COMMISSION NATIONALE DE L’INFORMATIQUE ET DES LIBERTÉS
COMMISSION NATIONALE DE L’INFORMATIQUE ET DES LIBERTÉS

ACTIVITY REPORT 2011

As provided by Article 11 of the Law of 6 January 1978, amended by the Law of 6 August 2004

In pursuance with the Law of 11 March 1957 (Article 41) and the Code of Intellectual Property of 1 July 1992, any reproduction, whether wholly or partially, of this publication for collective usage is strictly prohibited without the express authorization of the publisher. As a reminder, the abusive and collective use of photocopies jeopardizes the economic balance of the book publishing industry.

ISBN 78-2-11-008039-4
### Decisions and Deliberations

1,969 decisions & deliberations adopted
(+ 25.5% versus 2010)

249 authorizations, including 6 single authorizations

93 opinions issued, including 1 opinion on a single regulation

1 recommendation on political communication

2 waivers of notification

11 rejected authorizations

93 opinions issued, including 1 opinion on a single regulation

1 recommendation on political communication

### 2011 Key Figures

#### Notices to Comply & Sanctions

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>Notices to comply</td>
</tr>
<tr>
<td>5</td>
<td>Financial fines</td>
</tr>
<tr>
<td>13</td>
<td>Warnings</td>
</tr>
<tr>
<td>2</td>
<td>Acquittals</td>
</tr>
</tbody>
</table>

#### Prior Formalities

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,993</td>
<td>Notifications on video-surveillance systems (+37% versus 2010)</td>
</tr>
<tr>
<td>4,483</td>
<td>Notifications on geolocation systems (+33.5% versus 2010)</td>
</tr>
<tr>
<td>744</td>
<td>Authorizations on biometric devices (+5.4% versus 2010)</td>
</tr>
</tbody>
</table>

#### Complaints & Requests for Indirect Right of Access

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,738</td>
<td>Complaints (+19% versus 2010)</td>
</tr>
<tr>
<td>2,099</td>
<td>Requests for indirect access to police and intelligence records (+12% versus 2010)</td>
</tr>
</tbody>
</table>

#### Controls & Audits

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>385</td>
<td>Audits (+25% versus 2010)</td>
</tr>
<tr>
<td>151</td>
<td>Videoprotection audits</td>
</tr>
</tbody>
</table>

#### Correspondents

8,635 organizations have appointed a data protection officer (CIL) (+25% versus 2010)
# TABLE OF CONTENTS

## 1. NEW MISSIONS
- Vidéo-surveillance audits: status assessment and action plan
- CNIL certification labels
- Notification of personal data breaches
- Strategic forward-planning at CNIL: initial work, first publications

## 2. INFORM
- The CNIL informs you daily
- Replies to public enquiries
- Data protection officer

## 3. ADVICE AND PROPOSE
- National Consumer Credit Register

## 4. REGULATE
- Ethical Business Alert (Whistleblowing)

## 5. CONSULT AND INNOVATE
- WiFi, iPhone and geolocation
- Consultation on Cloud Computing

## 6. PROTECT AND INSPECT
- Record number of complaints
- Right of indirect access
- Audits

## 7. SANCTION
- Summary report on the 2011 activity of the Sanction Select Committee

## 8. TOPICS OF INVESTIGATION IN 2012
- Revision of EU Directive: A successful data protection Union

## APPENDICES
- CNIL membership
- CNIL: Means & Resources
Today, the CNIL has reached a decisive step in its development. Confronted to structural mutations linked to the growth of the digital society, the Commission sits at the core of the international debate on data protection in the 21st century; a unique era that invites us to revisit our action.

Structural changes first and foremost, as this is indeed a change of era driven by the digital age. Within just a few years, the digital world has become pervasive: with the increasing dematerialization of industries and services, we have shifted from a rather static, domestic world of physical records to an international, fluctuating universe of virtual data with multiple players involved. Data are pervasive and omnipresent everywhere, produced and consumed by individuals, enterprises and public authorities alike; and tomorrow, these data will increasingly deal with objects. They now represent a considerable merchant worth, at the heart of the economic challenges of the 21st century.

Confronted to this new ecosystem, my priority consists in consolidating the adjustments already initiated, and ensuring that the CNIL enters the digital era on a solid footing. This new environment can no longer be regulated the same way as in the past. We therefore need to rethink our action and revisit our operational tools in order to process these data flows and address increasingly diversified stakeholders.

It is true that our powers of regulation and sanction are indeed mighty, and we shall not hesitate to use them as needed. Nevertheless, these enforcement instruments will not be sufficient to establish a rule of law in this new digital universe. Indeed, we can no longer afford to simply issue general guidelines and verify their application a posteriori. Confronted with the complexity of the digital ecosystem, the regulator’s challenge consists in building relays; relays allowing for the engagement and accountability of all stakeholders, whether public, private or individual, in order to ultimately share the burden of regulation with them.

Isabelle Falque-Pierrotin,
CNIL President
To this purpose, we need to work closer to the field, to the various players and their specific business features. Such a novel approach will require making new tools available to them, to help them implement in practice and as early as possible the principles of the “Informatique & Libertés” Act on Privacy and Data Protection. A tool box already exists, but we need to supplement and refresh it, in cooperation with professionals. Whether Codes of Good Conduct, Charters, Certification Labels or Data Protection Officers or Correspondents (“CIL” or “Correspondants Informatique & Libertés” in France), all such levers must be in the service of corporate compliance with the Privacy & Data Protection Act.

Enforcement and oversight of compliance will lie at the core of the CNIL’s actions over the coming years.

This evolution also corresponds, I believe, to a new phase in the maturity of the stakeholders themselves. Under pressure from consumers and youngsters, data protection is starting to be perceived not just from the simplistic prism of a legal constraint, but rather as a competitive edge, or even a social advantage. Enterprises are of course concerned with limiting the legal risk, but they also wish to arouse trust from their target public, whether internal (employees) or external (customers, web users) and, in the event of problems, to mitigate any image-related damage.

Gradually, the issue of data protection is overstepping the mere scope of legal or IT corporate departments to invest the dimensions of marketing, sales or human resources.

Yet it should also start spreading to the level of top corporate management since tomorrow’s innovations and growth are increasingly linked to data processing issues.

Just think about automobiles, smart meters or home automation... many business sectors will need to take into consideration the issue of personal data management as a tool for customers to take ownership of their products and services, and therefore a means conducive to the sustainable development of their business activities.

Similarly, consumers have matured: even though many still fail to understand how and by whom their personal data are actually used, both consumers and web users, who represent a volatile but hard-to-please population, are demanding more transparency from businesses. They want to know about or even control such uses!

Businesses, and more generally digital-related players are confronted to these new demands; they cannot afford to disappoint them, at the risk of losing their customers’ contact and trust.

The CNIL must also adapt to the new social demand, and offer to the public at large educational guidance on solutions, by providing insights for a responsible and controlled use of personal data. The CNIL needs to fully play its role as a guide to digital life. This is one of the reasons why we decided to conduct a survey on smartphones, our new everyday-life instrument that contains numerous personal data, including sensitive data, yet lacking any specific protection. Based on the study findings, we developed ten recommendations to help better secure smartphones, in the form of a video tutorial. In the same didactic spirit on best practices, the CNIL also innovated with the production of an interactive video clip entitled Share the Party intended to raise the awareness of youngsters about the videos or photos they publish on social networks.

In order to anticipate on new uses, we can increasingly rely on the initiatives and works produced by our Department of Research, Innovation and Foresight. The many discussions initiated by the Department attest to our determination to establish an open dialogue with
highly diversified stakeholders, with exchanges of views that fuel and enrich our thinking, and sometimes even incite us into rethinking our models.

These structural changes occur in a highly turbulent international environment which is not conducive to an easy readjustment process.

Europe, USA and Asia are wrestling to develop legal frameworks of personal data protection that will be as efficient as possible in terms of economic growth. On a European scale, I am thinking of the Draft Regulation reforming the European Directive of 1995 relative to data protection. Last January 25, the EU Commission published its proposed draft, and the CNIL was extensively mobilized on this occasion. We are living a historical moment that must be fully comprehended, as the new regulation will refashion a new European landscape for data protection in the 21st century. The booming digital world and the growing globalization make it necessary to revise the existing European legal framework. The Draft Regulation, as it currently stands, constitutes a substantial progress that was both expected and necessary. Citizens’ rights are thus largely strengthened: recognition of the “right to oblivion”, of a right to the “portability” of personal data, and clarification of rules relative to enlightened consent and exercise of their rights. Concurrently, businesses also benefit from a simplification of administrative formalities, while remaining subject to stricter obligations.

Yet, the Draft Regulation also contains points of concern for us, raising the issue of the very functioning of the proposed scheme. Via the criterion on “Primary establishment” of the data controller or processor, the processing of complaints becomes further removed from the internet user, since complaints may be addressed by a foreign authority; furthermore, cooperation between data protection authorities appears much too restricted and unwieldy, even though it is key to having any clout when negotiating with the major Internet players. In this respect, the audit on Google’s new confidentiality rules launched last February and conducted by the CNIL on behalf of the European G29 data protection authorities is a perfect example illustrating how credibility can be boosted by a proactive collective action.

In this context of fierce international competition, the world is turning to Europe, in search of the continent’s ability to modernize its data protection model, while reasserting privacy as a fundamental right. Because not everything is merely about growth! The idea is to reconcile growth with a humanistic vision of fundamental rights, an approach specific to Europe, yet finding wide echoes in the French-speaking world in particular.

In order to assert its existence and have real clout on the international scene, Europe therefore needs to show audacity, innovation, and should not hesitate in pushing forward its many assets or change its habits, while remaining true to its fundamental principles.

Europe needs to modernize its data protection model, while reasserting privacy as a fundamental right”

The CNIL is thus confronted to a shifting and complex national and international context. I am fully confident in its ability to reinvent its action and to influence European negotiations. Its staff and members are well armed and strongly motivated to face such changes. As President of the CNIL, I feel particularly happy and enthusiastic at the chance to take part in this great adventure and to orchestrate it!
The newly extended scope of competence: key highlight of the year 2011

A newly extended scope of competence for the CNIL: in my view, this is the key highlight of the year 2011. This extended remit originates first of all from a decision by lawmakers who have entrusted our Commission with two new missions.

The first of these two new missions was introduced by Article 18 of Law No. 2011-267 of March 14, 2011, called “LOPPSI 2”, assigning to the CNIL competence to oversee all video-surveillance systems installed on the public highway, in application of the Law of January 21, 1995. As a reminder, prior to the adoption of this law, the CNIL only had competence over video-protection systems installed in private premises (without any public access, e.g. private companies). There are currently 35,000 such systems notified to the CNIL in compliance with the 1978 law alone. Yet, according to the 2011 annual report of the “Departmental Commission on Video-Protection”, a total of 897,750 video-cameras are installed in France in application of the 1995 law. Furthermore, the French Government has announced an ambitious plan to roll out new video-surveillance systems, with a target of 45,000 additional cameras by the end of the Legislature.

This new oversight mission on video-surveillance systems (Law of 1995) therefore concerns a number of cameras that is nearly 25 times higher than under the Law of 1978. The magnitude of this new mission assigned by the Lawmaker will require a substantial reinforcement of the CNIL’s resources. In the meantime, our Commission has already started to exercise its new power by auditing 150 video-surveillance systems in 2011. These audits were over and above 235 others relative to the application of the 1978 law as amended. With a total of 385 audits in 2011, versus 308 in 2010 (+25%), our Commission has pursued its efforts of concrete, in situ verification of respect for individual liberties in the digital age.

The second mission originates from the transcription into French law of the EU Directive revising the "Telecom Package", and introducing an obligation to report breaches of personal data protection to the CNIL (Article 38 of Ordnance No. 2011-1012 of August 24, 2011). Data controllers in charge of personal data processing in the telecommunication industry now have the legal obligation to inform the CNIL “in the event of a breach” of data integrity or confidentiality. In case of breach of data protection by one or several physical entities, the CNIL may subsequently demand that data controllers notify the data subjects on the one hand, and on the other hand conduct audits, send notices to remedy to the data controllers, or even initiate sanction procedures.
in case of non-compliance with security requirements under their responsibility. There again, this is a new mission which, while provided under a binding European regulation, is bound to sharply modify the scope of the CNIL’s activity, in an unavoidable though yet-unknown manner, and will require boosted responsiveness and technological expertise.

In this respect, the CNIL initiated several years ago a process to diversify its staff profiles, by refocusing its recruitments on additional engineer profiles. IT experts (apart from internal IT services) accounted for less than 3.5% of our workforce in 2006, while they now represent nearly 10%. Thanks to this investment in human resources, we were in a position in 2011 to create our own in-house lab designed to test new hardware equipment and develop our own software. It should be mentioned that the CNIL is the only privacy authority among its European and international peers to be equipped with such technological expertise, an indispensable asset in the digital world. The Commission created in early 2011 a Department of Research, Innovation & Foresight (DEIP) in order to leverage the new lab’s capabilities and expertise. The DEIP was allocated a specific research budget, and focuses on a multidisciplinary analysis of new uses and new technologies, in order to enlighten the Commission on the challenges of such uses: this was the case for instance of the survey on smartphones commissioned to the Médiamétrie Institute and published in December 2011; the survey findings fuelled in particular one of the pillars of the Commission’s auditing plan for 2012.

Lastly, the extension of the Commission’s scope of competence derives from its newly assigned power of certification: on October 6, 2011, the CNIL adopted two reference standards (published in the “JO” Official Gazette on November 3, 2011) providing for certification “labels” to be granted to enterprises applying for it. The certification labels, restricted for the time being to the fields of audit and training, constitute a way for companies to differentiate or single out their products based on their compliance with the French “Informatique et Libertés” Privacy Act. The first labels should be delivered sometime in the first half-year 2012. The much-expected certification process means that our Commission is entering a new field of business, namely “quality-based regulation”, significantly different from the “standard-based regulation” practiced ever since the CNIL was established.

Clearly, the year 2011 was rich in novelties and new missions.

Meanwhile, our Commission has continued to enhance its productivity, and therefore the level of services rendered to citizens. In 2011, the CNIL adopted 1,969 decisions and deliberations, versus 1,569 in 2010 (+25.5%). In addition, we have reduced down to 4 days the deadline for delivering receipts to file-notifying organizations, versus 13 months in 2006. This improvement has been sustained over the years, in spite of increasing request flows, with an increase in notifications received by the CNIL from 70,797 in 2010 up to 82,243 in 2011. The CNIL teams deserve credit for this excellent performance, and must be congratulated here for their strong motivation.

---

1 This survey is presented in greater details on Page 23 of this Report.
1. NEW MISSIONS

Vidéo-surveillance audits: status assessment and action plan

CNIL certification labels

Notification of personal data breaches

Strategic forward-planning at CNIL: initial work, first publications

ZOOM

Smartphone and privacy: a priority for analysis and action
VIDEO-SURVEILLANCE AUDITS: STATUS ASSESSMENT AND ACTION PLAN

The Orientation and Planning Law on the Performance of Domestic Security of March 14, 2011 (LOPPSI 2) amended Article 10 of the Law of January 21, 1995 on Domestic Security, allowing the CNIL to audit so-called “video-surveillance” systems. The Commission’s competence is now legally acknowledged to verify both the video-surveillance systems subject to the 1995 law (on public highway and public places) and the video-surveillance systems subject to the 1978 law (in non-public places, such as areas restricted to employees).

IMPLEMENTATION OF AUDITS: METHODOLOGY AND TYPOLOGY OF AUDITED ORGANIZATIONS

The CNIL responded to this extended competence from the onset when adopting its annual 2011 audit plan: at the Commission assembly on March 24, 2011, 150 audits of video-surveillance systems were targeted, an objective which was fully achieved. The 150 audits were conducted in various locations across the French national territory.

75% of the audits were conducted in the private sector (stores, hotels, restaurants, enterprises, banks, etc.) and 25% in the public sector (train stations, schools, museums, local government offices, etc.).

The audited organizations were selected to ensure compliance with the law across all situations where a video-surveillance system can be installed. Thus, they were selected based on their size – and therefore the number of persons potentially videotaped (e.g. audits were conducted both in small-size shops and in large department stores in Paris), on their location (shopping mall and high-street), and sometimes also on current news (e.g. press articles highlighting a system being installed).

The following main items were verified:

• Compliance with the Prefect authorization delivered in terms of purpose and camera orientation,
• Length of image retention,
• Information to videotaped persons,
• Security measures surrounding the system.

Approximately 15% of the audits were carried out in the context of investigations on complaints filed. It should be noted in this respect that the Law of January 21, 1995 expressly provides that “Any interested person may file a complaint [...] with the Commission Nationale de l’Informatique et des Libertés on any difficulties related to the operation of...
a video-protection system”. Thus for instance, the CNIL received a petition from a group of employees questioning the lawfulness of cameras installed in their company, or from customers who had noticed a video-surveillance system unannounced to the public, etc.

It should also be noted that the CNIL received a request from SNCF (French Railway Company) asking for audits to be carried out in order to check the compliance of its video-surveillance systems installed in train stations. The Law of 1995 allows video-surveillance system controllers to request the CNIL to audit their installations. In the context of this “partnership”, the CNIL conducted more than twenty audits of the video-surveillance systems installed in train stations across the entire French territory.

Any person may file a complaint with the CNIL on any difficulties related to a video-protection system

The ‘Commission Nationale de l’Informatique et des Libertés’ may, upon request from the Departmental Commission as provided under Paragraph 1 of this Article III, or from the data controller in charge of the system, or on its own initiative, verify that the system is used in accordance with [the relevant Prefect authorization] and depending on the relevant legal regime, in compliance with the provisions of this Law or of the above-mentioned Law No.78-17 of January 6, 1978.

1 LOPPSI 2 Act / March 14, 2011
MAJOR AUDIT FINDINGS

- The audited system controllers fully recognized the CNIL’s competence as regards audits of their video-surveillance systems.

  Based on the Commission’s findings, it was noted that none of the audited systems, except for one, had ever been verified by any other authorities (police, Prefectures, etc.). The CNIL’s audit therefore filled a gap in terms of verification of surveillance systems potentially intrusive on individual privacy.

- A lack of homogeneity was found in the authorizations delivered by the various Prefectures, both in terms of competence (i.e. application of the 1995 Law to places such as childcare nurseries, or non-public areas in retirement homes) and of areas allowed for filming (e.g. some Prefectures refuse video-filming in restaurants and eateries, while others accept it).

