud detection purposes.

But what about tomorrow? Theoretically, a more precise surveillance of individuals would be possible, though this would require considerable resources, with a dense mesh of readers capable of receiving the data contained in the tags from a distance of several metres away.

Reconciling RFID and privacy

In urban transports, it is essential to ensure that systems enabling passengers to travel anonymously continue to exist.

In the retail industry, tags fitted onto the products sold in supermarkets should have a way to be automatically neutralised at the cash register (by deactivation or physical removal). Technical devices ensuring RFID tag neutralising should therefore be imbedded at the manufacturing stage, whenever the chip has no intended application beyond the point of sale. Solutions already exist, but research needs to progress further in order to find practical ways to implement them. In this perspective, CNIL has been cooperating with the Retail Industry Cluster of the Nord region in France, in an effort to guide the development of RFID technologies.

Furthermore, it is essential to provide consumers with clear and detailed information on the use of such tag, on the related data processing involved and on the possibility for them to read the chip contents and check whether or not it is active.

Lastly, security standards must be promoted to guarantee that any personal data possibly contained in the tags cannot be read remotely by unauthorised third parties without the person's knowledge.

In view of their massive dissemination, of the individual nature of identifiers for each tagged object, of their invisible character and of the risks of individual profiling, **CNIL has been monitoring the development of these new technologies with extreme vigilance**. The Commission has regular contacts with the industry players, both on a national and a European scale, and is currently involved in the drafting of an EU recommendation on the subject that should be adopted in the first half of 2008. The recommendation is intended as a reminder that such technological developments should necessarily be matched by compliance with key principles of data protection, i.e. principles of legitimacy of purpose, proportionality, transparency and security.

Should the use of such technologies be more precisely framed and regulated by law? Whenever RFID devices enable any direct or indirect identification of a physical person, then they fall under the remit of the French Data Protection Act. From this standpoint, it does not appear necessary to adopt any other specific legislation, but it might prove necessary to adapt the French Data Protection Act in order to account specifically for this particular technology. The working party created within CNIL to this purpose, will be in charge of reviewing the enforceability of the data protection act, of recommending a revision of the law as felt appropriate, and assessing whether an addendum on this topic might be necessary (see Chapter 4).

Chapter 3 CHALLENGES

TRACKING WEB SURFERS

Surveillance of peer-to-peer networks

In October 2005, CNIL had rejected applications for the installation of 4 *peer-to-peer* surveillance systems filed by royalties collection and copyrights distribution institutions in the music industry (SACEM, SDRM, SPPF and SCPP). The organisations later appealed the Commission's decisions to the Conseil d'Etat who overturned them partially on 23 May 2007. The Conseil d'Etat ruled that CNIL had made an "error of judgement" by finding that the data processing intended to search for and detect illicit access to musical works on peer-to-peer networks was disproportionate with its purpose. Conversely, the Conseil d'Etat endorsed CNIL's analysis regarding the principle of mailing educational messages to targeted internet users. Thus the Conseil d'Etat ruled that such mailings were unlawful as they were not covered under the terms of the authorisation granted to internet service providers to retain login data on internet users.

Further to this ruling, the Commission contacted the royalties collection organisations to find out about their intentions. Three of them (SACEM, SDRM and SCPP) re-applied for approval, removing the invalidated educational messaging clause from their requests. Thus in November 2007, in pursuance of the ruling of the Conseil d'Etat, CNIL had to authorise these three organisations to implement their search and detect process for copyrights violations on internet. The last organisation concerned (SPPF) re-applied for approval in December 2007 and their own surveillance system, identical to the previous three, should be authorised in early 2008.

In July 2007, the French Minister of Culture and Communication created an adhoc committee to investigate solutions intended to "*fight against illicit downloads and develop lawful music offerings*", under the leadership of Mr. Denis OLIVENNES and with the participation of Mrs. Isabelle Falque-Pierrotin, CNIL member and President of the "Guidance Council" and representing the "Forum des droits sur l'Internet" (Internet Rights Forum). The committee issued several recommendations in November 2007, which, once taken on board by the Government, should lead to legal and technical adjustments, to be subsequently reviewed by CNIL.

Cross perspectives

Isabelle Falque-Pierrotin

Conseiller d'Etat

CNIL Commissioner in charge of Public Liberties sector

Emmanuel de Givry

Conseiller à la Cour de Cassation

CNIL Commissioner in charge of Risks & Rights Management sector

How did CNIL participate in the proceedings of the Olivennes committee?