  The following main cases of non-compliance as related to the effective conditions for video-surveillance systems, were noted during the audits:
  - Lack of Prefecture authorization or renewal of authorization (around 30% of audits). These cases are most frequently found when conducting an audit to assess the compliance of a system subject to the 1978 Law, revealing that the system also records in areas open to the public;
  - Lack of notification to the CNIL for systems subject to the 1978 Law (around 60% of cases);
  - Non-existent or insufficient information of individuals (around 40% of audits);
  - Inadequate camera orientation (around 20%). A number of audits revealed “hidden” cameras, in smoke detectors in particular;

- Excessively long period of image retention (around 10%); Insufficient security measures (around 20%).

  Accordingly, and based on Article 10 III of the 1995 Law, the CNIL issued three formal notices to comply regarding video-surveillance systems. The Prefectures having territorial competence over the matter were also informed.

  Audit findings also revealed the occasional use of dummy cameras, along with some malfunctions likely to affect the video-surveillance systems (no recording, poor image definition, etc.).

  Lastly, the audits have shown that videoprotection/videosurveillance system controllers frequently have difficulties understanding the linkage between the Informatique et Libertés Act and the Law of January 21, 1995.

40% OF AUDIT REVEALED NON-EXISTENT OR INSUFFICIENT INFORMATION TO DATA SUBJECTS

- Around 50% of the audited systems fall under the scope of the 1995 Law (cameras filming public areas, or “customers” areas) and of the Informatique et Libertés Act (non-public areas: i.e. “restricted” to employees).

  Yet, when delivering authorizations, the Prefecture authorities never refer to the 1978 Law among the legal provisions requiring compliance. At best, some Prefect authorizations mention the prohibited processing of recorded images.

  Nevertheless, the enforcement decree of September 14, 2011 relative to the legal framework applicable to the installation of video-surveillance cameras acknowledges that the Informatique et Libertés Act applies to systems installed in non-public areas. The CNIL has therefore decided to contact the local Prefectures to ensure that they refer properly to the relevant provision of the Informatique et Libertés Act.

FOCUS

Outlook for 2012

Similarly to the partnership model developed with SNCF, the CNIL will start auditing the RATP (metro authority) video-surveillance devices in 2012, in order to check that the system installed by RATP complies with the provisions of the 1995 Law. Audits will be conducted across the entire RATP metro network in the first quarter of 2012.

In 2012, the CNIL will continue auditing video-surveillance systems, affording priority among other to systems affecting a large number of people (e.g. systems installed in local government administrations or other premises with high public traffic), as well as video-surveillance systems also used for ancillary purposes such as “video-finishing” (“vidéo-verbalisation”) for traffic offenses.
CNIL CERTIFICATION LABELS

The Law of August 6, 2004 introduced the possibility for the CNIL to grant certification labels to products or procedures. In September 2011, the Commission amended its internal regulations in pursuance of Article 13-II of the Law of January 6, 1978 as amended, in order to specify the “conditions of implementation of the label certification procedure”.

For businesses, the CNIL Label is a differentiating factor attesting to the quality of their products or services. For their customers or users, it constitutes an indicator of quality, and therefore a factor of trust guaranteeing a high level of data protection. For the CNIL, it is a vector to disseminate the “Informatique et Libertés” privacy and data protection culture, along with a means to enhance the enforcement of the law. Certification labels therefore represent a strategic challenge for the Commission, fully in line with the planned revision of EU Directive 95/46 (Article 39 of the draft European Regulation).

The Commission opted initially to certify data processing audit procedures and Informatique et Libertés training programs. The CNIL Labels were officially launched in October 2011 with the adoption of the first two certification reference models.

LABEL CERTIFICATION PROCEDURE

Creation of a reference model

The first step is for a professional organization or institution regrouping data processing controllers to send to the Commission a request for a certification label related to products or procedures. Based on this initial application, the Commission will start investigating the opportunity of adopting a given reference model for a new category of products or procedures. In the course of this process, the Commission may meet with stakeholders (administrations, certification authorities, etc.) in order to ensure the consistency of its goals with the needs and level of market maturity.

Further to this preliminary investigation, if the Commission considers that granting a label to this category of products or procedures is appropriate, the CNIL will then develop a suitable reference model to be approved by its plenary assembly as a formal deliberation. Once this document is published in the Official Gazette (“Journal officiel”), any company wishing to apply for the certification label can send a request via the standard form accessible from the CNIL web site.

Two businesses with separate activities (e.g. a law firm and an IT service provider) may opt to partner and file a single label application; this is called a “joint certification label”. In this case, the applicants undertake to collaborate throughout the term of validity of the label.

Examination of a label application

This examination takes place in two phases: review of eligibility and assessment of compliance of the product or procedure.

The review of eligibility ensures that the application is complete in form, and that the product or procedure matches the item defined in the reference model. The application is deemed ineligible should the Commission fail to reply within a deadline of two months.

Once the application is found eligible, the Commission staff will proceed with an assessment of the product or procedure. The goal is to ensure that the product or procedure fulfills all requirements of the reference model, based on appropriate documentary evidence (application form, processes, curriculum vitae…). To this purpose, the CNIL staff may request any relevant additional material or document, and interview the applicant. Once the assessment is completed, the Commission’s plenary assembly will formally decide whether...
or not to grant the certification label. If the label is issued, then the final decision is deemed to authorize the use of the “Label CNIL” logo.

**Life of the CNIL Label**

The certification label is delivered for a term of three years. The beneficiary is required to present a renewal request six months at the latest prior to the label’s expiry date.

In case modifications in the characteristics of the certified product or procedure prior to the expiry date, the beneficiary has the obligation to inform the Commission in writing. Such modifications will then be analyzed by the staff in order to assess their extent. Should the changes be identified as substantial, the product or procedure will be fully reassessed; otherwise, the initial term of three years will continue as is.

In the event that the Commission may learn of facts or circumstances likely to challenge the compliance of a certified product or procedure, the CNIL may decide to withdraw the label further to a joint review process.

The reference models may involve specific obligations requiring the label beneficiaries to demonstrate that the initial conditions for label issuance are retained continuously throughout the term of validity (e.g. annual activity report forwarded to the Commission).

---

**FIRST TWO ASSESSMENT MODELS**

**Procedures for personal data processing**

The *Informatique et Libertés* audit addresses criteria designed to assess the legal compliance of personal data processing operations. The audit scope covers personal data processing operations carried out by a data controller within a delimited scope. This scope may be quite extensive and encompass all data processing operations in a company, or may be restricted to a given field, e.g. processing of human resources data.

The reference model designed to assess procedures for personal data processing audits (ref. CNIL Deliberation No.2011-316 of October 6, 2011) sets the criteria to be fulfilled in the following two categories:

- **Criteria relative to the data processing audit procedure.** These criteria include primarily requirements relative to the competence of auditors and to the audit implementation procedure (preparation, execution and finalization), inspired from international standards, and in particular the ISO 19011 Standard (*Guidelines for quality and/or environmental management systems auditing*, designed for adaptation to other types of audits),

---

**Focus**

**Stringent requirements on access to data**

In order to ensure the preservation of the interests and fundamental rights of data subjects in accordance with the principles of proportionality and security, the reference model sets two important limits to the access to personal data by auditors:

- Any data collected in the course of the audit must be anonymized whenever they are to be taken out of the premises of the audited organization. Thus, any material evidence included in the audit report must be presented in an anonymized format, except if the document is entirely drafted and consulted within the premises of the audited organization;
- Full confidentiality of personal data must be guaranteed via a clause in the contract signed between the auditor and the auditee; such clause must in particular refer to the above-mentioned principle of anonymization.
in view of the specific characteristics of the Law of January 6, 1978 as amended and of its provisions on the security of IT systems.

> Criteria on contents of the data processing audit. These criteria were developed in such a way as to be adaptable to the various approaches of audit professionals. They are verifiable; applicants may provide supporting evidence in a free format (excerpts from methodology, standard questionnaires, internal documentation, etc.). These criteria require the auditor to demonstrate the systematic and documented application of a methodological approach, thus giving the possibility of verifying the effective compliance of the audited data processing operations with legal provisions.

“**Informatique et Libertés**” training program

An “**Informatique et Libertés**” training program is a procedure intended to deliver and develop the knowledge and know-how necessary to ensure compliance with the **Informatique et Libertés** Act. The training session may take place over several days and include several self-standing modules. The certification label is granted to an organization and to the training program contents, but not to training individuals.

The reference model for training assessment (ref. Deliberation No.2011-315 of October 6, 2011) sets the criteria to be fulfilled in the following two categories:

> Criteria relative to the training activity. These criteria assess the organization’s compliance with the **Informatique et Libertés** Act, the trainers’ competence, along with the conditions of creation, delivery and updating of the educational contents. They are inspired from the international ISO 29990 Standard (**Learning services for non-formal education and training - Basic requirements for service providers**). This reference model is intended to identify, for each phase of the training activity, the key criteria to be fulfilled to create the appropriate conditions for high quality learning, both in form and in substance.

> Criteria relative to the training contents. These criteria specify the items to be addressed in the course of the training session. The reference model refers to the contents and architecture of the **Informatique et Libertés** Act, covering most of the law’s scope of application. These criteria require the organization to demonstrate that the training program and the trainer have the capacity to help learners understand and become knowledgeable about the aspects of the law contained in the training curriculum.

Apart from reviewing the educational material, the CNIL may, if deemed necessary, interview the trainers and attend a training session. These requirements are of two types:

> Requirements on the primary module, consisting of the fundamentals of the law (principles and definitions, rights of data subjects, etc.). These points must absolutely be addressed in the training program. The training session may however include several days or modules. Provided the above-mentioned requirements are fulfilled in one training day or module, the training program may be eligible for the certification;

> Requirements on optional modules which may for instance address the role of the Data Protection Officer, the oversight of health-related data processing, or the CNIL’s sanctioning powers. The modules are optional and will be evaluated only when included into the full learning curriculum.

The assessment should not be limited merely to a documentary review by legal experts, but must also rely on physical verifications of the audited information systems by IT experts.

**Necessity for verifications**

For instance, the auditor must assess the data retention periods, to be supplemented with a verification in the IT system to check its effectiveness.

The first certification labels will be granted in 2012. A list of the audit procedures applicable to the certified data processing operations and training programs will subsequently be accessible on the CNIL web site.

**Focus**

**Prerequisite: applicant’s Informatique et Libertés process**

Since training organizations collect and process the learners’ personal data, it was found necessary to define requirements relative to the organization’s compliance with the **Informatique et Libertés** Act, as it would be inconceivable to grant the CNIL Label to any organization failing to provide minimum guarantees of compliance with the Law of January 6, 1978 as amended.
NOTIFICATION OF PERSONAL DATA BREACHES

The media regularly report on thefts of customer accounts during computer hacking attacks, or disclosures on the internet due to the inadequate configuration of a web site. Such mistakes are multiplying, frequently to the detriment of individuals whose personal data end up being lost, stolen, disclosed or destroyed.

In such circumstances, the law did not recommend any specific form of alert. The only legal obligation of data processing controllers was to guarantee the security of the data. But what to do when security fails and a mistake is made?

NEW EUROPEAN-SCALE OBLIGATION

"Prevention is better than cure"

Back in 2002 in the State of California, the concept was born of forcing business players holding sensitive data to inform an authority as well as the data subjects about any breach of confidentiality of the data. A large majority of US States have since adopted similar laws.

Preventing rather than curing, this could be the fundamental principle of this new obligation. From the consumer’s perspective, prevention means warning them so they can take action (e.g. cancel and change their credit card) rather than risk identity theft or bank account fraud.

From the business perspective, business players have the responsibility to prevent data breaches by reinforcing their internal security measures rather than merely reporting notifications that are costly and damaging to their brand image.

Numerous countries have adopted this principle, including Germany, Spain or Ireland.

In France, this new responsibility had already been proposed by Senators Anne-Marie ESCOFFIER and Yves DETRAIGNE in a bill “designed to better guarantee privacy rights in the digital age”, which unfortunately had failed to reach final adoption by the Parliament.

From Brussels to Paris: adoption of a new obligation

The European Commission drew its inspiration from these existing mechanisms and adopted the principle of such an obligation when revising the “Telecom Package” Directives.

However, since the Telecom Package is the European legal framework for electronic communications, the obligation to notify security faults was restricted to providers of electronic communication services.

The national data protection authorities from EU Member States, speaking jointly as the G29, have expressed their position with the publication of two official opinions issued prior to the final adoption of the Directive, followed with a further opinion about the legal framing of breaches of personal data. The G29 expressed its wish to see this obligation generally extended to all parties using
personal data, and in particular to e-commerce sites and on-line banks.

This recommendation was unfortunately not followed, due to the industry-specific nature of the Telecom Package (addressing only electronic communications). The Draft Regulation revising the 1995 Directive however extends this obligation to all data processing controllers.

On 26 August 2011, the Telecom Package Government Decree transcribed into French law the notification obligation, now incorporated into Article 35 bis of the Informatique et Libertés Act.

---

NEW REMIT FOR THE CNIL

**A complex mission**

All personal data breaches related to telecom service providers must now be systematically notified to the CNIL, regardless of their degree of severity.

The CNIL will have to analyze numerous situations against the particularly broad definition of “breach” (or “violation”).

Destruction, loss, alteration, disclosure or unauthorized access will constitute cases of breach of personal data. Such breach may result from an act of malevolence, e.g. in the case of computer hacking; or from an error made by an employee that would destroy or disclose a customer file due to a faulty operation.

The CNIL will therefore need to manage new flows of information and verify that individuals were duly informed as required by law.

Unlike notifications made directly to the CNIL, the process of notifying data breaches to individuals is not systematized. If all breaches, including inconsequential ones, were notified to individuals, the data subjects would end up being submerged with alerts and would no longer pay them any attention. Such an attitude would actually be prejudicial to the very raison d’être of the system. This is why only breaches that may prejudice individuals must be notified. The Directive 2009/136/EC specifies that “A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation [...].”

In practice, the destruction of a customer file that was previously saved, does not appear prejudicial to individuals. Similarly, in the case of a customer file subject to computer hacking but without any possibility of being opened without prior decryption with a confidential password that has not been hacked, the risks to individuals also seem limited.

The law specifically provides for such cases by waiving the obligations for service providers to inform individuals whenever appropriate protection measures have been adopted.

---

**What is the EU Telecom Package?**

The phrase “Telecom Package” designates a set of EU legal texts adopted in 2002, defining a common legal framework on the regulation and control of electronic communication networks and services. This is therefore an industry-specific tool that is not intended to apply generally to all Internet stakeholders.

The main purpose of this legislative package was to regulate the management of national communication networks open to the public and to force the major incumbent telecom operators to open up the market to competition.

This regulatory framework has been widely revised since then, with the adoption of new provisions by the European Parliament and EU Council on 25 November 2009. One of the goals was to improve the protection of personal data and individual privacy in the sector of electronic communications.

The Member States were under the obligation of transcribing the new provisions into their national laws prior to 25 May 2011.
Should such measures prove insufficient to guarantee that the data cannot be used by any third parties, the Commission may send formal notice to the service provider to notify the data subject of the breach. This procedure is intended to encourage data controllers to adopt efficient security measures from the onset.

**Ever more security**

In 2012, the CNIL will therefore need to implement the new mission entrusted to it by the lawmakers. In particular, it will have to support electronic communication service providers in assessing and implementing efficient protection measures.

The CNIL already questions the data controllers regularly about their security obligations and offers advice and guidance on the best practices to be implemented, both for the review of their authorization requests and for the investigation of advice queries. A “personal data security” guidebook was published on the topic in 2010.

**Towards more transparency**

The new obligation of notification is part of a process of increased accountability of the parties responsible for personal data.

It no longer involves waiting until the victims file a complaint and for the CNIL to check and sanctions; the data processing controller must now fully endorse the responsibility for any errors previously committed in order to enable individuals to avoid falling victim of breaches. This obligation will enable the CNIL to gain a better vision of the security level implemented, as well as to offer better support and guidance.

**Security fault or breach of personal data: What is the difference?**

The term “security fault” is often used as a synonym of “breach of personal data”; yet a security fault (or security breach) does not always concern personal data. For instance, a breach of security instructions by an employee misusing the IT tool does not necessarily mean that the stored personal data have been compromised. The English phrase “data breach” is more explicit, since it refers both to the fault and to the data.

The enforcement decree for the Telecom Package Ordnance was published on March 31, 2012, amending the “Informatique et Libertés” enforcement decree of 2005 (articles 91-1 et seq. were added). These legal provisions specify the conditions for the application of the new Article 34 bis of the Informatique et Libertés Act, and describe how the CNIL must be notified, along with cases where individuals must also be notified.
STRATEGIC FORWARD-PLANNING AT CNIL: INITIAL WORK, FIRST PUBLICATIONS

The DEIP, or Direction des Études, de l’Innovation & de la Prospective (Department of Research, Innovation & Foresight) was created in January 2011 to develop strategic forward-thinking within the CNIL. Serving as a resource center on forward-planning and market intelligence for the entire Commission, the DEIP Department works in liaison with other departments to contribute to identifying and analyzing innovative technology uses and the related trends in regulatory methods.

Analysis of usages lies at the core of the DEIP’s forward-planning work. In 2011, the Department looked at the behaviors of youngsters on social networks (ref. Chapter 3) and at smartphone use practices. This research is conducted based on an approach that is deliberately multidisciplinary – economic and sociological, in particular – rather than merely technological or legal.

The first forward-planning projects decided by the Commission were initiated following the recruitment of a “Prospective” Research Coordinator in July 2011.

INITIAL PROJECTS

Upon proposal from the DEIP Department, the Commission decided to launch two major forward-looking studies in 2011, both of which are currently underway.

Smartphones and their ecosystem

The smartphone has become the central nervous system of digital life. The DEIP has therefore decided to explore the trends over the next 5-10 year timeline as related to the smartphone “object”: business players, upgrades in profiling and personalizing techniques, potential forms of regulation, etc.

The first step involves a status assessment of practices. A poll was conducted to gain knowledge and understanding of the daily practices of smartphones users, and assess their level of perception on issues of personal data protection. The highly enlightening results from this survey were made public in December 2011, and their subsequent in-depth analysis is presented in this annual activity report. The findings revealed a strong perception of opacity and of insufficient security as regards the data “exiting” the smartphones, leading the Commission to devise an action plan, focused among other on developing a genuine education about smartphone uses.

Concurrently, a technical and economic study of smartphone uses was commissioned in October 2011 to a research and consulting firm who partnered with a consultant specialized in information technology law and with an IT security consulting firm. Their initial focus will consist in an inventory of mobile-related technologies and services, such as position sensors or geolocation, but from a forward-looking angle: i.e. what evolutions can we expect within the next 5 or 10 years? It also involves a status assessment, as well as an analysis of trends in the players’ business models and strategies (Apple, Google, Amazon, SFR, Nokia etc.). These technologies and
strategies will be analyzed simultaneously in terms of security and risk assessment. In light of this information, existing regulations and their potential evolutions will then be analyzed in order to arrive at four or five scenarios on smartphone regulations over the next 5 to 10 years. The research findings should be available in the spring of 2012.

Project on “Privacy 2020”

This ambitious project is entitled “Privacy, Liberties and Personal Data by 2020. What challenges for regulations and for the CNIL?”. The CNIL has opted for a resolutely open approach to conduct this project regarded as strategic for the Commission. The process consists in interviewing experts and stakeholders in various fields: economists, sociologists, historians, philosophers, representatives from research institutes, community associations, think tanks, business players, etc. These interviews are intended to collect their perceptions on future evolutions regarding the topics of privacy, individual liberties and personal data. The purpose also involves learning about their interpretation of future forms of regulations and of the CNIL’s future role. The project further provides the Commission with an opportunity to boost its visibility with some stakeholders and to build up a network of academic experts, as a prelude to creating a forward-looking think-tank on privacy and data protection issues.

Work on this project was launched in September 2011, in the form of some thirty semi-directive interviews to be later compiled into a comprehensive report, and subsequently followed by a seminar to be organized some time in 2012.

Lastly, the Commission has decided to establish a “Prospective Committee” in 2012. As an advisory and consulting body reporting to the DEIP Department, it will in particular be in charge of issuing opinions regarding the DEIP research program, and will contribute to the evaluation of the research findings. This joint Committee will comprise two Commissioners and six independent experts with competence in economics and sociology among other fields.

IP NEWSLETTER

The IP Newsletter (IP stands for “Innovation & Prospective”), created in September 2011, is edited by the CNIL Department of Innovation & Foresight and circulated in both print and electronic formats. The quarterly newsletter is designed to inform a broad net of experts, stakeholders and parties from all horizons interested in issues related to technologies, uses and privacy. It is intended to fuel forward-thinking in debates and investigations about future issues of personal data and privacy protection, and to encourage exchanges with experts and stakeholders.

The first issue primarily presented the DEIP’s activities, the work conducted on social networks and youngsters (ref. Chapter 3), and the European research program PRACTIS about the future of privacy. Other publications will gradually be accessible, in particular on the CNIL web site. The DEIP Department thus plans to publish its “Cahiers de la Prospective” reporting on the results of its projects and research.

The in-house “prospective watch” has also expanded significantly. A documentary intelligence database on forward-planning topics related to personal data protection is currently being compiled. A “Prospective” section was created on the Commission intranet to circulate alerts and analysis memos.

Along this line, the CNIL should be equipped by late 2012 with a new documentary IT system enabling a new knowledge management policy to be implemented, an indispensable tool for efficient forward-planning watch.
PARTNERSHIPS AND COOPERATION

In 2011, the CNIL further developed its cooperation with the world of research and academia, and initiated several partnerships to this purpose, as a way for the Commission to be closer to the heart of the innovation and research process, to better hear and understand the needs and concerns of both researchers and enterprises.

The Commission bolstered its cooperation with ANR (the National Research Agency) via a number of initiatives:

- **Participation in research project steering committees.** The DEIP Department is involved in the following steering committees:
  - program “Concepts, systems and tools for global security”;
  - multidisciplinary research program on security;
  - program “Contents and interactions” (CONTINT) designed to fund innovative projects related to digital contents for all types of media (cinema, web, personal contents, etc.) and to robotics. Apart from the benefits of publicizing the CNIL in the research arena, this cooperation has the added benefit of identifying projects that may involve potential issues of data protection, thereby ensuring that related ethical issues are embedded from the onset, and that the projects will receive guidance on their data protection and privacy components.

- **The Commission is also a member of the ANR Review Committee for a multidisciplinary research project addressing the use of personal data on the Internet.**

The CNIL has entered a partnership with INRIA, reflected firstly in the signature of an agreement in July 2011, and in late 2011 in the joint launch of an educational research project entitled “Mobilitics”. The project is intended to understand and explain the privacy risks related to the use of smartphones via an in-depth analysis of the data that are saved, stored and disseminated by the devices. The initial findings should be available in the spring of 2012.

A **partnership agreement was signed in December 2011 between the CNIL and the “Conférence des Grandes écoles” (CGE), designed in particular to raise the awareness of students, faculty and administrative staff to privacy issues related to communications, to encourage the appointment of CILs (Data Protection Officer), and to envisage joint research projects.**

Other cooperation initiatives are also underway or under consideration, based on various conditions, with some individual “Grandes Écoles” targeting specific research projects.

Lastly, a number of ad-hoc partnerships were signed, for instance with UNAF in partnership with “Action Innocence” on a survey conducted with youngsters in June 2011 about their use of social networks (ref. Chapter 3).

**FOCUS**

**CNIL “Informatique et Libertés” Thesis Awards**

The CNIL “Informatique et Libertés” Thesis Awards are intended to reward valuable thesis work and to spur academic research on the topic of privacy and personal data protection. The awards target numerous disciplines such as human sciences, law, political science, economics or technical disciplines. A prize of 7,000 euro is awarded to the winner, to facilitate the thesis publication.

The jury presided by CNIL member Jean-Marie Cotteret awarded the “Informatique et Libertés” 2011 Award to Jean-Raphaël DEMARCHI, researcher at the Center for Studies & Research in Private Law (CERDP) and Lecturer at the University of Nice-Sophia Antipolis, for his thesis entitled “La preuve scientifique et le procès pénal” (Scientific Evidence and Criminal Trial). The thesis is planned for publication very shortly.
The CNIL decided to create an in-house laboratory equipped with dedicated IT resources, in order to try and test innovative products and applications, for the following purposes:

- Have access to new products as early as possible before their marketing or recently introduced on the market in order to test their functionalities, and assess their impacts on privacy protection;
- Disseminate a technological culture and education on uses, by developing for the public at large a number of tools designed to better protect privacy, and test the feasibility of new privacy-protection solutions;
- Under a rationale of “privacy by design”, bolster its duty of adviser to enterprises, relative to incorporating personal data protection requirements into their technology development processes;
- Contribute to the development of privacy-protection technological solutions;

The CNIL needs to understand and support technological, social and legal innovation

- Strengthen the technical credibility and influential capacity of the CNIL, among other with the technical and scientific communities;
- Conduct advanced technical analyses on specific topics, e.g. for purpose of publication in specialized journals.

The Lab, installed and supervised jointly by the Direction des Etudes, de l’Innovation et de la Prospective (DEIP) and the Expert Appraisal Department, was gradually established in 2011. Once the hardware platform was fully installed, the Lab began to work on a myriad of technical investigations and analyses, such as the transmission of geolocation data via iPhones (see Page 58). In this particular case, an iPhone 3Gs was “placed under surveillance”, leading to a number of findings on the data transmitted. The Lab also conducted several quick analyses when the media reported on the discovery of the “Carrier IQ” software imbedded by smartphone manufacturers at the request of US telecom operators. The lab equipment verified whether traces from this software were visible or not on the French devices. The CNIL lab found no traces left by the software on the lab’s Android-based devices; and although a trace seemed to be left on the Apple iOS devices, the software seemed to be inactive from the start. Investigations of this type will be multiplied in the future in order to respond very quickly to the introduction of new products and services.

Concurrently, the Lab will grow in scale from the technical perspective, with the performance of more extensive projects, in particular under the partnership with INRIA. The Lab will gradually expand its works with more experimenting, testing and tool developments. It will then be in position to broaden the scope of its activities to support innovative and experimental initiatives carried out by the CNIL in all areas of interest.
SMARTPHONE AND PRIVACY: A PRIORITY FOR ANALYSIS AND ACTION

19 million
MOBILE INTERNET SURFERS IN FRANCE

48%
OF SMARTPHONE OWNERS USE IT ON SOCIAL NETWORKS

65% of mobile users feel that their personal data are not well protected

The CNIL has opted to use forward-looking analysis and practical experimentation in order to investigate over the long term the personal data issues raised by these ubiquitous digital mobile companions. Within just a few years, mobile devices have become the primary interface for “always-on nomadic communication” as well as the central nervous systems of users connected everywhere and all the time. Yet, the smartphone still remains a “black box” for its owner. Worries are growing about the users’ largely justified impression that they are incapable of having any clear idea regarding the recording, storage and “external leakage” of their personal data related to the use of the available functions, services and applications. The volume of data liable to be released is considerable, ranging from contact lists, to geolocation, including all kinds of identification data.

Such a situation is unacceptable both for users and for the CNIL. It is also unsustainable over time for the business players. Improvements will have to take place, at the risk of triggering recurring scandals and controversies. Accordingly, the CNIL intends to reinforce its role as a “prescriber of best practices”, by cooperating with business players, for the benefit of the users’ rights to privacy. Several initiatives were launched in the second half of 2011 in this perspective, leading to an enhanced understanding of the issues related to smartphones, and laying the foundations for a 2012 action plan focused in particular on actions to be conducted by the in-house laboratory.
At the CNIL’s request, the Médiamétrie Institute questioned on the Internet a group of 2,315 persons between November 4 and 14, 2011, including a targeted sample of 198 persons aged 15 to 17, with the following goals:
- Determine the types of smartphones used in France, and the daily uses;
- Measure the perception of smartphone users about the contents and personal data stored on their phones;
- Describe and understand the risks perceived by users, and the protection systems installed;
- Propose practical advice to smartphone users.

The main findings, presented to the press on December 12, 2011, are also accessible on the CNIL web site.

The smartphone: a companion of every moment

While the smartphone-equipped population still remains somewhat specific (male, high socio-economic status, urban, etc.), differences are however quickly fading away with the democratization of the device: according to GFK Institute, 11.4 million smartphones were sold in 2011, and according to Médiamétrie, there were 19 million mobile internet surfers in France in late 2011.

The poll nevertheless identified differences in the perception of the place taken by smartphones in our lives depending on age: used as a simple “advanced” telephone by the 50+ population (described as a “communication tool” by 35%), but an indispensable device for the “always-on” population (described as an “always-on connection tool” by 30% of the 15-17 age group).

While youngsters have very specific uses (games, social networks, instant messaging), the service offering is so wide-ranged that each profile has its own intensive uses (e.g. 50+ group: management of medical data). Thus, 48% of smartphone owners use it on social networks (69% of 15-17 group), and 67% of those do so every day. The poll further revealed that as owners become more familiar with their device, its uses become more intensive: interviewees who owned a smartphone for over 2 years consult their bank account in greater numbers. Appetence for highly “personal data-intensive” applications appears to be substantial and to grow along with confidence.

The smartphone was initially a business tool, with the conventional image of the businessman or manager and their “Blackberry”, but this is absolutely no longer the case today; 74% of smartphone owners use it primarily for personal purposes. A trend reversal is actually observed: the personal devices have become so important, so convenient, so useful and so powerful that individuals also want to be able to use them in business contexts, and possibly against compensation. Enterprises are forced to adapt to this demand, with systems like BYOD, for “bring your own device”: they are attempting to develop and supply business solutions and applications that are usable on personal devices. The CNIL opinion poll thus revealed that 56% of the interviewees use their main smartphone partially for business purposes, and 36% of the higher income category (“CSP+”) report using it “equally for business and personal purposes” (vs. 21% of the general population) (see graph below).

Opacity of personal data uses

Awareness of the presence of personal data on smartphones is largely shared among their owners. The poll shows no major gap between the users’ intuitive perceptions and the reality of the data actually recorded, nor any real “negligence” about personal data. It should however be noted that 15% of the respondents stated that they store no personal information on the phones, which is actually impossible, indicating for this portion of the population (higher ratio in the 50+ age group and for persons who have owned their smartphone for under 6 months) a low level of knowledge about the challenges related to such information and to the use of the device.

Conversely, opacity prevails in any case regarding “exits” or “leaks” of personal data (communication to operators, manufacturers, application publishers...).
or other third parties). Over half of the respondents think that their data cannot be transmitted without their prior approval, while the other half believe that it is possible. In any case, regarding all questions of this type, individuals expressed both their lack of knowledge and their desire to better understand what mobile services or applications can or might do with their personal data, in terms of storage and transmission. This anxiousness is particularly evident with respect to geolocation, regarded as a newly emerged issue about sensitive data.

Furthermore, a lack of clarity still persists in the users’ mind regarding what business players are doing with their personal data and regarding their rights: 51% of the respondents believe that their data may not be saved or transmitted without their approval, thereby attesting to a lack of knowledge of actual facts.

The world of applications (“apps”) that is becoming parts and parcel of the daily life of smartphones users, further darkens this opacity: “apps” are omnipresent... and sometimes much too nosy! 63% of respondents who have already downloaded apps, stated having actually refused to install one because of the terms of use; and this number would probably increase if users really knew what they were authorizing (authorizations being sometimes worded in insufficiently explicit terms). Numerous studies, including those carried out by the Wall Street Journal about the most popular smartphone apps in the US (e.g. What they know – mobile)\(^4\), reveal that a lot of personal data are now transmitted unbeknownst to the users. This lack of knowledge is partly due to the fact that the terms of use for services and applications, hardly legible or comprehensible, are rarely read (71% of respondents fail to read them systematically), but due first and foremost to the fact that providers fail to show much transparency in this respect.

**Geolocation: a new sensitive issue?**

Geolocation services are probably the function that is currently spreading the widest and fastest. Over 55% of smartphone owners use geolocation services: obviously, for searching for itineraries or maps, scouting one’s surroundings, or recommendations about specific places. Other functions like identifying one’s presence in a given place, or checking on the location of one’s family members still remain very limited, but are however already used by 10 to 25% of geolocation service users.

The reaction of poll respondents was nevertheless unequivocal: over 90% of them want to be able to choose the time when they are geolocated, to control the recipients of the geolocation data, to know how these data are used, as well as be able to refuse any transmission.

These findings are consistent with those of a focus panel conducted by the CREDOC and published in the October 2011 report on the “Spread of ICTs in French society”\(^3\). According to this survey, 81% of mobile phone owners would like to have the possibility of prohibiting the transmission of their geolocation data to commercial businesses. The CREDOC further commented that “most interesting is the change that has occurred with younger users: while they were relatively at ease with it in 2008, 75% of them now wish to be able to veto the transmission of their geolocation data to third parties (+21 points in three years, the highest growth rate)\(^5\). Geolocation should most likely be regarded as a new source of sensitive data, usable and communicable by business players, to be framed by regulations consistent with the high expectations of individual users.

---

\(^1\) For this target sample, replies were collected with parents’ approval.  
\(^2\) A minority most likely use as their primary phone the device supplied and funded by their employer, although such cases remain a minority. Thus only 25% of managers use a company-supplied smartphone, according to the latest Manager Climate Survey conducted by Opinion Way on behalf of the CFE CGC trade union (May 2011).  
\(^3\) Source: CREDOC – La diffusion des TIC dans la société française - (2011).  
\(^4\) http://blogs.wsj.com/wtk-mobile/
The smartphone: a black box we don’t know how to protect

Smartphone owners neglect protection systems, most likely due to technical ignorance or simply for convenience. Thus, over one fourth of the respondents stated having no lock-down code. Yet at the same time – and this is another privacy paradox, 65% of them feel that their personal data are not well protected.

The poll also clearly reveals that smartphone owners do not all have a similar perception of either the protections implemented or the risks incurred. Very few are really “confident”, less than one fourth may be qualified as somewhat “paranoid”, but the two main families of French smartphoneers emerging from the survey are made up of the “nonchalant” (28%) and “insouciant” or “carefree” (34%) who are not really interested in the protection of their smartphone-based data and do not feel it is important, either because they do not want to devote any time and effort to it, or because they do not believe that the related risk is important.

In addition, several poll results show that the 15-17 age group is “relatively” cautious. Teenagers use more lock-down codes than the average population, and are more mistrustful about the recorded data. A possible explanation for this finding is first of all that the smartphone is often the one valuable object that is truly their own. Furthermore, they are most likely concerned primarily with limiting their parents’ supervision. And lastly, their “user experience” is intensive and multi-format and they use it as a means of digital technology learning and acculturation.

This poll simply reconfirmed that youngsters no longer use Internet “like before”, and that the role played by parents in digital education cannot merely be a matter of technical control (e.g. via parental control software) or of on-line time management. Yet in reply to the question “Would you use the geolocation function to locate your children if it were simple to use?”, 65% of parents with children under 18 replied “yes”. Apart from watching over their children, parents must also fully play their role of digital educators, and speak clearly with their children about real uses. Particularly since the survey shows that, by doing so, they can learn some lessons about their own practices!

40% of users store data of a secret nature
30% of smartphone users have identified the CNIL as a legitimate stakeholder for information on security.

ACTION PLAN 2012

As regards security and information about personal data, over 30% of smartphone users have identified the CNIL as a legitimate stakeholder, ahead of operators and manufacturers.

Based on the poll findings, the CNIL has started to advise users with a list of tips that were delivered to the media for publication at a press conference on December 13, 2011.

These privacy security tips were later illustrated in a video tutorial, also accessible on the CNIL web site.

Based on these findings, the CNIL intends to develop on its own a number of projects and tools to better comprehend this “shadow economy” of personal data on smartphones, in particular by mobilizing the resources of its new in-house lab.

Over the coming months, the CNIL will be inventorying the players’ best practices in terms of information and user control over personal data. This is an issue of utmost importance for the entire mobile economic ecosystem, as shown by the initiatives adopted by GSMA (the global association representing the interests of mobile operators worldwide) on the issue of “Mobile and Privacy” since 2011 (definition of design principles and guidelines), along with recent controversies about unlawful access to personal data by some applications (e.g. list of contacts).


The CNIL’s annual audit program will also take into account this priority related to smartphone ecosystems.