E. de Givry: I testified before a hearing in October 2007, similarly to other public officials. Our goal was to enable the committee members to mainstream as best as possible issues of data protection into their investigations and recommendations. The hearing was an ideal opportunity to respond to many technical and legal questions related to privacy protection on the internet.

I. Falque-Pierrotin: As a member of both CNIL and the Olivennes committee, I was able to share my expertise with the committee on issues of personal data protection. The committee members were not necessarily aware of the assets offered by the French and European data protection systems, their constraints or the guarantees they provide. This particular dimension of combating illicit music downloads needed to be clearly incorporated into the committee's enquiry, particularly since it is a major concern for internet users.

How did CNIL respond to the recommendations issued by the Olivennes committee?

I. Falque-Pierrotin: In view of the proposals contained in the committee's report, the Government and later the Parliament will have to discuss these issues and make choices. They will need to decide on the necessary reconciliation between the defence of copyrights and the defence of individual liberties. Those will be difficult choices that will impact more broadly the vision of our country regarding internet regulation. CNIL will of course play its rightful role in this decision-making process.

E. de Givry: The Commission has duly noted that the report issued by the Olivennes committee includes repeated reminders that any systems considered will have to be submitted to CNIL for approval, and that the fight against music pirating must rely on "*proportionate and pragmatic solutions, respectful of individual liberties*", which is precisely what CNIL has always advocated.

CNIL's investigations

CNIL has conducted several on-site investigations of internet service providers who practice peer-to-peer network surveillance. Investigations on the elements collected during these investigations should be completed in the first quarter of 2008.

IP address regarded as personal data by all European data protection authorities

In two successive rulings issued in April and May 2007, the Court of Appeal of Paris judged that IP addresses collected during searches and findings of internet counterfeiting acts do not enable, even indirectly, any identification of physical persons, and that consequently they do not constitute personal data. Concerned about the consequences of such an analysis of Internet privacy protection, CNIL contacted the Minister of Justice and the Public Prosecutor to the Cour de Cassation (Supreme Court) in an attempt to lodge an appeal against both rulings in the interest of the law. In a letter dated 8 October 2007, the Minister of Justice agreed to lodge the appeal to the Cour de Cassation who should issue its ruling sometime in 2008. It should be noted that, in an opinion published on 20 June 2007, the data protection authorities of EU Member States issued a reminder that IP addresses were indeed to be regarded as personal data.

Cybersquatting and Typosquatting: AFNIC watching!

The non-profit "Association Française pour le Nommage Internet en Coopération" (AFNIC) is the institution in charge of administrative and technical management of the domain names ending with ".fr" (France) and ".re" (Reunion Island).

Practices involving so-called *cybersquatting* (abusive use of domain names owned by known brands or renowned companies) and *typosquatting* (registration of a domain name similar to a known domain, e.g. "legifrance.fr" instead of "legifrance.gouv.fr") have been multiplying. In an effort to curb these practices, AFNIC has set up a system providing for automatic updates of a watch-list of physical persons resorting to such methods in violation of its Naming Charter, whose normative character has been confirmed by courts of law. The Charter specifies the rules relative to the registration and maintenance of domain names administered by AFNIC.

Individuals recorded on this watch-list are no longer authorised to register any new ".fr" domain names for one year, the one-year period corresponding to the normal lifespan of a domain name. In the event of repeated violations during a period of 7 years, the ban will be extended to 3 years. In case of attempted ID misappropriation of registered .fr domain names in violation of the exclusion decision, the ban period will be extended to 5 years.

In its decision issued on 13 September 2007, CNIL authorised AFNIC to set up this watch-list, after having duly noted the guarantees provided, in particular as regards the information of the internet users concerned about the implementation of this procedure.

Search engines and community sites

What personal traces are stored by a search engine?

Every time you carry out a search on internet, search engines generally collect numerous data about you: personal cookie, IP address of the computer and contents of the query. These data are frequently retained over long periods of time, i.e. over one year for all major industry players. These personal data can then be deleted or anonymised.

This means that a search engine knows exactly what searches you have submitted for at least the past year, including all ads that you may have accessed to...