10 tips for smartphone users

1. Do not record confidential information (PINs, access codes, bank account ...) in your smartphone (to avoid risks of theft, hacking, identity theft ...).
2. Do not disable the PIN code and change the operator’s default code. Choose a somewhat “complicated” code. Not your birthday!
3. Set up an autolock time for the phone. In addition to the PIN, it will lock the phone after a while and make it inactive. This prevents any access to data in the phone if lost or stolen.
4. Whenever possible, enable encryption of the phone’s backups on your computer. To this purpose, use the settings of the platform with which you connect the phone. This action will ensure that no one will be able to use your data stored on the computer without the password you set.
5. Install an antivirus or a security program whenever possible ... after getting information about their efficiency.
6. Write down the “IMEI” number of your phone. It can be used to remotely lock your telephone, if lost or stolen
7. Do not download applications from unknown sources. Prefer official platforms.
8. Check to which data an application you’re installing will have access.
9. Read the terms and conditions of service before installing an app. And user’s reviews may also be useful!
10. Adjust the settings in the phone or in geolocation-based applications (Twitter, Foursquare, Plyce ...) to always control when and by whom you want to be geolocated. Disable the GPS or WiFi when no longer using a location-based application.
The CNIL informs you daily
Replies to public enquiries
Data protection officer
THE CNIL INFORMS YOU DAILY

The CNIL is vested with a general mission of public information about the rights granted to individuals under the “Informatique et Libertés” Privacy Act. The Commission conducts public communication initiatives via the press, its web site, a presence on social networks or the provision of educational tools. The CNIL is frequently approached by numerous organizations, firms or institutions to carry out training and awareness sessions about the “Informatique et Libertés” Act, and also participates in symposia, fairs or conferences to inform as well as get informed.

PARTNERSHIP WITH FRANCE INFO

In 2011, the CNIL renewed its partnership agreement with France Info radio, initiated in 2007. The partnership involves a weekly participation in the radio talk show called “Le droit d’info” discussing privacy protection, presented by Karine Duchossois every Friday. This partnership contributes to improving public knowledge about privacy rights and providing advice about enhanced privacy and data protection in daily life. A total of 50 chronicles were broadcast on the radio station over the year, focusing on subjects like video cameras in schools, smartphone-based purchases, cloud computing, facial recognition, comments about employees, phishing, etc.

AWARENESS TO INTERNET BEST PRACTICES

In 2011, in line with its initiatives conducted in previous years with pupils and teachers in primary and secondary schools, the CNIL pursued its commitment to raise the awareness of youngsters about Internet best practices. Thus in June 2011, the Commission entered the world of virtual communities by creating a special operation on Habbo Hotel, the Social Gaming site for 13-18 year olds1. The goal was to approach children and teenagers by addressing them directly via a platform they use every day. The operation involved various activities (video contest, quiz, chat room…) to help youngsters discover

1 http://www.habbo.fr/ Habbo is a Social Gaming site for 13-18 year olds. This is a virtual community where members can chat, meet, visit their apartments, buy items to furnish their apartments, dress their avatars or trade objects. Initially created in Finland in 2000, Habbo is the second largest social network after Facebook. The site exists in 37 countries and has 200 million members worldwide. The average member age is 14.4 ans (78% in 13-18 age group).
With this first-time involvement in a virtual network dedicated to young people, the CNIL has demonstrated its role as a key player in the digital world, and its ability to partner with web enterprises in order to promote a responsible Internet respecting the fundamental values of identity and privacy.

The CNIL then approached secondary school students and their teachers, with a special issue of its newsletter entitled "Le journal des 14-18 ans" devoted to geolocation. Over the past few years, geolocation has boomed, and with the expansion of smartphones, multiple applications have been developing for daily uses. Yet 72% of French smartphone users think that the transmission of the location data in real time via Internet is risky. The CNIL believe that it is crucial for future citizens to be aware of the impacts of geolocation on their privacy.

The newsletter special issue was sent to 20,000 history and geography teachers, often in charge of civic education as well, in 8th grade classes and to the Documentation & Information Centers in junior high-schools across France. It is intended as educational material to help teachers engage into a dialogue with their students about geolocation and related issues: "Mobile-based geolocation: a status assessment"; "What is augmented reality?"; "Geolocation and advertising"; "The right to freedom of movement", etc.

It may prove difficult at times for internet users to find their way through the various account parameter settings. The CNIL decided to demonstrate how to control the personal information posted on social networks in an educational manner. To this purpose, a video tutorial was produced to present how to create lists of friends on Facebook. Facebook enables members to split their contacts into lists of family members, close friends, colleagues, etc. and to set confidentiality parameters based on the type of information to be shared with each category of contacts. The tutorial demonstrates step by step how to create such lists of friends.

80 VIDEO CLIPS WERE PRODUCED DURING THE HABBO CONTEST

video tutorials

With this first-time involvement in a virtual network dedicated to young people, the CNIL has demonstrated its role as a key player in the digital world, and its ability to partner with web enterprises in order to promote a responsible Internet respecting the fundamental values of identity and privacy.

The CNIL then approached secondary school students and their teachers, with a special issue of its newsletter entitled “Le journal des 14-18 ans” devoted to geolocation. Over the past few years, geolocation has boomed, and with the expansion of smartphones, multiple applications have been developing for daily uses. Yet 72% of French smartphone users think that the transmission of the location data in real time via Internet is risky. The CNIL believe that it is crucial for future citizens to be aware of the impacts of geolocation on their privacy.

The newsletter special issue was sent to 20,000 history and geography teachers, often in charge of civic education as well, in 8th grade classes and to the Documentation & Information Centers in junior high-schools across France. It is intended as educational material to help teachers engage into a dialogue with their students about geolocation and related issues: “Mobile-based geolocation: a status assessment”; “What is augmented reality?”; “Geolocation and advertising”; “The right to freedom of movement”, etc.

... VIDEO TUTORIALS ...

It may prove difficult at times for internet users to find their way through the various account parameter settings. The CNIL decided to demonstrate how to control the personal information posted on social networks in an educational manner. To this purpose, a video tutorial was produced to present how to create lists of friends on Facebook. Facebook enables members to split their contacts into lists of family members, close friends, colleagues, etc. and to set confidentiality parameters based on the type of information to be shared with each category of contacts. The tutorial demonstrates step by step how to create such lists of friends.

PUBLICATIONS DEDICATED TO PROFESSIONALS

In 2011, the CNIL published two new guidebooks for professionals.

A practical guide for lawyers was published in the context of the partnership agreement signed with the Conseil National des Barreaux (National Bar Council). This guidebook provides practical answers to questions that lawyers may have regarding the enforcement of the *Informatique et Libertés* Privacy Act, whether as data controller or as legal counsel for their own clients.

It was distributed to the attending lawyers at the National Lawyers Convention in October 2011.

Furthermore, in an era of growing computerization of medical records and dematerialized exchanges of health-related data, the CNIL has published a practical guide for health-care professionals, providing information about measures to be adopted to handle their medical records in compliance with the *Informatique et Libertés* Act. The guidebook also provides advice on how to implement the necessary measures to guarantee the integrity and security of health-care data and ensure full respect for patients’ rights. The document was distributed to all healthcare establishments in the country.

CNIL WEB SITE WWW.CNIL.FR

In 2011, 212 news items were published on the web site. Since January 2011, news updates are also published on the English version on a monthly basis. As of year-end 2011, the Infocnil Newsletter had 36,661 subscribers (versus 33,000 in 2010).

In December 2011 on the occasion of the publication of the opinion survey on “Smartphones and Privacy”, the CNIL launched a mobile-based version of its web site, providing access to all news, practical datasheets and Q&As in an optimized mobile display version.

**New demo on browsing traces**

The web section entitled “Vos Traces” [French only], intended to raise Internet users’ awareness about the issue of browsing traces left behind unbeknownst to them, has existed since the very first release of the CNIL web site. In June 2011, it was entirely revamped and enriched with new demos. Five demos are offered to experiment some of the techniques used by various web players: geolocation via the IP address, cookies and flash cookies, history of sites visited, and targeted advertising.

36,661

SUBSCRIBERS
**SOCIAL NETWORKS**

In 2011, the CNIL reasserted its presence on the social networks Facebook, Twitter, and Dailymotion, and on the professional networks Viadeo and LinkedIn. With 11,600 Twitter followers and 3,223 Facebook fans, the importance of these new communication channels is growing to communicate the Commission’s messages. The CNIL ranks fifth in the Twitter rating of French institutions conducted by the communication agency La Netscouade.

**CNIL’S IMAGE**

Since 2004, the CNIL has been measuring its brand awareness along with the level of information of individuals about their privacy rights. The IFOP survey was conducted this year on a sample of 967 persons representative of the French population aged 18 and over. The survey involved face-to-face interviews at home, carried out from November 23 to 28, 2011.

52% of the interviewees have heard about the CNIL, versus 32% in 2004 and 47% in 2010. The CNIL’s brand awareness went over the 50% mark for the first time this year.

37% of the interviewees have the feeling that they are sufficiently informed of their rights on issues of privacy and personal data protection, versus 21% in 2004 and 34% in 2010.

---


---

**Have you heard about the CNIL, even if only by name?**

<table>
<thead>
<tr>
<th>Year</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>32</td>
<td>68</td>
</tr>
<tr>
<td>2005</td>
<td>37</td>
<td>63</td>
</tr>
<tr>
<td>2006</td>
<td>39</td>
<td>61</td>
</tr>
<tr>
<td>2007</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>2008</td>
<td>53</td>
<td>47</td>
</tr>
<tr>
<td>2009</td>
<td>58</td>
<td>42</td>
</tr>
<tr>
<td>2010</td>
<td>53</td>
<td>47</td>
</tr>
<tr>
<td>2011</td>
<td>52</td>
<td>48</td>
</tr>
</tbody>
</table>

**Do you personally have the feeling that you are sufficiently informed of your rights on issues of privacy and protection of your personal data?**

<table>
<thead>
<tr>
<th>Year</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>21</td>
<td>78</td>
</tr>
<tr>
<td>2005</td>
<td>29</td>
<td>70</td>
</tr>
<tr>
<td>2006</td>
<td>27</td>
<td>72</td>
</tr>
<tr>
<td>2007</td>
<td>26</td>
<td>64</td>
</tr>
<tr>
<td>2008</td>
<td>33</td>
<td>55</td>
</tr>
<tr>
<td>2009</td>
<td>37</td>
<td>62</td>
</tr>
<tr>
<td>2010</td>
<td>34</td>
<td>61</td>
</tr>
<tr>
<td>2011</td>
<td>37</td>
<td>63</td>
</tr>
</tbody>
</table>
Are users satisfied?

- 93% are satisfied with the prior notification procedure, vs. 96% in 2010
- 79% are satisfied with their contact with the CNIL, vs. 87% in 2010

Source: Satisfaction survey conducted by IFOP at end September 2011 with 1,013 users
DATA PROTECTION OFFICER

The year 2011 was particularly fruitful for Data Protection Officer (CIL). The initiatives conducted by the CNIL in their favor may be summed up in four key highlights, or four key words: federate, guide, promote and assess.

Since the August 2004 amendment of the Informatique et Libertés Act, enterprises and administrations can appoint a Data Protection Officer (or CIL, Correspondant Informatique et Libertés). With the introduction of new sanctioning powers and of the CNIL certification label, the CIL correspondent has become a symbol of new instruments created by the French lawmakers to guarantee the efficacy of data protection. The primary duty of the Data Protection Officer is to ensure that the organization who appointed him/her formally to act as correspondent with the CNIL, complies with its obligations under the Informatique et Libertés Act. The CIL also plays a role in counseling and disseminating the Privacy and Data Protection culture with employees, managers and colleagues. As such, the Correspondent is a vector of legal and IT security in his/her organization. The CIL has become a must for any organization concerned about its social responsibility, corporate values, and respect for the rights and liberties of users, customers and employees.

FEDERATE

For the first time since the creation of the function in 2004, the CNIL organized a full-day event dedicated to CIL correspondents on April 8, 2011 at the Palais du Luxembourg in Paris. The primary goal of this event, attended by 200 Correspondents, was to enable feedback and exchanges of views between the CILs and the CNIL regarding the past six years, and to look at the future of the profession together. Two round-table panels were organized to this purpose, one devoted to CIL networks, and the other to the respective roles of CILs and of the CNIL in response to technological innovations. It also provided an opportunity for the French and foreign privacy officers to testify about their experience and their work. Considering the major success of the event and expectations expressed by Correspondents, the CNIL decided to continue this initiative over time and to organize a similar event every two years.

GUIDE

CIL correspondents regularly express their wish for support and guidance from the CNIL regarding communications within their organizations, in order to explain the issues involving the Informatique et Libertés Act and their profession. This recurring need emerged again just before the European Privacy & Data Protection Day organized every January 28 since 2007. Accordingly, the CNIL has produced a “Communication Kit” intended exclusively for data protection officer which was sent to all CILs in December 2011. The kit contains posters, stickers and postcards focusing on the CILs duties and the European event of January 28, along with a brochure on privacy in daily...
This type of initiative should enable the CILs to boost their visibility within their organizations and enable them to raise the awareness of people around them (colleagues, customers, family or friends) to the issue of data protection in an entertaining and interactive way.

**PROMOTE: RECOGNITION OF THE PROFESSION**

Within their organizations, the CILs act as experts on data protection in the context of their mission of regulation and counseling. It was necessary to professionalize the function in view of the specific knowledge in law and information technology required to perform their duties. The function is often a full-time position and the CIL sometimes heads a department with a staff of several persons in charge of ensuring the organization’s compliance with the law. Against this backdrop, the CNIL has requested “Pôle Emploi”, the French national employment agency, to register the profession of CIL in the “Répertoire Opérationnel des Métiers” (ROME – a reference directory listing jobs per professional category).

Following this request, the profession of CIL was introduced into the category “Legal Defense and Counsel” (data sheet K 1903). This functional link to legal professions results from the fact that the very role of the CIL is to ensure compliance with the law. This does not however exclude other professional profiles from fulfilling this function. In practice, many CIL correspondents hold different positions: ethics officer, auditor, IT engineer, quality manager, etc. But such official recognition of the profession by a major player of the national employment policy in France bolsters the role and legitimacy of the CIL.

**ASSESS**

In the context of its annual audit program in 2011, the CNIL decided to assess the efficiency of CIL correspondents. To this purpose, the Commission audited organizations who have appointed a CIL. It also conducted benchmarking audits of organizations having similar business activities, with or without a data protection officer, in order to assess their respective level of compliance with the *Informatique et Libertés* Act. A total of 18 organizations were audited, including 8 in the benchmarking audits (4 with a CIL, and 4 without). This audit campaign yielded an initial status assessment of the CIL profession. Based on the findings, the CNIL also decided to adopt new measures intended to promote the development of the profession, while preventing any potential excesses.

Based on audit results, the CILs were broken down into three categories, depending on the way they accomplish their duties:

- competent CILs, dedicated to their duties,
- CILs fulfilling their duties partially due to lack of time, resources or recognition, and
- CILs appointed as “stalking horses” for the sole purpose of being granted lighter notification procedures or for window dressing.

Thus, it clearly emerged that the efficiency of data protection officer is largely dependent on the means and resources allocated by the organization’s data controller as well as on their personal engagement.

Some audits found that some correspondents and data controllers were not really aware of their obligations. Yet, the appointment of a data protection officer should lead to improvements in the organization’s operation and management of issues related to data protection. In an effort to achieve this goal, the CNIL will intensify its training workshops for CILs, focusing in particular on internal audit procedures and strategies. In addition, the Commission will conduct new audits every year.
Article 11 of the Law of January 6, 1978 as amended confers to the CNIL a duty of adviser to the Government and Parliament. This counseling duty is reflected in the form of “official opinions”.

National Consumer Credit Register

ZOOM

Comments on the bill relative to identity protection
NATIONAL CONSUMER CREDIT REGISTER

The Lagarde Law reforming the consumer credit system¹ created a special Committee in charge of pre-designing the creation of a national consumer credit register. The brief assigned to this Committee was not to decide on the appropriateness of introducing a centralized credit record in France, likely to record information on some 25 million persons, but to investigate the practical conditions of its introduction.

WORK AND REPORT OF THE “PRE-DESIGN COMMITTEE”

The CNIL attended all of the meetings held by the Committee and its working groups. The Committee addressed in particular the issues of identifiers, types of loans, collected data, etc. The CNIL contributed among other to the Committee’s work on compliance with the provisions of the Informatica et Libertés Act (proportionality of data collected, limited retention period, etc.).

The Committee’s report was published in August 2011 and submitted to public enquiry by the Minister of Economy, Finance & Industry until September 15. In the context of this public consultation procedure, the Commission issued an opinion at its plenary assembly on September 8, 2011. In view of the significant stakes inherent to the introduction of a central credit record in France, the Commission, in its capacity as data protection regulator, expressed its views on the principle of such a record per se, and on the use of the registration number in the Répertoire national d’identification des personnes physiques (national registry of social security numbers) as an identifier recommended by the Committee.

Introduction of a central credit record

The CNIL has expressed reservations regarding the relevance of a central credit record to prevent over-indebtedness, a position stated with constancy by the Commission on numerous occasions³. The purpose of such a central credit record is to prevent the risks of over-indebtedness. It is intended to collect information relative to outstanding loans as potential signals of alert on situations of existing over-indebtedness in order to avoid granting “too much credit”. Yet, current situations of over-indebtedness seem to result from cumulative causes, some of

THE CENTRAL CREDIT RECORD WOULD CONCERN 25 million persons

What is a central credit record (“centrale de crédit”)?

A central credit record, also called “positive record” or “credit register” is a file compiling all outstanding loans, i.e. loans granted by banks to private individuals (mortgage loans, consumer loans, etc.). This credit record, accessible to all credit establishments, is intended to help them better assess the solvency of individual borrowers in order to prevent over-indebtedness.

Conversely, the so-called “negative record” contains only loan reimbursement incidents. In France, this record is called the FICP⁴ and currently compiles such data about 2.5 million persons.

¹ Law No.2012-737 of July 1, 2010 / ² FICP: Fichier national des incidents de crédit aux particuliers (national consumer credit incident record) / ³ In particular in its 2001 Annual Report and during hearings by members of Parliament.
which are unpredictable (e.g. increasing energy bills, etc.) or from a deterioration of the borrower’s economic situation further to a “life accident” (unemployment, illness, divorce, etc.), rather than from an abuse of loans. In some cases, particularly in the event of first-time home buying, the very first loan, i.e. the loan leading to the borrower’s recording into the central credit record would already be “one loan too many”.

Furthermore, the Belgian central credit record introduced in 2003 has not had any significant effect to date on over-indebtedness. Following a decline in the number of loan defaults in 2006 and 2007, their number actually started to increase again as of 2008\(^4\), which clearly establishes a link between over-indebtedness and economic situation. Consequently, there are no statistical data that would demonstrate the efficiency of a central credit record in preventing over-indebtedness.

Lastly, a prior study on the effects of the Lagarde Law – which came into force in 2011 only – on over-indebtedness should be conducted.

In any case, the CNIL considers that its comprehensive investigations on the topic have now been finalized since 2007\(^5\) and that “the Legislator alone [is] competent to rule on the social usefulness of creating ‘positive records’ in the credit sector”.