Internet has become a part of our daily lives: whether to find the dream holiday destination, the best tiramisu recipe or the reviews on the latest Georges Clooney film, search engines are inescapable! Searching for childhood friends, networking or simply publicising ourselves on the web... so many reasons among others that explain the current success of community sites. Yet, these "free" sites actually exploit web surfers' personal data for commercial or advertising purposes without any clear information provided about it to the surfers.

Questions to Philippe Lemoine

Chairman & CEO of Laser

CNIL Commissioner in charge of Technology sector

Why did CNIL take an interest in search engines and community sites?

Whether we're talking about search engines like Google or Yahoo! or about community sites like Facebook, MySpace or LinkedIn, all these web-based services operate with the same business model:

they offer free services in counterpart for financing revenue from advertisers, who in turn exploit these sources of personal data supplied by the users themselves, sometimes unbeknownst to them, in order to increasingly fine-tune their marketing targets.

Accordingly, it was perfectly natural for CNIL, similarly to other data protection authorities, to be concerned about actual compliance of such sites and services with the principles of data protection, and to scrutinise the conditions under which personal data are processed and internet users are informed about the processing and about ways to exercise their privacy rights.

But these services often prove very useful. What risks do they present for citizens?

When personal data on life style, personal relationships, leisure activities or even political and religious opinions are disclosed to search engines or site networks, internet users make their private life visible for all to see on the web, enabling web sites to compile huge data mines liable to be tapped for multiple commercial uses. We are insufficiently aware of this reality, though at times we may witness outright rejections of tactless invasions of advertisements. But our awareness of the challenges facing our public and private liberties is very inadequate, particularly among the younger generations.

The risk is very real indeed and further amplified by the fact that internet users are not always familiar enough with these new tools. For instance, even if parameter settings can be personalised on the web service, the default configuration frequently facilitates a broad dissemination of the data, in such a way that data supposed to remain within your sphere of privacy often end up displayed publicly on the web.

What measures are currently under way or planned by CNIL on this topic?

CNIL has contacted all major industry players and urged them to take into better consideration the data privacy issues, whether for the protection of sensitive data, information of private users and their rights to refuse any commercial exploitation of their personal data, or on data retention time. However, we cannot afford to restrict our action on a purely national scale. Consequently, the Article 29 Working Party (group of European data protection authorities) will be publishing an opinion on search engines in early 2008. This opinion will reassert the rules of data protection applicable to search engines and formulate a number of practical recommendations. The G29 further intends to adopt an equivalent approach for community sites.

Concurrently, internet users also need to enhance their basic knowledge on personal data protection. Information and awareness measures are therefore needed and will be conducted by CNIL, particularly for younger users.

KNOW YOURS RIGHTS!

How to request the deletion of a web page containing personal data

When internet users request a web site publisher to remove their personal data from publication lists, the publisher will dereference the relevant page, but the data may remain available on the web for some time, resulting sometimes in reactions and complaints filed with CNIL from users who believe their request was not taken into account.

So what really happens? Search engines retain a temporary copy of all pages visited by their indexing engines. Questioned by CNIL on the subject, Google explained that when a web page is removed by the site publisher, this copy called a "cache page" is also deleted from search results but only after the

next site indexing process is completed by the search engine robot. The re-indexing time lag varies depending on various factors, such as site popularity or update frequency, but takes place on average every 2 to 3 weeks (some news sites may be updated virtually every day). During this time interval, it may still be possible to view the cache version of the deleted page even though the actual page is no longer published on the original site.

WORKERS BEING GLOBALISED IN SPITE OF THEMSELVES!

Under its 2007 annual investigation programme, the Commission decided to conduct investigations to check the conditions of data file processing linked to human resources management.

Nearly **fifty investigations** were thus carried out in order to verify HR-related personal data systems: personnel records, recruitment files, as well as biometric and geo-positioning devices, whistle-blowing systems, etc.

The investigations revealed the following findings.

Assessment of whistle-blowing systems

Whistle-blowing systems, mandatory for listed companies in the United States under the Sarbanes-Oxley Act, enable company employees to report any behaviour violating legal requirements or company rules, without having to go through the traditional management lines.

The very first finding is that French workers do not make much use of such systems. These mechanisms, set up by parent companies headquartered abroad, seem unsuitable to the usual practices found within French companies. It would appear that such systems present little usefulness in the existing context of the legal requirements provided under the French Code of Labour or versus the traditional ways of resorting to the normal management line to report any malfunctions.

The second observation resulting from our investigations is an inadequate understanding of the requirements arising from the French Data Protection Act when implementing whistle-blowing systems. This is the case for a number of companies who have signed a compliance commitment under the "Single Authorisation No.4", even though very few of the systems in place are actually restricted to the fields of *"finance, accounting, banking and anti-corruption"*, as specified by Article 1 of the French law. In reality, the companies' whistle-blowing system is most often backed by their own code of conduct, generally drafted by the parent company and covering a much broader scope than that allowed by CNIL single authorisation.

Substantial growth of transborder data flows

In 2007, CNIL authorised 1682 transfers of transborder data flows and 538 other applications are pending investigation.

Two different cases may be observed in the Human Resources sector.

Firstly, data flows may be transferred at the request of the parent company located for instance in the US for purposes of streamlining their corporate HR management tools: in which case, all subsidiaries use the same software and the data are hosted on the servers at the parent company.

In such context, a complete lack of compliance with the legal obligations of the French Data Protection Act has been found in a number of cases: absence of information to the personnel, ignorance about the allowable post-transfer data retention time, lack of CNIL authorisation which constitutes an offense punishable by 5 years in jail and a €300,000 fine in pursuance of Article 226-16 of the Criminal Code.

In the second case, data are transferred abroad under subcontracting agreements: a company decides to outsource its payroll management or recruitment process to an independent service provider located abroad or hosting its databases in a foreign country. Frequently, the company data controller do not even know where the data are actually located, though they have the responsibility for it.

Such situation ignore the obligations of the law providing for **information of individuals whose data may be transferred to non-EU Countries**, as well as the provisions requiring that the data controllers responsible for data processing should have “full control” over the security of the data for which they are responsible. Such control implies knowledge of the physical location of the databases and assurance that any data transfer will be done in such a way as to guarantee their confidentiality.

Geo-location systems applied to employee vehicles

These systems enable an employer to track at all times the geographic location of employees driving a vehicle equipped with a GPS device.

Legitimate purposes justifying the implementation of geo-positioning tools are sometimes badly understood by companies who tend to neglect to define precisely the expected goals for resorting to such devices. Consequently, companies run the risk of not being able to justify the legitimacy of purpose, particularly with respect to the relevant CNIL recommendation adopted on 16 March 2006.

Some ten investigations conducted on the subjects have largely revealed a **lack of information to the employees about their rights** (right to access, rectification and opposition) along with the absence of any definition on the retention period for the data collected by employers.

Questions to ...

Hubert BOUCHET

Member of the Social & Economic Council
CNIL Commissioner in charge of Labour sector

Why did you decide to take a closer look at whistle-blowing systems?

CNIL began focusing on the subject as soon as the first plans emerged to put into application in France this provision of the Sarbanes-Oxley Act. The Commission investigated the subject in depth in cooperation with a number of North-American authorities, in the perspective of defining a framework to implement such systems while complying with French requirements on personal data protection. CNIL ultimately adopted a "Guidance Document" published on 10 November 2005 along with a "Single Authorisation" on 8 December that same year (Single Authorisation No.4). It was therefore felt necessary, as a second step in this process, to assess how the companies had implemented these systems which generally exclude labour-related aspects from their scope.

What are the main lessons derived from these investigations?

These whistle-blowing mechanisms obviously appear as “imported” instruments, failing to match the social and labour realities of French companies. They correspond neither to the reality of the practices of French companies, nor to the mentality of French workers. To be exhaustive, I should even add that CNIL has noted the reluctance of many corporate officers responsible for implementing the systems. From the standpoint of “data privacy and liberties”, such mechanisms are highly delicate to set up, particularly as regards issues of scope of application and information of employees.

What were the other findings in terms of human resources management?

The use of information technologies for purposes of HR Management, in the broad sense of the term, is now widespread and undeniable: biometrics, computerised career and recruitment management, video-surveillance, automated access and presence control, etc. All involve data processing are subject to the requirements of the French Data Protection Act. Nevertheless, all legal obligations are not always properly understood by HR managers, particularly in terms of filing declarations, data retention time or personnel information. This was noted in particular for data flows transferred to non-EU Third Countries, which are covered by specific regulations often neglected by French companies who consequently incur serious legal risks, including criminal penalties.

Chapter 4 - PLANS FOR 2008

IT OUTSOURCING: how to guarantee data protection?