**Use of the Social Security Number (or NIR)**

The “Pre-Design Committee” considered that creating an identifier derived from the social security number (or NIR) was the “sole option enabling a reliable identification within the future Register”. The CNIL has reiterated its reservations regarding the use of the NIR number which should, in its opinion, be restricted strictly to the social sphere. The Commission emphasized potential abuses, due in particular to the risk of interconnection and of purpose diversion of this identifier. It further considers that the use of an NIR-derived identifier should be in last resort only, i.e. if no other solution could be envisaged and provided that the NIR number is subjected to “double hashing” for encryption.

---

\(^4\) Source of data: Banque nationale de Belgique

\(^5\) CNIL Deliberation No.2007-044 of March 8, 2007

---

**INFOS**

**What is “cryptographic hashing”?**

A hash function is an algorithm that generates a digital fingerprint from a set of data, in the form of a chain of non-significant characters, making it impossible to retrieve the original data. In addition, it is very unlikely that two distinct sets of data will generate the same digital fingerprint.

---

**The Legislator alone [is] competent to rule on the social usefulness of creating ‘positive records’ in the credit sector**
On the occasion of the parliamentary debates on the Bill No.682 relative to identity protection submitted to the Senate on July 27, 2010 (now adopted as Law No.2012-410 of March 27, 2012), the CNIL felt it necessary, in accordance with its general remit of counseling and information provided by Article 11 of the Law of January 6, 1978 as amended, to publish its analysis on the subject in the form of a Commentary Memo dated October 25, 2011.

Since the early 2000s, several projects for biometric and electronic ID cards have emerged. The Interior Ministry thus referred three draft bills to the CNIL for review: the bills entitled “Titre fondateur” and “INES” which were abandoned, and the bill entitled “Protection de l’identité” (Identity Protection) which was the subject of the CNIL Deliberation No.2008-306 issued on July 17, 2008, not published officially.

The CNIL has expressed itself on multiple occasions about projects of biometric processing implemented to deliver identity or travel documents, in particular in its Opinion issued on December 11, 2007 about biometric passports. The Interior Ministry and the national agency in charge of secured ID documents (ANTS, or Agence nationale des titres sécurisés) are implementing a personal data processing system called TES, to handle the establishment, issuance, renewal and retrieval of passports, and the procedures designed to prevent...
**What is the proposed digital ID card?**

The digital identity card, as planned under the Bill, was a physical ID card with two secure electronic chips added. The first chip would certify the cardholder’s identity and contain identification elements: first and last names, gender, birth date and birthplace, domicile, height, eye color, fingerprints and photograph. The second optional chip would enable the cardholder to be authenticated on electronic communications networks and to create an electronic signature that could be used for on-line administrative formalities and e-commerce.

Zoom on the biometric passport

The biometric passport was authorized by Decree No.2008-426 of April 30, 2008 adopted further to the CNIL’s opinion on the subject. The system relies on an electronic chip added to passports, containing biometric data (photograph and two fingerprints) and on the creation of a centralized database. The sole purpose of this data processing is to secure the issuance of passports and to fight identity fraud.

To this end, the Interior Ministry has adopted an organization limiting possibilities of querying the biometric database: the civil registry database was split from the biometric database. This segregation is secured by creating a single identifier number preventing the name from being found based on this number alone. Thus, it is possible to find the corresponding biometric data from a name, e.g. to verify the identity of the passport owner in case of loss or theft; however, it is not possible to identify a person from their fingerprints alone.

and detect counterfeiting or forgery. This process is in line with the European efforts to secure and integrate biometrics into passports and travel documents (Council Regulation No.2252/2004).

The Bill refers largely to the system implemented for biometric passports. It provides for the issuance of biometric ID cards (equipped with a chip containing two fingerprints among other) and the creation of a database containing all the data required to deliver the document to the applicant, and in particular a set of eight fingerprints.

The system was however significantly enlarged, firstly with a second chip enabling new services like authentication and electronic signature. But most of all, the Bill plans for the creation of a database common to both ID card and passport applicants, and enables persons to be identified from their fingerprints.

For these reasons, the planned system is unprecedented in France. The centralized record would actually have the ability to retain the civil status data and biometric data of all French citizens, including minors, who ever applied for an identity document. Very few European countries currently have such a centralized database, but none of them retain sets of eight fingerprints, as planned in the initial Bill.
<table>
<thead>
<tr>
<th>Country</th>
<th>Electronic ID card</th>
<th>Biometric ID card</th>
<th>Chip</th>
<th>Database</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Photo</td>
<td>Fingerprint (number of digits)</td>
<td>Centralized Photo Fingerprint (number of digits)</td>
</tr>
<tr>
<td>Germany</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>[At citizen's request: 2] NO</td>
<td>NO NO NO</td>
</tr>
<tr>
<td>Austria</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES YES NO</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyprus</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>No ID card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>[1]</td>
<td>YES YES [2] Same data base as passport. ID card is a prerequisite for passport</td>
</tr>
<tr>
<td>Estonia</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td>Chip used only for authentication and signature</td>
</tr>
<tr>
<td>Finland</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td>Chip used only for authentication and signature</td>
</tr>
<tr>
<td>Greece</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>No ID card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>No ID card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>[min 2, max 3]</td>
<td>NO YES Suspended Decentralized database</td>
</tr>
<tr>
<td>Poland</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>[2]</td>
<td>YES YES</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roumania</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td>Planned</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>ID card launched in 2006, but interrupted since May 2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovakia</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovenia</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>[?]</td>
<td>NO NO NO Little used</td>
</tr>
</tbody>
</table>

[1-2] Electronic ID cards across the EU, November 2011
Because  /  Consult and innovate  /  Protect and inspect  /  Sanction  /  Topics of investigation in 2012  /  Appendices

POSITION OF THE CNIL

Under the circumstances, the CNIL felt it necessary to publish its analysis on the subject in a Commentary Memo adopted at its plenary assembly on October 25, 2011.

Firstly, the Commission issued a reminder that biometric data are not personal data “just like others”. They enable an individual to be identified based on biological facts, produced by that person’s body. The CNIL has always paid special attention to these data, particularly those called “traceable” such as fingerprints or facial features which may be captured and used unbeknownst to the individual concerned. Consequently, this characteristic of biometric data increases the level of requirements as regards their use.

With respect to the issuance of biometric identification documents, the Commission reiterated its ongoing position, namely that the introduction of an electronic component containing biometric data into identity and travel documents has to be proportionate with the need to bolster the security of the document issuance and verification procedures. It however expressed its wish for additional guarantees to be provided regarding in particular the minimum age to collect biometric identifiers or the technical security systems relative to electronic components.

Regarding the creation of the biometric database, the CNIL noted firstly that some anti-fraud solutions appear to be just as efficient and more respectful of individual privacy, apart from compiling such a database. Such is the case for instance of the procedure to verify civil status details capable of securing the “source documents” to be presented for the issuance of ID documents, which the Commission has recommended for implementation on numerous occasions since 1986. Under the circumstances, the Commission considered that the proportionality of biometric data retention against the legitimate goal of fighting document fraud had not been demonstrated.

Furthermore, the Commission stated that measures should be adopted to ensure that the data processing would not be used for any purposes other than the issuance of identity and travel document and fighting against identity fraud. It thus recommended the prohibition of any interconnection of the records with any other personal data processing operation, and to ensure, via any necessary technical and legal means, that the system would not be misused for purposes other than for its original purpose, and in particular for any police purposes. The CNIL cited for instance the option of limiting the number of fingerprints recorded in the central database, or the absence of any univocal link between the biometric data recorded in the central base and the civil registry data (so-called “weak link” technique, see below).

Weak link or strong link: what is it?

The “strong link” method is used to identify a person based on biometric data. Thus a set of fingerprints in the central database can identify the corresponding person, and vice versa. It is therefore possible to build a match table between civil registry data and biometric data. This method is used to produce biometric passports.

Conversely, the “weak link” method is an innovative identification technique making it impossible to identify a person from a set of fingerprints. The individual is not matched to any number that would refer to their identity, but to a data group containing the fingerprints of several persons. Querying the database will only yield a group number, thereby thwarting any fraud attempt without revealing the identity of the fingerprints owner.

While the CNIL did not issue an explicit opinion on this technique, it considered however that the “weak link” method would ensure that the centralized database cannot be used for purposes other than its initial goal, and particularly not for any identification of individuals by police or judiciary authorities.

Description of the architecture of a “weak link” centralized database

<table>
<thead>
<tr>
<th>Civil Registry database</th>
<th>Biometric database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual A</td>
<td>Group No.1234</td>
</tr>
<tr>
<td>Group No. 1234</td>
<td>Biometric data A</td>
</tr>
<tr>
<td>Individual B</td>
<td>Group No. 4567</td>
</tr>
<tr>
<td>Group No.4567</td>
<td>Biometric data B</td>
</tr>
<tr>
<td>Individual C</td>
<td>Group No. 1234</td>
</tr>
<tr>
<td>Group No.1234</td>
<td>Biometric data C</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
</tbody>
</table>

The “strong link” method is used to identify a person based on biometric data. Thus a set of fingerprints in the central database can identify the corresponding person, and vice versa. It is therefore possible to build a match table between civil registry data and biometric data. This method is used to produce biometric passports.

Conversely, the “weak link” method is an innovative identification technique making it impossible to identify a person from a set of fingerprints. The individual is not matched to any number that would refer to their identity, but to a data group containing the fingerprints of several persons. Querying the database will only yield a group number, thereby thwarting any fraud attempt without revealing the identity of the fingerprints owner.

While the CNIL did not issue an explicit opinion on this technique, it considered however that the “weak link” method would ensure that the centralized database cannot be used for purposes other than its initial goal, and particularly not for any identification of individuals by police or judiciary authorities.

```
weak link or strong link: what is it?

The “strong link” method is used to identify a person based on biometric data. Thus a set of fingerprints in the central database can identify the corresponding person, and vice versa. It is therefore possible to build a match table between civil registry data and biometric data. This method is used to produce biometric passports.

Conversely, the “weak link” method is an innovative identification technique making it impossible to identify a person from a set of fingerprints. The individual is not matched to any number that would refer to their identity, but to a data group containing the fingerprints of several persons. Querying the database will only yield a group number, thereby thwarting any fraud attempt without revealing the identity of the fingerprints owner.

While the CNIL did not issue an explicit opinion on this technique, it considered however that the “weak link” method would ensure that the centralized database cannot be used for purposes other than its initial goal, and particularly not for any identification of individuals by police or judiciary authorities.

Description of the architecture of a “weak link” centralized database

<table>
<thead>
<tr>
<th>Civil Registry database</th>
<th>Biometric database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual A</td>
<td>Group No.1234</td>
</tr>
<tr>
<td>Group No. 1234</td>
<td>Biometric data A</td>
</tr>
<tr>
<td>Individual B</td>
<td>Group No. 4567</td>
</tr>
<tr>
<td>Group No.4567</td>
<td>Biometric data B</td>
</tr>
<tr>
<td>Individual C</td>
<td>Group No. 1234</td>
</tr>
<tr>
<td>Group No.1234</td>
<td>Biometric data C</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
</tbody>
</table>
```

The “strong link” method is used to identify a person based on biometric data. Thus a set of fingerprints in the central database can identify the corresponding person, and vice versa. It is therefore possible to build a match table between civil registry data and biometric data. This method is used to produce biometric passports.

Conversely, the “weak link” method is an innovative identification technique making it impossible to identify a person from a set of fingerprints. The individual is not matched to any number that would refer to their identity, but to a data group containing the fingerprints of several persons. Querying the database will only yield a group number, thereby thwarting any fraud attempt without revealing the identity of the fingerprints owner.

While the CNIL did not issue an explicit opinion on this technique, it considered however that the “weak link” method would ensure that the centralized database cannot be used for purposes other than its initial goal, and particularly not for any identification of individuals by police or judiciary authorities.

Description of the architecture of a “weak link” centralized database

<table>
<thead>
<tr>
<th>Civil Registry database</th>
<th>Biometric database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual A</td>
<td>Group No.1234</td>
</tr>
<tr>
<td>Group No. 1234</td>
<td>Biometric data A</td>
</tr>
<tr>
<td>Individual B</td>
<td>Group No. 4567</td>
</tr>
<tr>
<td>Group No.4567</td>
<td>Biometric data B</td>
</tr>
<tr>
<td>Individual C</td>
<td>Group No. 1234</td>
</tr>
<tr>
<td>Group No.1234</td>
<td>Biometric data C</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
<tr>
<td></td>
<td>Etc...</td>
</tr>
</tbody>
</table>
In addition, the Commission commented on the possibility of implementing facial recognition devices, as planned under the Bill. In a context where video-surveillance systems are multiplying, and as related to their interconnection and interoperability, the **CNIL expressed its utmost reservations as regards the possibility of using such functions.**

Lastly, the Commission wished for an enhanced framework to regulate the new electronic functionalities of the ID card (signature and on-line authentication), further noting that the Bill did provide for significant guarantees (in particular the optional nature of the activation and use of these functionalities).

In order to guarantee that these functionalities would not allow for the creation of a single identifier, or worse yet the compilation of public information about citizens’ actions, the **CNIL suggested some additional regulatory measures:** implementation of mechanisms of “partial disclosure” limiting the transmission of data strictly to the information necessary to perform the service, clear information measures prior to any data transmission, or technical measures likely to guarantee communication security.

The CNIL was invited to speak at numerous hearings before the Parliament regarding this Bill. The Government modified some of the Bill’s provisions further to these hearings, and following the publication of the CNIL’s commentary memo. In particular, a clause was introduced into the text prohibiting the use of facial recognition devices; fingerprints recording in the central database was restricted to two digits only, and the purposes of this data processing were further detailed.

However, other guarantees requested by the CNIL were not all introduced into the Bill. Among other, the principle of retention in the centralized base of biometric data related to the entire French population was kept in the text. In addition, the possibility of using biometric identification functionalities was not restricted to the issuance of identity and travel documents alone: by providing for their use for judiciary purposes – albeit limited to situations related to fighting identity fraud – the Bill potentially opens the way to a gradual enlargement of cases where the database could be used, as evidenced by the recent FNAEG example.

As a consequence, a number of senators and members of Parliament referred the Identity Protection Law adopted by the Assemblée Nationale on March 6, 2012 to the Constitutional Court (Conseil Constitutionnel) for review, in an effort to prevent this risk.

The Law No. 2012-410 relative to Identity Protection was published on March 27, 2012 in a version amended in accordance with the ruling of the Constitutional Court. The electronic chip in the digital ID card will thus contain only the first and last names, gender, birth date and birth place, domicile, height, eye color, two fingerprints and a photograph.

The CNIL will keep close attention to the future fate of his law, and will in particular review a draft Decree from the Council of State (Conseil d’Etat, or Supreme Administrative Court) intended to define its enforcement conditions.

In accordance with its competence under Article 11 of the Informatique et Libertés Act, the CNIL has thus played its role of adviser to public authorities, by proposing adjustments conducive to protect individual liberties, the right to privacy and the processed biometric data.
In pursuance of Article 24 of the Law of January 6, 1978 as amended, the CNIL drafts and publishes standards designed to simplify the obligation of notification, after reviewing as needed any proposals made by representative organizations.
In its Decree of 8 December 2009, the Social Chamber of the Cour de Cassation (French Supreme Court of Appeal) highlighted some difficulties in the interpretation of a number of provisions of the Single Authorization No.AU-004, in particular as related to its scope of application.

Consequently, the Commission found it necessary to clarify its Single Authorization, in view of the organizations’ legitimate aspiration for more legal security. Before doing so, it conducted new audits of the main stakeholders affected by whistleblowing mechanisms, in an effort to determine to what extent it was appropriate to modify the terms of the Single Authorization.

In 2005, the scope of application of the Single Authorization was as follows: accounting, finance, banking, anti-competition practices, and anti-corruption. This Single Authorization allowed for a simplification of procedures for companies subject to the obligations of the Sarbanes-Oxley Act (SOX) requiring listed companies to bolster their internal control via the adoption of whistleblowing mechanisms. A total of 2109 organizations have now used it to notify their ethical alert processing systems.

"Necessary clarification to provide for enhanced legal security”
What is an “ethical business alert”?*

A whistleblowing procedure (or “ethical business alert” in France) is a mechanism enabling employees to report breaches of business ethics they have witnessed, i.e. ethical problems likely to seriously jeopardize the business of the company or to give rise to issues of corporate liability. It may involve for instance a special telephone “ethical hot line” or a dedicated e-mail address. The reports (or “alerts”) thus collected are then verified confidentially by the company, following which the employer can decide which remedies are appropriate in the circumstances.

Some of these mechanisms may involve the automated processing of personal data which, due to their extent, may be liable to lead to the dismissal of individuals and termination of their employment contract. Accordingly, such data processing systems fall under the scope of application of Article 25-I 4° of the Informatique et Libertés Act, and as such, must be authorized by the CNIL.

In the context of its authorization powers, the CNIL ensures that the whistleblowing mechanisms implemented will not foster a generalized system of denunciation via the collection and processing of anonymous reports. In addition, the Commission has always stressed that these mechanisms should be used only as a complement to traditional alert reporting systems (management line, personnel representatives, labor inspectorate, etc.) and should be intended only to address cases where traditional mechanisms have failed.

---

**Key figures**

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>Total since 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of notifications of compliance with AU-04 in 2011</td>
<td>357</td>
<td>2,109</td>
</tr>
<tr>
<td>Specific authorizations (approved)</td>
<td>19</td>
<td>134</td>
</tr>
<tr>
<td>Specific authorizations (rejected)</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

* to 24/02/12

---

**THE NEW SINGLE AUTHORIZATION AU-04**

**Anti-competition practices are now included within the scope of application of the AU-04 authorization.** This change was decided further to several rulings from the Competition Authority enjoining the sanctioned organizations to prevent any breach of competition law by implementing an ethical alert mechanism accessible to their entire personnel.

The intent was also to include into the AU-04 the Japanese “Financial Instrument and Exchange Act” of June 6, 2006, also called “Japanese SOX” since it is closely inspired by the American SOX Act.

Organizations had until June 2011 to become compliant with the new Single Authorization or to file an application for a Specific Authorization, backed by substantiated and motivated reasons why their mechanism failed to comply with the framework specified in the AU-04.

**Non AU-04 compliant mechanisms**

The CNIL has noted a sharp increase in the number of authorization requests on whistleblowing systems failing to comply with the AU-04. In 2011 alone, the Commission reviewed some thirty such cases.