Following the publication of its guidelines in the 2006 Activity Report (p.74), CNIL decided to create a working committee to look at the issue of call centre relocations and IT services outsourcing.

Call centres raise a dual issue: companies may outsource their customer management to a call centre provider, for technical support through hotlines, ordering goods or services or simply to provide information. Call centres may also be set up by companies for their promotion of new products or services. In both cases, data records are compiled and processed, and must therefore comply with regulations on data protection.

Furthermore, these IT resources and services increasingly tend to be outsourced outside the European Union, in particular to countries where specific legislation on personal data protection frequently does not exist. According to the professional union Syntec Informatique, the proportion of IT services relocated offshore by French companies will grow from 1.6% to 5% by 2009, i.e. an increase much higher than the growth rate of these services themselves.

The significant impact of IT and call centre outsourcing on employment, whether in France or in the provider countries, means that economic and labour-related aspects are top-ranking issues among the questions raised by offshoring practices.

Yet, regardless of the type of process involved, from a simple hotline to the transfer of medical data, compliance with the obligations of the French data protection law is mandatory for any outsourcing operations.

In addition, this raises the further question of how such data transfers towards these countries can take place while guaranteeing full respect for the legal rights of the individuals concerned.

The Commission's goal when creating this working committee chaired by Didier Gasse, was to assess the current status of practices, to identify the risks involved based on the type of situation, and to review the legal formalities applicable to data flow processing.

The task of the working group is to propose solutions encouraging companies to improve their compliance with data protection regulations when drafting their code of ethics or internal corporate policies, and to look at ways of simplifying prior formalities.

The working group started its work in the first quarter of 2007. Initial hearings were held with representatives from the French Association of Customer Relations Centres (AFRC) and the Professional Union of Customer Centres (SP2C). Morocco was identified as the preferred French-speaking country for call centre offshoring.

The above actions fit in line with the CHIL' current policy of consultation with its European DPA counterparts, aimed at demonstrating to Third Countries the benefits of adopting a specific legislation on data protection. The idea is to secure the legal framework applicable to French companies outsourcing outside the EU, while fostering economic development in high-growth sectors in the host countries.

DISCOVERY CASE: ANOTHER SENSITIVE ISSUE WITH THE USA

What is it?

“Discovery” or “pre-trial discovery” designates the US procedure that allows one party in a litigation case to file a motion requiring the other party to turn over all information items at its disposal (facts, actions, documents, etc.) that may be material to the resolution of the dispute in the context of evidence search, even though such information might be unfavourable to the party concerned.

CNIL has found that a growing number of motions are being filed, requiring the disclosure of personal data held, among other, by French subsidiaries of US corporations subject to pre-trial discovery procedures in US litigation cases. It has become frequent to see companies or their foreign subsidiaries forced to turn over copies of the full contents of the hard disks or e-mail boxes of some employees, or even the entire personnel.

Furthermore, though in a different legal context, a number of US authorities, such as the *Securities and Exchange Commission* (SEC) or *Federal Trade Commission* (FTC), may also issue information injunctions demanding that foreign companies produce documents or evidence, by virtue of their respective powers of investigations.

Information injunctions may concern French companies who are subsidiaries of US corporations listed on the US market, or French-law companies operating in the US.

Numerous challenges to the French data protection act

Such disclosure requirements breach the French legal provisions on data protection, and more specifically those applicable to the information and consent of individuals, to the proportionality of the data processing involved and to the conditions of data transfers outside the EU.

In addition, these situations give rise to difficulties falling within remits other than just the Data Protection Act, related among other to international judicial cooperation, protection of domestic economic interests, industrial and commercial secrecy, or even to national sovereignty.

Existing procedures to protect the interests of French companies

In pursuance of the 1970 Hague Convention, any information injunction issued by US judiciary or administrative authorities, must be subject to a request for international judicial cooperation filed with the relevant department at the Ministry of Justice. After investigation, the request may be either rejected or transferred to the jurisdiction having geographic competence over its enforcement.

The French Law of 26 July 1968 on the disclosure of documents and information of an economic nature prohibits, unless otherwise provided under international covenants, any person from requesting or disclosing any documents or information of an economic, commercial, industrial, financial or technical nature likely to be used to compile evidence intended for use in legal or administrative proceedings or arising from them. Hence, such requests from foreign administrative authorities may be legally allowed only if covered under an international agreement or treaty.