The CNIL staff receive numerous enquiries every day from companies and lawyers regarding the conditions of authorization on these processing operations.

In France, the goals of some ethical alert procedures are far remote from the framework specified in the AU-04 Authorization or covered under the SOX Act. The main discrepancies occur in the scope of application (which exceeds the strict financial scope) and in the legal foundation (mechanisms implemented outside the scope of any regulatory or statutory obligations).

When the scope of application is broader than specified in Article 1 of the Single Authorization, the company must list in detail the domains covered under the scope. The selection of each domain must be duly motivated, due to the serious nature of potential whistleblowing alerts and their related consequences for a company in terms of criminal penalties, image or business continuity.

The Commission reviews on a case per case basis the proportionality of the scope of application of each ethical alert mechanism.

In 2011, the CNIL granted 19 Specific Authorizations and rejected one.

The rejection was grounded on several breaches of the Informatique et Libertés Act and non-compliance with the CNIL’s rules on ethical business alerts (excessively broad scope, incomplete information to individuals, encouraged anonymity, etc.).

In this case, the CNIL found that employees could report about all issues concerning non-compliance with laws or regulations, as well as any behaviors conflicting with the principles of the corporate code of conduct. In addition, the anonymous use of the company’s whistleblowing system was presented as the normal way of reporting alerts.
Numerous actions are launched by companies and public authorities to promote diversity, particularly in the labor market, and fight against discriminations.

Some employers have set up computerized alert systems to prevent and identify cases of discrimination at the workplace. To this purpose, they make available to their employees a dedicated complaint channel managed by staff trained on discrimination issues. Employers are thereby hoping to overcome any inhibition an employee may have about reporting such sensitive and personal issues as discrimination.

According to the Defender of Rights (formerly known as HALDE), self-censorship tends to prevail among employees on these issues, particularly since the traditional reporting channels are not always very efficient. Lack of support or attention from the management is most frequently mentioned in such situations. In addition, since some cases of discrimination affect intimate life or privacy, employees find it difficult to talk to their line manager or personnel representatives (sexual orientation, health problems, philosophical opinions, etc.). Such mechanisms are not covered under the scope of the AU-04 and a specific authorization is required. For the first time on March 3, 2011, the Commission authorized two companies to implement an ethical business alert system dedicated to complaints and claims about discrimination topics. Since then, five more companies have been granted a specific authorization.

The Commission has authorized ethical alert systems dedicated to fight discrimination after verifying that proper guarantees were incorporated, in particular:
- the obligation for whistleblowers to identify themselves (no anonymous reports);
- information to the personnel about the purposes of the mechanism, the persons authorized to deal with reports, and their right of data access and rectification;
- the optional and complementary nature of the mechanism (no obligation for employees to use it);
- confidential treatment of the identity of the whistleblower;
- limited data retention period;
- security measures (confidentiality of data and traceability of access).

The CNIL issued a reminder that such whistleblowing tools should remain optional and complementary to other systems. It is essential to afford priority to the management line and legal channels for reporting purposes, in particular via the personnel representatives.

Lastly, the CNIL paid close attention to the information delivered to the organizations’ personnel representatives. In some companies, a collective bargaining agreement addressing non-discrimination among other has been signed jointly with trade unions, attesting to the strong engagement of both employers and employees on this issue. The implementation of these mechanisms thus does not result merely from a unilateral decision by the employer.

What is the “UK Bribery Act”?  
The UK Bribery Act came into force on July 1, 2011, and requires all companies doing business in the United Kingdom to implement appropriate internal procedures designed to prevent bribery of any business partners, with offenses subject to heavy criminal penalties.
5.

CONSULT AND INNOVATE

WiFi, iPhone and geolocation

ZOOM
Consultation on
Cloud Computing
WIFI, iPhone AND GEOLOCATION

Although geopositioning is often associated with GPS technology, most smartphones frequently use an entirely different location technique based on the detection of WiFi hot spots.

What are the privacy risks raised by this technology? In an attempt to reply to this question, the CNIL lab experts have kept an iPhone 3Gs under surveillance to analyze its communications and observe the geolocation data transmitted to the device manufacturer.

REQUEST FOR GEOLOCATION

Whenever an iPhone user requests geopositioning via for instance the “Boussole” or “Maps” applications, the device queries the Apple geolocation server. To do so, it sends to Apple a short list of some WiFi access points (or hot spots) detected in its surroundings. The Apple server then replies with a list of the locations of several hundreds of WiFi hot spots found around the phone. The iPhone itself then calculates its own position based on the data supplied on line.

YOUR IPhone “CHATS” WHILE YOU SLEEP...

The iPhone surveillance yielded some surprises: at night, the iPhone also contacts Apple’s geolocation servers at regular intervals, without any intervention from the user. To this purpose, the device sends to Apple geolocation data on the position of the WiFi hot spots that it has detected in the previous days or hours.

It appears that Apple servers are populating and updating their WiFi geopositioning database by exploiting iPhones whenever their owners are not using it. This type of approach can raise concerns for the privacy of individuals, yet an analysis of data exchanges has shown that the specific phone is not identified, which is reassuring.

TOWARDS OTHER TYPES OF CHATTERING?

Smartphones are personal objects which communicate with the networks on an ongoing basis. Even if the manufacturer of your iPhone is not “tracking” you, what about the multiple applications you have installed and what about your personal data? Replying to this question will be a huge challenge for data protection authorities in the coming years.

INFO +

WiFi geolocation: how does it work?

Most Internet modems are equipped with a WiFi access point that emits signals continuously. These signals contain a single identifier number called MAC address (or BSSID) specific to each WiFi hot spot. Based on a map of WiFi hot spots identified via their MAC address, some service providers like Apple or Google offer a WiFi geopositioning tool: by analyzing the MAC addresses of the WiFi hot spots detected by the phone, the position of the phone itself can then be calculated.
or enterprises, the related business model is similar to leasing IT resources generally billed according to actual consumption. The range of cloud service offers has boomed over the past three years, in particular with on-line storage and publication of documents, or with the social networks for instance, leading some to believe that “tomorrow, the place where we'll store our data and run our applications will no longer be our PC... but a nebula of IT mega-centers scattered all over the planet”1.

**THE CLOUD: A PROTEAN CONCEPT**

Based on the NIST definition (National Institute for Standards and Technologies), the Cloud Computing model can be defined in terms of five key characteristics:

- **Simplicity of on-demand self-service**: A user can unilaterally provision computing capabilities (server time, storage capacity) as needed, automatically, immediately and generally without any human interaction with each service provider. The complexity of IT resource management disappears since issues of design, administration or maintenance are also migrated to the provider.

- **Extreme flexibility**: The resources provided have a high and fast capability of adjustment to any upscaling demand, in a generally transparent way for the user. This adaptability and extensibility of resources may often appear unlimited to the user.

- **“Light” access**: Access to resources requires no proprietary or dedicated hard-

---

1 Excerpt from the article “Vers la fin de l’ère du PC – Microsoft dans le piège Internet” by Dominique Nora, Nouvel Observateur correspondent in San Francisco, May 1, 2008.
ware or software. Capabilities are available via readily available (and sometimes free) applications, generally from a simple Internet browser. Access is thus possible from virtually any type of device with network access (desktop or laptop computer, PDA, mobile phone, etc.), almost independently of their capacities, configuration or operating system.

Resource pooling: The provider’s computing resources are pooled to serve multiple users and machines, and are frequently spread out in different hosting centers (possibly in various places around the planet). Physical and virtual resources are dynamically assigned and reassigned according to consumer demand, and it may be difficult if not impossible to know where the data are physically stored at any given time (or where they are processed).

Pay-per-use: As a general rule, payment for Cloud Computing services is proportional to their use, even when payment takes place indirectly via advertising for instance. The client pays according to the applications, computing time, use time, or storage capacity provided.

In addition, the NIST definition of Cloud Computing includes three service models and four deployment models.

Three service models correspond to the various types of services provided in the Cloud:
- Provision of infrastructure (for computing, storage, etc.): *Infrastructure as a Service*, or “IaaS”. These services are evolutions of conventional hosting services upgraded to the Cloud model.
- On-line applications: *Software as a Service*, or “SaaS”. This type of service provision is the most widespread and best known form of Cloud Computing (Google Apps, Salesforce, etc.).
- On-line development platforms: *Platform as a Service*, or “PaaS”. These services, designed for application suppliers, provide the necessary tools to develop an application that can then be offered as SaaS to the end client.

The deployment models depend on the level of infrastructure pooling:
- The *private cloud* is a client-dedicated infrastructure. Whenever the infrastructure is shared by several clients with similar interests, the term of “Community Cloud” is also used.
- Conversely, the *public cloud* is a pooled among all clients of a single service provider. In this case, the end user generally has no way of knowing which other users are present on the server, network or hard disk where the tasks are performed.
- Lastly, the *hybrid cloud* consists in two or more Cloud entities of distinct nature, and provides for mechanisms of data transfers between these entities.

The cloud computing market potential is gigantic and strategic for all enterprises using IT services. So much so that the European Commission has adopted it as a priority pillar of its *Digital Agenda*, in particular to help European SMEs leverage as much value as possible from cloud computing. For small and medium size enterprises, the Cloud is presented as an opportunity for significant cost cutting while guaranteeing a high service level. Furthermore, the intrinsic elasticity of the Cloud can support corporate growth and enable the companies to better control the fluctuations of their business activity.

However, many companies have fears regarding the legal and technical implications of switching to the Cloud, first and foremost the concern about data confidentiality.
**DEVELOPMENT OF CLOUD COMPUTING: A CHALLENGE FOR PERSONAL DATA**

From the users’ standpoint, Cloud Computing is characterized by a simplified management of IT services and resources (upscaling in one click, pay-per-use, etc.). For the service provider, Cloud Computing constitutes a genuine upgrade in service outsourcing, based on multiple servers spread out in multiple geographic locations anywhere across the world. It provides for a full dematerialization of resources that are accessible from any place and at any time.

The physical location of data and the determination of applicable jurisdictions have however become major issues. Since the data may be transferred to different servers that may be physically located anywhere on the planet, it is therefore difficult to regulate them efficiently, particularly since clients themselves cannot identify beforehand on which servers their data will be stored.

Under the circumstances, it may prove complicated for data subjects to exercise their rights. To which jurisdiction should the data subjects turn to enforce their rights? How to ensure that data subjects are entitled to their right of access when their data are stored in a server located on the other side of the world? How to check that data are really deleted when they have previously been saved and stored in multiple servers?

Furthermore, in order to optimize the allocation of resources among the various storage centers, personal data are transferred and exchanged continuously between the client and the provider. The client’s IT system management is sometimes fully entrusted to the provider, therefore transferring the risks to the latter. In some cases, it may happen that the client uses the Cloud Computing services of a provider who in turn sources services from another provider, for its infrastructure for instance. Determining the roles of the various players and identifying their respective qualifications may then prove extremely complex, particularly since the public addressed by Cloud Computing offers is highly diversified: from small businesses to multinationals, along with private users.

Lastly, in view of the multiple storage places and of the permanent accessibility to data, the security provided by Cloud Computing is a major issue.

Against this backdrop, the CNIL intends to adopt a position on the topic in order to clarify the legal and technical frame of regulation for Cloud Computing. The Commission wishes among other to identify the risks linked to switching to the Cloud, and to develop recommendations to clients and providers. Considering the importance of this issue, and before publishing its recommendations, the CNIL launched a public consultation procedure from October to December 2011 designed to collect the opinions of Cloud stakeholders on the issue of personal data protection and security in the Cloud.

**PROPOSALS AND CONSULTATION TO CLARIFY THE ISSUE OF DATA PROTECTION IN THE CLOUD**

The CNIL’s consultation procedure was intended to obtain feedback on practical proposals relative to the various aspects of personal data protection in the Cloud.

**Qualification of parties**

Under the terms of Article 3 of the Informatique et Libertés Act, the data controller is defined as the physical or moral entity who determines the purposes and resources of the personal data processing. The processor processes the personal data on behalf of and according to the instructions of the data controller (Article 35 of the Informatique et Libertés Act).

The CNIL proposed the following analysis:

- The Client is necessarily responsible for the processing since he/she determines the purposes and resources for the data processing operation, and is thus regarded as the data controller;
• The Provider is presumed to be the subcontracted processor, unless this presumption is ruled out by a number of indications showing that the provider also acts as data controller.

In the context of the ongoing discussions on the revision of EU Directive 95/46/EC, the CNIL has proposed the creation of a legal status for the Processor, to ensure that processors are bound by a number of specific obligations.

**Applicable Law**

Since Cloud Computing relies on the use of multiple servers located in various places in the world, this leads to obvious difficulties in determining which law is applicable. The flexibility and fluidity of data transfers mean that as many legal regimes might be potentially applicable as there are countries where the data processing servers are located. Yet it is particularly important to identify which law is applicable, among other to determine which obligations are legally binding on the data controller.

**Under the terms of Article 5 of the Informatique et Libertés Act**, the law is applicable if the data controller:

- is physically located on the French territory, or
- uses processing resources located on the French territory (and not established on the territory of another Member State).

Although the CNIL favors a broad interpretation of the concept of processing resources, it nevertheless questioned Cloud stakeholders about the criteria to be taken into consideration when determining which law is applicable.

**Regulating data transfers**

Under the terms of Article 68 of the Informatique et Libertés Act, personal data may be transferred only if the Member State where the data recipient is located provides an adequate level of protection. Article 69 of the law provides expressly for instruments to regulate this type of transfers: standard contract clauses, internal corporate rules (or BCR, Binding Corporate Rules), Safe Harbor or waivers.

However, using such instruments implies knowing in which country (or countries) the data will be processed, information essential to comply with the CNIL notification/authorization process and to inform the data subjects about such transfers to these countries.

Yet, Cloud Computing is more frequently based on the lack of any stable physical location for the data. The client is therefore rarely in a position to know where the data are located or where they have been transferred and stored. In a context where potential places for data storage are multiplying, the legal instruments intended to regulate the above-described data transfers have reached their limits. In an attempt to resolve this difficulty, the CNIL has asked service providers whether they would be prepared to incorporate standard clauses into their service provision contracts, and has invited all Cloud stakeholders to investigate the feasibility of introducing BCRs for the processors.

Such “Processor BCRs” would enable a client to entrust a processing subcontractor with its data, with the assurance that the data transferred within the processing company are afforded an adequate level of protection.

**Data security**

Whenever an organization uses Cloud Computing services, the management of data security is largely delegated to the provider from whom it often proves difficult to obtain any guarantees on the actual security level. In pursuance of Article 35 of the 1978 Act as amended, the processor “shall offer adequate guarantees to ensure the implementation of the security and confidentiality measures” for which the data controller is responsible; while the data controller has the “obligation to supervise the observance of such measures of security and confidentiality”.

The CNIL considers that security requirements should be materialized in a contract in order to clearly assign the roles and responsibilities of the parties. Among other, such a contract addresses efficiently any incidents liable to lead to the loss or disclosure of data. However, many Cloud offers are based on standard agreements that cannot be negotiated by the client. In order to inventory the players’ practices, the Commission has asked them for their opinions regarding contractual relationships between client and provider.

---

1 As proposed in the Report relative to “Questions raised about personal data protection by processing operations outsourced outside the European Union”, http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/20100909-externalisation.pdf
many service offers, including from large
companies, “administration”-type events
enabling the creation/deletion of accounts
or access to data are not logged); •
Access control: for instance, the
account of staff members who left the
organization must be immediately deac-
tivated, since they could still access the IT
systems even though they are no longer
physically present on the premises;
• Authentication: similarly, the authen-
tication process must be strengthened.
Using a strong authentication process is
necessary whenever the accessed data
are sensitive and/or voluminous.

The CNIL stresses the importance of
encryption as the only way to prevent the
providers’ IT administrators to access the
data entrusted to them. The parties were
therefore invited to express their views
regarding the opportunity of the proposed
measures on Cloud Computing, and in
particular on the topic of encryption.

While this public consultation was
the first ever organized by the CNIL, the
numerous replies (49) demonstrate that
the sector is indeed anxiously awaiting
the CNIL’s position on the subject. The
Commission will publish the findings
from this consultation procedure in 2012,
along with its recommendations on meas-
ures to be adopted for the protection of
personal data when switching to Cloud
Computing. Concurrently, the CNIL will
continue to coordinate its joint action with
its European peers and with the European
Commission, in view of the inherently
international nature of issues related
to Cloud Computing. The G29 group of
European data protection authorities is
currently preparing an opinion for later
publication.

In agreement with the recommenda-
tions of ENISA (the European Network
and Information Security Agency), the
CNIL advises data controllers to conduct a
risk analysis whenever they intend to
use Cloud Computing services, in order
to assess the impact of this switch on
their information systems. This proce-
dure is still not very widespread, but it
is an efficient way to evaluate precisely
the cost/benefit balance of a project. The
CNIL has asked contributors to share their
comments about this recommendation.

As regards practical security meas-
ures, the CNIL stresses the importance of
some security aspects:
• External protection of the network: fire-
wall, proxy server with content analysis,
intrusion detection, etc.;
• Terminal protection (desktop, laptop,
PDA, mobile phone): antivirus, operating
system and software regularly updated,
firewall;
• Encrypted links2: to guarantee the con-
fidentiality of exchanges;
• Traceability: retain a log of connections
and operations carried out on the data (in
subscribing to a Cloud Computing service. In
addition, the CNIL has identified a need
for new security standards encompassing
the issue of personal data protection in
the Cloud, in order to bolster transparency
for the clients. The CNIL has thus invited
Cloud players to express their views on
these topics.

While this public consultation was
the first ever organized by the CNIL, the
numerous replies (49) demonstrate that
the sector is indeed anxiously awaiting

2 E.g. using https (Hypertext Transfer Protocol Secure) to secure browsing
6. PROTECT AND INSPECT

- Record number of complaints
- Right of indirect access
- Audits
In continuation of the increase previously noted in 2010, another sharp increase in the number of complaints filed with the CNIL was observed in 2011. With a total of 5,738 complaints filed, a new record was achieved last year!

The numbers attest to the undeniable and growing interest of individuals for the protection of their personal data and their growing awareness on this issue.

Similarly to 2010, while all sectors experienced this activity growth, issues related to the “right to oblivion on Internet” grew 42% from 2010 to 2011 (requests for the deletion of contents – texts, photos, videos – displayed on web sites or blogs) and to video-surveillance by 30% from 2010 to 2011. The CNIL also keeps receiving a large number of complaints related to the banking and credit sector, to labor issues (in particular video-surveillance of employees) or to retail businesses (customer files, unsolicited advertising, etc.).

The new on-line complaint section, easily accessible on the CNIL web site at www.cnil.fr, also explains the significant increase in the number of complaints filed: 26% of the complainants filed their complaints on line in 2011 while they were only 8% to do so in 2010.

The investigation time may vary from a few days to several months depending on the complexity of the complaint, on the quality of the replies given by the data controller, or on the actions undertaken to investigate the case (on site inspection, formal notice to remedy, sanctioning procedure, etc.). In spite of the growing volumes of complaints received, cutting down the complaint resolution deadlines remains an ongoing priority of the CNIL Complaint Department, in an effort to deliver a high-quality service level.

This figure is all the more notable that it does not include the thousands of written enquiries from private individuals processed directly by the SORP Department, which were previously recorded as complaints. It does not include either the multiple questions asked by private individuals on the telephone, which were handled by the SORP and the Complaint Department.

Filing a complaint on line: How does it work?

1. I visit www.cnil.fr and click on “Plainte en ligne” (Complain on line).
2. I select the case that concerns me (e.g. deletion of contents on Internet, opt out of advertising, access to or update of my personal data...).
3. I receive brief and precise information on the case I have selected.
4. I check that I have exercised my rights of access, objection or rectification of my personal data; model letters are suggested by the CNIL.
5. I access the on-line complaint form where I describe my problem and attach any useful documents (e.g. copy of exchanges with the data controller, copy of unsolicited ads received, etc.).
6. The transmission of my complaint is secured, and I receive an acknowledgment of receipt via e-mail and postal mail.
7. My case is processed by the CNIL Complaint Department, whom I can contact if I wish (via postal mail or telephone).
8. Following investigations on my complaint (depending on the complexity of the case), the CNIL will inform me about the actions taken with the data controller and about the outcome.
In pursuance of Article 41 of the Law of January 6, 1978 as amended, any individual wishing to verify their personal data potentially listed in records related to home security, national defense and public safety (STIC, JUDEX, former Homeland intelligence record, etc.) may file a request in writing with the CNIL.

In 2011, the CNIL received 2,099 requests for indirect access, versus 1,877 in 2010. This number attests to a significant increase in requests (+12% versus 2010) although it remains lower than in previous years further to the debates on the creation of the EDVIGE police record and the reorganization of the intelligence departments at the Interior Ministry.

The increase results primarily from growing requests regarding police records (STIC and JUDEX) filed by individuals who were refused access to certain types of jobs or worry about being confronted to such a situation in the future. It is estimated that 1.3 million jobs may be currently affected by administrative procedures of this type.

In its ordinance of June 29, 2011 (CE No. 339147 – combined 10th and 9th subsections), the Conseil d’Etat acknowledged the right of access of heirs to the banking data saved in the FICOBA record (record of bank and related accounts), as “beneficiaries of the account balance held by the deceased”, a ruling that led to an increase of requests for indirect access. Processing of these requests however remains subject to the adoption of a protocol of agreement with the tax authorities which should be finalized shortly.

As a general rule, every request for indirect access requires verifications to be made in several data records in order to reply to the individual’s expectations. Thus, the 2,099 requests received in 2011 required 4,833 checks in various records, and primarily in national police and Gendarmerie records (STIC and JUDEX), in records held by the Information Générale administration of the Interior Ministry (EASP and PASP1) and in the Schengen Information System (SIS).

1 Files relative to “Administrative inquiries related to public safety” and to the “Prevention of risks against public safety”
A total of 3,374 verifications were conducted in 2011, leading to the resolution of 2,393 requests, most of which were received in previous years. Over 60% of these verifications addressed police records, with the following results.

CRIMINAL POLICE RECORDS AND EMPLOYMENT ISSUES: PROGRESS ON LOPPSI

Based on an amendment proposed by Delphine BATHO, MP from Deux-Sèvres (and member of the Parliamentary Information Commission on Police Records), Article 230-8 of the Code of Criminal Procedure, derived from Law No. 2011-267 of March 14, 2011, now provides for the systematic addition in police records of a caption relative to any charges that were dismissed under a discontinuance of proceedings, regardless of the reason (reference to the law, reparation to the victim, non-significant prejudice, therapeutic injunction, etc.).

The effect of this added mention, restricted until now to rulings of discontinuance of proceedings due to “absence of offense” or “insufficient charges”, is to exclude the related cases from the scope of administrative inquiries conducted to authorize access to some types of public or private jobs (security agents, airport activities, municipal police officers, rail security agents, etc.).

Although possibilities for deletion remain strictly restricted (charges dismissed, acquittal, discharge or discontinuance of proceedings due to “absence of offense” or “insufficient evidence”) and subordinated to the agreement of the Public Prosecutor, this much awaited legal amendment will mitigate the penalizing effect of the consultation of police records for jobseekers.

The effective and immediate application of this provision to all existing records (around 6.5 million persons implicated in legal proceedings were recorded in the STIC file and 2.5 million in the JUDEX file in 2011) is however confronted with structural difficulties linked to updating the files, which to a large extent depends on communication from the Public Prosecutors with police authorities about the judiciary outcome of each of the offenses recorded.

While significant progress deserves to be mentioned, a nearly real-time updating of these records will only be possible in the future via the planned interconnection between the Justice Ministry’s CASSIOPEE application and the TPJ system (“Traitement des Procédures Judiciaires”) intended to shortly supersede the STIC and JUDEX records.

Focus

Mr. P., 35, applied for the issuance of a professional permit to work in private security. Concurrently, he filed with the CNIL a request for indirect access to his police record. Further to verifications, two cases of misdemeanor were deleted from the STIC record and two remaining cases were updated with a mention of discontinued proceedings for “failure of the complainant to appear” and “non-significant prejudice”. Mr. P., who had been able to obtain his initial professional permit in spite of these mentions in his record, should no longer have any problem renewing the permit in the future, since he is now “unknown” administratively in this record.
Bad track-records!

Lack of updates by the Prosecutor’s offices

► Mrs. B., 34, was placed in custody for detention and use of a forged foreign driver’s license. After receiving the certificate of authenticity of her license delivered by the Ministry of Transports in her home country, the Public Prosecutor had informed Mrs. B. of its decision to discontinue the proceedings on the grounds of insufficient evidence. The Prosecutor further ordered that the driver’s license be returned to its rightful owner. Mrs. B. then decided to file a request with the CNIL to check for any potential recording of her case in the STIC files. Investigations revealed that her case had indeed been recorded in the file under the charges of “forgery and use of forged document, fraudulent obtention of administrative documents” subjected to a retention period of 20 years. After verification by the CNIL, these data were deleted from the record.

► Mr. K., 39, received in 2006 a letter from the Public Prosecutor’ office informing him that it has approved his request for data deletion from the STIC records for charges of “concealment of stolen good” since the proceedings had been discontinued for insufficient evidence. To Mr. K.’s surprise, he found out during investigations about his application for naturalization that these charges were still recorded in the file, and could prove prejudicial to his naturalization. After verification by the CNIL, these data were effectively deleted from the record, in line with the request from the Public Prosecutor.

Recording of data on a minor

► Mr. and Mrs. G. filed a request for indirect access to criminal police records on behalf of their 17 year-old minor son, to check the status of his personal data in the STIC record. Their son had been taken into custody on charges of “deterioration of public property” following which the charges had been dismissed. The department in charge of managing the STIC record was informed of the dismissal only on the occasion of verifications carried out by the CNIL, following which the data were immediately deleted from the record.

► Mrs. M. filed a request to the CNIL on behalf of her 17 year-old son who had been charged with “sexual abuse” in his school and later cleared of these charges. Since her son wanted to join the Gendarmerie Nationale, she wanted to check that this case was not registered in police records. After verification by the CNIL, it was found that the charges were still in the JUDEX record, and the data were subsequently deleted.

Incorrect recording of facts

► Mr. G., 57, an airline captain with 20 years of experience, was faced with problems to renew his airport identification badge. Even though the badge was ultimately issued, it turned out to have a validity term of 1 year instead of the usual 3 years. Since he was unable to get any further explanations, Mr. G. decided to exercise his right of indirect access to find out the source of his difficulties. The verifications carried out by the CNIL resulted in the deletion from the JUDEX record of a case of “clandestine work, embezzlement and fraud” in which he was never implicated. Mr. G had merely been summoned to appear in the proceedings but neither as a suspect nor as a victim. When the investigation report was entered in the JUDEX record, his name had mistakenly been recorded as the perpetrator, leading to the source of his problems.

► Mr. C., 27, working as a CIT security agent, decided to exercise his right of indirect access to police records after finding out to his great surprise in the course an administrative investigation that he was registered in the STIC record for charges of “sexual assault”. Mr. C. did remember that at a summer camp when he was a minor, another child had been victim of sexual assault, but he himself had only been questioned just like all other children in his dormitory. Only two youngsters had been prosecuted and sentenced. Further to verifications by the CNIL, this case was deleted from the record, since Mr. C. had indeed not been implicated in this case.

► Mr. L., 35, a municipal police officer, decided to exercise his right of indirect access to the STIC record when he discovered that an incident with a dog owner who had later filed a complaint against him in the context of his professional duties, had been recorded in the files. Further to verifications conducted by the CNIL, the incident was deleted from the STIC record since misdemeanors are not authorized to be recorded.

Expriy of the retention period

► Mr. C., 24, an aeronautic mechanic, decided to exercise his right of indirect access to police record after his application for an airport access badge, indispensable in his job, was rejected. After verifications conducted by the CNIL, his record for charges of “simple theft” kept in the STIC file beyond the 5-year authorized retention period was deleted.
Identity theft

Miss B., 24, undergoing training as flight attendant, filed a request for indirect access by the CNIL, after her younger sister confessed to using her ID card when she was arrested by the police for "shoplifting". While Miss B. was already aware that someone else was misusing her identity after receiving several notifications from a number of transport companies, this latter case could have been potentially prejudicial to her future career, leading her to file an official complaint at the police station. Based on a comparison of fingerprints she had filed along with her complaint, the CNIL was able to have the shoplifting charges removed from her record.

NEW PARLIAMENTARY REPORT ON POLICE RECORDS

Following several hearings before the report authors, the Commission is pleased to see that the conclusions reached by the Parliament members are largely consistent with its own analysis on many issues. MPs Delphine BATHO and Jacques-Alain BENISTI stressed in particular the improved relations between the Commission and the Interior Ministry. They further highlighted the development of an Informatique et Libertés data protection culture in the management of police records, along with the approach initiated to sort out data processing operations not previously notified to the CNIL.

This progress however remains very incomplete and efforts need to be pursued over the coming years. In their latest report published on December 21, 2011, and similarly to previous reports, the MPs inventoried all processing operations carried out or under development at Interior Ministry administrations. Their findings revealed the existence of 80 records versus 58 inventoried in March 2009 in the first report), some of which are unlawful under the terms of the Informatique et Libertés Act. The CNIL has therefore contacted the Interior Ministry to obtain the necessary information and ask about the measures envisaged by the Ministry further to these findings.
AUDITS

2011 was a significant year for the CNIL’s auditing activity further to the LOPPSI 2 Act (Orientation and Planning for efficient homeland security, dated March 14, 2011) which extended the CNIL’s auditing powers to include the oversight of so-called “videoprotection” systems. The Commission’s work on this topic is presented in Chapter I of the report. In addition, the Law of March 29, 2011 relative to the “Defender of Rights” also changed slightly the exercising conditions of the CNIL’s auditing powers.

In pursuance of the case law of the European Court of Human Rights (April 16, 2002 - Société Colas Est vs. France) and of the Conseil d’État (Order PRO DECOR and INTER CONFORT of November 6, 2009), the CNIL informs the managers of private business premises of their right of objection prior to starting any auditing operations.

The law of March 29, 2011 supplemented the Informatique et Libertés Act, specifying the conditions under which objections can be referred to judiciary authorities in order to authorize the audit. Thus the CNIL President may refer the case to the Juge des Libertés et de la Détention (JLD) who then has a deadline of 48 hours to issue a ruling.

In 2011, three organizations exercised their right of objection, and in each case, the judge issued a ruling authorizing the auditing operations.

Moreover, the March 2011 law introduced the possibility for the CNIL to petition the competent JLD judge to authorize inspection visits, prior to the start of auditing operations; accordingly, the manager of the premises cannot object to the audits. The capacity to petition the judge beforehand may be exercised whenever justified by urgency, seriousness of the facts or high risks of document destruction or concealment.

In 2011, the CNIL used this possibility four times: in each case, the judge authorized the audit to proceed, on the grounds of the evidence delivered by the CNIL to support its petition.

Once again in 2011, the number of audits conducted increased sharply; the CNIL carried out 385 audits throughout the year, i.e. a 25% increase versus the previous year, illustrating once more the Commission’s determination to enforce compliance with the Informatique et Libertés Act, via in situ inspections.

As regards the organizations audited for compliance with the Informatique et Libertés Act, it should be noted that 85% belong to the private sector and 15% to the public sector.

Concerning the nature of the audits, 40% were conducted in the context of the 2011 annual audit plan adopted by the CNIL plenary assembly. As previously announced, the Commission had targeted the following topics in its audit plan:

• “Security of health data”: in 2011, over twenty audits addressed the processing
of health-related data. These audits were conducted in health care establishments (private clinics, hospitals, etc.), health data hosting providers, aggregators of medical data, etc.

- “Client/prospect: can we escape being tracked?”: some twenty audits were carried out on this subject in 2011, addressing primarily e-commerce sites (issue of the new legal regime for cookies), providers of marketing services (routers and advertising agencies), as well as firms involved in client/prospect data management (mega-databases). A review of the audit findings should be communicated some time in 2012.

- “Debt collection agencies / Private investigators”: around ten audits were conducted with private investigation and debt collection agencies. Although more audits on this topic will continue in the first quarter of 2012, it can already be noted that the audits and sanctions adopted since 2006 have helped structure this business sector where many agencies have for instance appointed data protection officers (or “Informatique et Libertés Correspondents”).

- “Transborder data flows”: around fifteen audits were carried out in 2011 with multinational companies headquartered in France who were granted authorizations to transfer data outside the European Union. Until now, these audits have not revealed any major lack of compliance with the authorizations granted, or any unsupervised transfers.

It should further be noted that 24% of the audits were conducted in the context of complaint investigations, 11% in sanction procedures and 25% in response to topical issues such as security faults reported to the CNIL.

Lastly, the CNIL carried out numerous audits in 2011 in the context of partnership agreements signed with other administrative authorities.

Such is the case for instance of the protocol signed on January 6, 2011 with the French Directorate of Competition, Consumers and Fraud (Direction générale de la concurrence, de la consommation et de la répression des fraudes, DGCCRF). Under this information exchange and cooperation agreement, the CNIL was able to intervene with web sites where DGCCRF investigators had found cases of non-compliance, either via notices sent by mail or via in situ inspections.

A number of audits were also conducted based on reports received from the Labor Inspectorate or from the Defender of Rights.
Summary report on the 2011 activity of the Sanction Select Committee
SUMMARY REPORT
ACTIVITY OF THE SANCTION
SELECT COMMITTEE

65 formal notices to comply were issued in 2011, of which 27 decided by the CNIL Select Committee prior to the reform introduced by the Law of March 29, 2011 relative to the Defender of Rights, and 38 by the CNIL President since the reform.

19 sanctions were issued by the Select Committee, including 13 warnings in 2011, 5 financial penalties and one injunction to cease data processing.

65
FORMAL NOTICES
TO COMPLY

19
SANCTIONS WERE
ISSUED

13
WARNINGS
A significant number of notices to comply were closed in 2011 (105 versus 67 in 2010 and 75 in 2009). Formal notices to comply are used primarily as an instrument enabling organizations to remedy any non-compliance with the Informatique et Libertés Act. The high rate of notice closure shows the efficiency of this procedure, designed to help organizations become aware of any lack of compliance with the law and to provide support in remediying the situation.

Consequently, this approach explains why the number of warnings issued by the Select Committee is higher than the financial penalties. Issuance of a warning is not conditioned to the prior adoption of a formal notice, while financial sanctions are considered only in case of failure to remedy and comply.

Most frequently sanctioned failures to comply with the Informatique et Libertés Act

- Information to data subjects – Right to access and to object: 15%
- Lack of reply to CNIL’s requests: 5%
- Adequacy, relevance and non-excessive nature of data: 25%
- Legal and fair data collection: 30%
- Data security and confidentiality: 25%

Significant number of notices to comply were closed in 2011 (105 versus 67 in 2010 and 75 in 2009). Formal notices to comply are used primarily as an instrument enabling organizations to remedy any non-compliance with the Informatique et Libertés Act. The high rate of notice closure shows the efficiency of this procedure, designed to help organizations become aware of any lack of compliance with the law and to provide support in remediying the situation.

Consequently, this approach explains why the number of warnings issued by the Select Committee is higher than the financial penalties. Issuance of a warning is not conditioned to the prior adoption of a formal notice, while financial sanctions are considered only in case of failure to remedy and comply.

Warning: is it a sanction?