Thus a Mutual Assistance Agreement was signed between the French "Commission des Opérations de Bourse (COB), now called "Autorité des Marchés Financiers" (AMF), and the US Securities Exchange Commission (SEC). French companies requested by the SEC to disclose information must file a prior information request to the AMF in order to protect themselves from any subsequent risk of criminal prosecution.

Questions to...

Bernard Peyrat

Judge at the Cour de Cassation,
CNIL Commissioner in charge of Commerce sector

Why did CNIL create a working committee on this subject? And how does it operate?

CNIL was contacted by French companies and law firms requesting its advice on a binding legal framework relative to the disclosure of information to foreign judiciary or administrative authorities. Such requests made by foreign administrations as well as by parent companies to their subsidiaries or even to their trade partners, raise multiple legal issues, linked to business secrecy, patent protection, international judicial cooperation, business intelligence and to many other realms that do not necessarily lie under CNIL's scope of competence.

Conversely, CNIL has a direct vested interest in the conditions under which personal data are transferred. What about information and consent of employees, clients or prospects, and lawyers involved? What of the conditions of data transfers outside the EU? And first and foremost, what about the proportionality of the data processing?

This is an extremely delicate issue since it is often difficult for a subsidiary to reject or even simply object to a request from its parent company or from an administrative authority, particularly in the United States where legislation and case law grant considerable powers to public administrations or to the judges in charge of assessing the legitimacy of pre-trial discovery motions filed by a litigant.

Together with my colleagues Georges de la Loyère and Philippe Nogrix and with CNIL departments, we decided to conduct hearings of all stakeholders: public authorities, lawyers, enterprises, etc. These broad exchanges of views will fuel our investigations in the perspective of arriving at recommendations in an area which, it should be emphasized without any exaggeration, involves substantial challenges linked to both an “economic war” and a “war between legal cultures”, opposing the Roman-Germanic and the Anglo-Saxon sides.

What are your goals?

We have a dual goal. Firstly it is necessary to issue a reminder on the obligation to comply with the legal framework as provided by our data protection law or by international conventions, a mandatory requirement for injunctions issued by foreign authorities to be legally allowed and binding, an obligation of which many companies are not aware. In addition, we must contribute to the issue on an EU level in order to adopt a common policy. This is why our own national investigations at CNIL will fit into a European-scale continuum, fuelling the work initiated by the European DPAs within the G29 Working Party. Backed by the respective analyses of national laws in EU Member States, the G29 will work in consultation with the European Commission and other EU institutions to initiate negotiations with the US, among others, on the subject.

Annex –

CNIL - 2007 Key Figures**CNIL Decisions: 393**

In 2007, CNIL held 40 formal meetings: 25 plenary sessions, 12 Select Committee meetings and 3 Bureau meetings, leading to the adoption of **393 Decisions** (+30% versus 2006).

Consulting and expert appraisal

6 opinions on proposed bills or decrees

Sanctions

9 financial sanctions with fines ranging from €5,000 to €50,000

5 warnings

101 formal notices to comply

Simplification

4 Unique Authorisations

2 opinions on a single regulatory document

Declaration formalities

214 authorisations approved

26 authorisations rejected

22 opinions on sensitive or high-risk data processing

Auditing

164 investigations

140 organisations audited

Referral of complaints

7,115 cases referred, i.e. 4,455 complaints (+25% versus 2006) and 2,660 requests for access to Police and Gendarmerie records (+67% versus 2006).

The largest numbers of complaints were filed in the following sectors, in descending order: *banking-credit, commercial prospection, labour, telecommunications*.

The most frequent reason for complaints was to oppose an inclusion in a data process.

Data Protection Correspondents:

In 2007, over 1050 organisations informed CNIL of their decision to appoint a Data Protection Correspondent ("CIL"), versus 650 in 2006 and 73 in 2005, i.e. a total of 1723 organisations.

Declarations of data files with CNIL: 56 404

Over the period of January 1 to December 31, CNIL recorded 56,404 new personal data files processed. Since 1978, a total of 1,216,404 data files have been declared to CNIL.

Memento

Zoom on figures

In 2007, CNIL:

- recorded 56,404 new personal data files processed;
- numbered 685 Data Protection Correspondents;
- received 4,455 complaints;
- adopted 393 decisions;
- conducted 164 investigations;
- sent 101 notices to comply;
- issued 5 warnings;
- ordered 9 financial sanctions;
- referred 5 reports to the Courts.