Article 45 of the law of January 6, 1978 as amended by the “Defender of Rights” reform, now specifies expressly that a warning is a sanction, which is not conditioned by the prior issuance of a formal notice to comply, as is the case for a financial penalty. A warning may be required and issued directly further to the disclosure of a non-compliance. At the request of the CNIL President, the Select Committee may therefore use this channel to sanction proven facts, even though they may have been remedied on the day of the hearing. For instance, a security fault reported to and confirmed by the Commission may be subjected to a warning procedure, even though it has been remedied on the day of the hearing. The warning may also sanction proven failures to comply persisting up to the day of its issuance.
## List of sanctions issued in 2011

<table>
<thead>
<tr>
<th>Date</th>
<th>Name or type of organization</th>
<th>Decision adopted</th>
<th>Main failure</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2011</td>
<td>Google</td>
<td>Financial penalty of 100,000 euros</td>
<td>Abusive data collection</td>
<td>Telecom</td>
</tr>
<tr>
<td>03/02/2011</td>
<td>Pupil tutoring*</td>
<td>Warning</td>
<td>Abusive comments</td>
<td>Home tutoring</td>
</tr>
<tr>
<td>03/03/2011</td>
<td>Pupil tutoring*</td>
<td>Warning</td>
<td>Abusive comments</td>
<td>Home tutoring</td>
</tr>
<tr>
<td>03/02/2011</td>
<td>Marketing of gift packs*</td>
<td>Financial penalty of 50,000 euros</td>
<td>Right to object disregarded</td>
<td>Retail</td>
</tr>
<tr>
<td>17/03/2011</td>
<td>Credit and debt collection firm*</td>
<td>Warning</td>
<td>Abusive comments</td>
<td>Banking</td>
</tr>
<tr>
<td>24/03/2011</td>
<td>Banking*</td>
<td>Warning</td>
<td>Information collection</td>
<td>Banking</td>
</tr>
<tr>
<td>16/06/2011</td>
<td>PM Participation</td>
<td>Financial penalty of 10,000 euros</td>
<td>Unfair collection</td>
<td>Real estate</td>
</tr>
<tr>
<td>30/06/2011</td>
<td>Social housing management firm*</td>
<td>Warning</td>
<td>Unfair and unlawful data collection</td>
<td>Public sector-property management</td>
</tr>
<tr>
<td>30/06/2011</td>
<td>Public administration*</td>
<td>Dismissal</td>
<td>Security and confidentiality</td>
<td>Public sector</td>
</tr>
<tr>
<td>05/07/2011</td>
<td>Yellow Pages **</td>
<td>Public warning</td>
<td>Unfair collection and processing</td>
<td>Telecom</td>
</tr>
<tr>
<td>05/07/2011</td>
<td>Sport Federation*</td>
<td>Warning</td>
<td>Insufficient security</td>
<td>Sport</td>
</tr>
<tr>
<td>05/07/2011</td>
<td>Network of real estate agencies**</td>
<td>Public warning</td>
<td>Abusive comments</td>
<td>Real estate</td>
</tr>
<tr>
<td>12/07/2011</td>
<td>Association LEXEEK **</td>
<td>Financial penalty of 10,000 euros and injunction to cease processing</td>
<td>Right to object disregarded</td>
<td>Association</td>
</tr>
<tr>
<td>21/07/2011</td>
<td>Political movement*</td>
<td>Warning and emergency procedure</td>
<td>Security and confidentiality</td>
<td>Public sector</td>
</tr>
<tr>
<td>15/09/2011</td>
<td>Mail-order sale company</td>
<td>Dismissal</td>
<td>Right to object disregarded</td>
<td>Retail</td>
</tr>
<tr>
<td>15/09/2011</td>
<td>Real estate agency*</td>
<td>Warning</td>
<td>Lack of reply to CNIL's requests</td>
<td>Real estate</td>
</tr>
<tr>
<td>13/10/2011</td>
<td>Health care data hosting center*</td>
<td>Warning</td>
<td>Security and unlawful data collection</td>
<td>Health care</td>
</tr>
<tr>
<td>13/10/2011</td>
<td>TV, phone &amp; Internet service provider*</td>
<td>Warning</td>
<td>Security and confidentiality</td>
<td>Telecom</td>
</tr>
<tr>
<td>10/11/2011</td>
<td>Urbna &amp; rural developer*</td>
<td>Warning</td>
<td>Abusive comments</td>
<td>Public sector</td>
</tr>
<tr>
<td>01/12/2011</td>
<td>GROUPE DSE FRANCE</td>
<td>Financial penalty of 20,000 euros</td>
<td>Unfair collection</td>
<td>Real estate</td>
</tr>
</tbody>
</table>

* Sanctions not made public by the Select Committee. - ** Referred to the Conseil d'Etat.
8.

TOPICS OF INVESTIGATION IN 2012

Revision of EU Directive: A successful data protection Union
REVISION OF EU DIRECTIVE: A SUCCESSFUL DATA PROTECTION UNION

A YEAR OF INVESTIGATION AND CONSULTATION FOR THE EUROPEAN COMMISSION

Strategic priority for the European Commission
The revision of EU Directive 95/46/EC, setting the European legal framework on personal data protection, is a priority goal of the European Commission and its Vice President Viviane Reding, Commissioner in charge of Justice, Fundamental Rights and Citizenship.

The Communication published by the European Commission in November 2010 formed the foundation for the investigations conducted in 2011. The EU Commission introduced five key goals: reinforce individual rights, bolster the “internal market” dimension and ensure a broader harmonization of data protection rule, extend the scope of application of general regulations on data protection to the field of police and judicial cooperation, reassert the global scope of data protection, and strengthen the role of national data protection authorities and of the G29, the group of European data protection agencies, in the perspective of enhanced compliance with data protection.

European Parliament and EU Council taking over the debate
The European Parliament and the EU Council intervened in the debate, with a response to the European Commission Communication of November 2010. Thus the Directorate of Justice and Home Affairs (JHA) of the European Union and the European Parliament (LIBE Committee) greeted favorably the EU Commission’s orientations. The Parliament however expressed concerns about the measures provided regarding applicable law, and called for a clarification of the related criteria in order to ensure a homogeneous and high level of protection across the entire Union and prevent any phenomenon of “forum shopping*”.

The term of “forum shopping” refers to a company choosing to register its head office in one country rather than another, based on considerations of more favorable national legislation.

The European Commission’s project has matured in 2011, with the consultation of various players and experts regarding the practical implementation of its major guidelines. On January 25, 2012, the EU Commission adopted a draft Regulation and a draft Directive reforming the legal framework of data protection.

Charter of Fundamental Rights of the European Union
The Charter was adopted by the European Council at its meeting in Nice on December 7, 2000. However, the Lisbon Treaty, since its entry into force on December 1, 2009 conferred to the Charter the same legal value as other Treaties. Since then, the Charter is therefore legally binding on all EU Member States, and all citizens can avail themselves of the Charter in the event of non-compliance with European legislation regarding their fundamental rights. The Charter contains 54 articles defining the fundamental rights of individuals within the EU, classified under six individual and universal values forming the foundation of the European construction: dignity, freedoms, equality, solidarity, citizens’ rights and justice.

The Charter is the first document of this type to recognize explicitly data protection as a fundamental right. Thus, Article 8 proclaims that “Everyone has the right to the protection of personal data concerning him or her”.

* The term of “forum shopping” refers to a company choosing to register its head office in one country rather than another, based on considerations of more favorable national legislation.
THE CNIL MOBILIZED TO RETAIN A HIGH LEVEL OF PROTECTION ACROSS EUROPE

Close involvement in the G29

As the official body representing all data protection authorities in the European Union, the G29 was closely involved in the revision of the EU Directive.

At the European Commission’s request, the G29 issued five opinions, to which the CNIL contributed extensively, relative to the following fundamental issues: legal regime applicable to sensitive data, simplification of the processing notification system, cooperation between data protection authorities, applicable law, and concept of consent. In addition, the European Commission organized several meetings with the G29, dedicated to look at orientations for the reform.

As G29 Chairman until 2009, Alex Türk had initiated the drafting of a strategic opinion paper regarding the future of privacy, which was later taken on board by the European Commission in its November 2010 Communication. The CNIL favors a balanced approach to the revision: the expectations of enterprises must be heard, and changes to the current framework must first and foremost benefit the citizens.

Developing relations with the EU Commission and the European Parliament

The CNIL has met with the European Commission authorities in charge of drafting the revised directive. Backed by its 30-year long experience, the CNIL advocates a data protection system that is all at once participatory and decentralized, as it seems to be best suited to the digital world and to the diversity of situations in the field, where several legal facets are interwoven, whether labor law, criminal law, tax law, business law, etc., that national authorities alone are in a position to recognize. In order to be both efficient and democratic, European governance on data protection must rely on in-depth cooperation between the competent sovereign authorities.

As the sole European body elected directly by the citizens, the European Parliament is concerned with all issues affecting fundamental rights. The Parliament proved particularly strict and demanding on the Swift (1) and PNR (2) projects. The CNIL felt it would useful to meet with several Europeans MPs in May 2011, in the context of the draft Parliamentary Report on the European Commission’s Communication. The encounters provided the opportunity to establish initial contacts with several key players at the Parliament and to set the cornerstones of cooperation with them.

Lastly, the CNIL President met with Ms. Reding in Paris on November 26, 2011, taking this opportunity to reiterate the CNIL’s positions regarding the orientations chosen for the draft Regulation, a few weeks before the draft was finalized by the EU Commission.

---

1 PNR (Passenger Name Record): information collected from airline passengers when booking flights. 2 SWIFT (Society for Worldwide Interbank Financial Telecommunication): cooperative company governed by Belgian law, founded in 1973, offering a range of services to banks, including a system of secure e-mail.
MAINTOPICSOFDISCUSSION
WITHTHEEUROPEANCOMMISSION

Alongside all other national data protection authorities, the CNIL welcomes the progress made in the EU draft Regulation to reinforce the rights of individuals, in particular regarding the right to oblivion, data portability and consent. Nevertheless the CNIL feels that a number of provisions still remain unclear or may raise problems.

Competenceofauthorities:theEuropeanCommission’srisky approachtocitizens’rights

In an effort to remedy the fragmented nature of national legislations, the European Commission has opted to focus on a strict harmonization of the applicable rules and on facilitating the life of businesses whose processing operations have an impact on the territories of several Member States. It thus provides for a clause allowing for competence to be ascribed to a single authority, based on the criterion of primary establishment of the data controller, which generates concerns for the CNIL.

This option could have significant political consequences since it would contribute to keep citizens away from their competent authorities; if the competent authority is that of the jurisdiction when the data controller’s primary establishment is domiciled, then, regardless of the public targeted by its business activity, the national data protection authority would merely act as a “drop box” for citizens who would otherwise have grounds to solicit it about their problems. This would mean in practice that, in the event of a problem encountered by a user on a social network whose primary establishment is domiciled in another Member State, the complaint would be addressed by the authority having jurisdiction over that State, rather than the authority with jurisdiction over the user’s place of residence. A citizen subsequently wishing to object to the conclusions reached by investigations on his complaint would then have to appeal to a foreign court, which would be largely unfeasible.

The CNIL has highlighted the drawbacks of this approach; indeed it would be paradoxical for personal data protection to end up being weaker than under consumer law which favors jurisdiction based on the consumer’s place of residence. Furthermore, for a single business transaction, a French citizen would have to refer the case both to the DGCCRF for consumer aspects, and to another authority located in another Member State for the data protection aspect.

In addition, such a criterion would encourage forum shopping practices for data processing operations having an immediate impact on the French territory, in particular for those carried out by the major Internet operators.

International transfers: data protection authorities must retain their role of oversight

In view of the steadily growing globalization of data exchanges and services, as illustrated by the boom of Cloud Computing for instance, international data transfers constitute a crucial economic and political challenge, for France and for all EU Member States.

In order to mitigate the risk of losing control over the exchanged data, the CNIL considers that the guarantees provided under the draft Regulation can derive only from legally binding instruments: e.g. standard contractual clauses or internal corporate rules, previously validated by the data protection authorities on the basis of predefined reference standards.

Such instruments, which have been tested and upgraded for several years by the European Union, and have aroused great interest from enterprises, will allow for enhanced protection when transferring abroad the citizens’ personal data. Accordingly, this system should not be made vulnerable by using any non-binding instruments, not previously approved by the data protection authorities.

The risk is that the “Primary establishment” criterion may keep citizens away from their national authorities

The term of “forum shopping” refers to a company choosing to register its head office in one country rather than another, based on considerations of more favorable national legislation.
Data protection is everybody’s business: what are the roles and responsibilities of players?

The notion of accountability of the players involves a general obligation of being accountable by requiring them to implement proactive measures of data protection (appointment of a data protection officer, impact assessments, regular audits, etc.). Once implemented, such measures must enable the enterprise to fully demonstrate its compliance with regulations. Thus, the notion of accountability would introduce the issue of privacy protection at the core of corporate practices to ensure real and efficient protection.

It is essential for the authorities to retain a power of oversight and control over these new instruments, particularly as regards reference standards relative to training and auditing, so that compliance and effectiveness of the measures adopted can be fully assessed.

The measures taken to ensure the accountability of players should not merely be self-regulation measures that would substitute for fundamental values, but should rather be regarded as a complement to existing guidelines.

EUROPE FACED WITH THE CHALLENGE OF A CHANGING INTERNATIONAL ENVIRONMENT

The ongoing investigations about the future of data protection in various regions of the world represent an opportunity to progress towards more consistency between national and international instruments and a more holistic and global approach. The CNIL along with all EU data protection authorities at their international conference in 2009 have adopted common principles named the “Madrid Standards”. The goal is now to implement a legally binding instrument applicable worldwide, based on these principles.

Furthermore, all existing legal regimes across the world are undergoing modifications, which attests to the growing awareness on the importance of the topic:

» Council of Europe: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as “Convention 108”) dates back to 1981. The Council of Europe has launched an extensive public consultation for the purpose of modernizing it. The CNIL supports in particular the intended global scope of the Convention 108 and encourages non-EU States to ratify it. The Advisory Committee intends to finalize a proposal on this topic and submit it to the Council of Ministers in late 2012.

» Organization for Economic Cooperation & Development (OECD): in 1980, the OECD adopted a set of Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. On the occasion of the Guidelines’ 30th anniversary, the OECD initiated a revision process to which the CNIL has contributed. The conclusions regarding the appropriateness of revising the Guidelines will be published in 2012.

» APEC (Asia-Pacific Economic Cooperation forum): the sub-committee on privacy protection met in September 2011 in San Francisco, USA, a meeting which the CNIL attended for the first time as an observer representing the International Conference of Data Protection and Privacy Commissioners. The meeting addressed the implementation of the Cross Border Privacy Rules (CBPR). This system is still not operational, but the question of a possible interoperability between the CBPRs and the European BCRs (Binding Corporate Rules), already implemented, will be a crucial issue over the coming years.
APPENDICES

CNIL membership

CNIL: Means & Resources
CNIL MEMBERSHIP

BUREAU

President
Isabelle FALQUE-PIERROTIN, Councilor at Conseil d’État CNIL member since January 2004 and Vice President from 2009 to 2011, Isabelle Falque-Pierrotin was elected as CNIL President on September 21, 2011.

Deputy Vice President
Emmanuel de GIVRY, Honorary Counsel at the Cour de Cassation
Sector: Human Resources
CNIL member since February 2004 and Deputy Vice President since February 2009.

Vice President
Jean-Paul AMOUDRY, Senator from Haute-Savoie
Sector: Banking & Credit
CNIL member since January 2009 and Vice President since October 2011.

MEMBERS (COMMISSIONERS)

Jean-François CARREZ, Honorary Chamber President at the Cour des Comptes
Sector: Transports, Elections
CNIL member since January 2009. Member of Sanction Select Committee.

Dominique CASTERA, Member of Social, Environmental & Economic Council
Sector: International Police Cooperation – Associations
CNIL member since October 2010.

Jean-Marie COTTERET, University Professor Emeritus
Sectors: National Police & State Security
CNIL member since January 2004. Vice Chairman of the Sanction Select Committee.

Claire DAVAL, Attorney at Law
Sector: Justice
CNIL member since February 2009. Elected Chairperson of the Sanction Select Committee.

Claude DOMEIZEL, Senator from Alpes-de-Haute-Provence
Sector: Sustainable Development & Housing
CNIL member since December 2008. Elected Member of Sanction Select Committee.

Didier GASSE, Master Councilor at Cour des Comptes
 Sector: Telecommunications & Internet, E-voting
CNIL member since January 1999.

Gaëtan GORCE, Senator from Nièvre
Sector: Public liberties and e-administration
CNIL member since December 2011.

Philippe GOSSELIN, Member of Parliament, La Manche
Sector: Tax & Labor Issues
CNIL member since June 2008.

Sébastien HUYGHE, Member of Parliament, Nord district
Sector: Identity, Defense & Foreign Affairs
CNIL member since July 2007. Elected member of the Sanction Select Committee.

Jean MASSOT, Honorary Section President at the Conseil d’État
Sector: Healthcare & Health Insurance – Public archives and data
CNIL member since April 2005.

Marie-Hélène MITJAVILE, Councilor at the Conseil d’État
Sector: Research & Statistics
CNIL member since January 2009.

Eric PERES, Member of Social, Environmental & Economic Council
Secteur : Education et enseignement supérieur
CNIL member since December 2010.

Bernard PEYRAT, Honorary Councilor at the Cour de cassation
Sector: Commerce & Marketing
CNIL member since February 2004.

Dominique RICHARD, Consultant
Sector: Cultural & Sports Affairs, Videoprotection
CNIL member since January 2009. Elected member of the Sanction Select Committee.

Government Commissioners
Élisabeth ROLIN
Catherine POZZO DI BORGO, Assistant
CNIL: MEANS & RESOURCES

CNIL STAFF

The steady trend in staff growth, initiated in 2004, was confirmed in 2011, due to the new duties and missions assigned to the CNIL by the amendment to the *Informatique et Libertés* Act.

With 11 additional positions created, i.e. an annual workforce increase of 7.5%, the CNIL had 159 budget-approved positions in 2011 versus 148 in 2010, thereby doubling its payroll expenses within 7 years.

The steady staffing increase enables the CNIL to gradually catch up with the gaps already noted in 2004, particularly as compared to its European peers who employ an average staff of 200. The additional positions enabled the Commission to respond to its traditional tasks of audits, sanctions, coordination of the CIL network, authorization of sensitive data records, or label certification award, among others.

Yet this significant increase in resources still remain insufficient, as underlined in the recent parliamentary debates on the adoption of the 2012 Finance Act.

In 2011, the scope of the tasks entrusted to the CNIL by the legislator was considerably extended.

Firstly, the provisions of the LOPPSI 2 Law of March 14, 2011 entrust the CNIL with a new mission of oversight on video-surveillance systems installed on the public highway, in application of the Law of January 21, 1995; yet these systems number hundreds of thousands.

Secondly, Article 17 of the Law of March 22, 2011 relative to the transcription into French law of the “Telecom Package” European Directive leads to an obligation for data controllers to report any security faults to the CNIL, i.e. in case of breaches of integrity or confidentiality of personal data. It is still very difficult at this time to quantify the number of security faults likely to be reported to the CNIL.

In view of new legal provisions, the CNIL headcount is therefore likely to further increase significantly over the coming years.

BUDGET

In 2011, the CNIL was endowed with a total budget of 15.8 million euros, an increase of 8% versus 2010, of which 10.3 million euros allocated to personnel expenses and 5.5 million to operating expenses.

The budget allocated to personnel expenses increased by nearly one million euros between 2010 and 2011, a 10% increase inherent to the additional staff positions created at the CNIL.

The 2011 operating budget also increased but to a lesser extent, rising only by 140,000 euros versus 2011, after appropriation of the “precautionary reserves” and the freeze of the “Fonds d’Etat exemplaire”. This limited increase confirms de facto the trend observed since 2004, namely that increases in operating funds do not follow increases in personnel expenses funding. For several years now, the CNIL has pursued a policy of operating cost control designed to reduce the expenditure ratios linked to premises occupancy, purchases of IT office equipment, or to staff travel and accommodation expenses.