



Country or Jurisdiction Report

FRANCE

Web site: <http://www.cnil.fr>

1. Measurement of diversity, “ethnic statistics,” equal opportunity: the CNIL launches a debate

The fight against discrimination, which involves all areas of social life: education, employment, housing, health and so on, is the subject of much debate in France. Everyone agrees on the need to fight all forms of discrimination, but in order to do so, the various forms have to be identified and quantified. What criteria should be used? What are the best statistical methods? Who can do the job?

The *Commission Nationale de l'Informatique et des Libertés* (CNIL), France's national privacy commission, published its first recommendations on the subject in July 2005, and followed up by holding more than sixty hearings between November 2006 and February 2007 to seek the views of researchers, statisticians, trade unions, religious leaders, representatives of associations, experts, business leaders and others. The CNIL also sought the opinions of Web users with an online questionnaire that heard from roughly 1000 respondents. The hearings were covered by France's main political information channel *Public Sénat*.

The hearings revealed a broad range of viewpoints, some differences of opinion, and difficulty in achieving a consensus. When they drew to a close, however, the CNIL was able to draw two main conclusions:

- France must improve its statistical capability;
- There are things that can be done at once to improve knowledge of our society, and thus to combat the various forms of discrimination more effectively.

The CNIL accordingly developed 10 recommendations, which were published in May 2007.

- It is essential to make broader use of existing sources of information, and give researchers easier access to personnel records, administrative files and public statistical databases, within privacy rules.
- To assess the reality of discrimination as it is experienced, questionnaires must be used to conduct surveys of the people concerned. As long as they are optional and based on self-identification, and the answers remain confidential, people should be asked questions about their nationality and place of birth, and those of their parents. It is also important that people who feel discriminated against indicate the criteria—physical appearance, language, name and so on—on which they feel the discrimination is based.
- Analysis of first and last names, provided it does not lead to classification into ethnic or racial categories, can be useful under certain conditions in detecting potentially discriminatory practices.
- The CNIL continues to have reservations about the establishment of an “ethno-racial” reference system.
- Lastly, French privacy legislation must be amended to ensure better protection for individuals and sensitive personal data by guaranteeing the scientific nature of research, and strengthening CNIL monitoring of research data for which the consent of those concerned is not in itself sufficient.

2. Increased monitoring and sanctions

In 2006 and 2007 the number and scope of audits conducted by the CNIL increased, as did the sanctions imposed by its limited staff.

With passage of the Act of August 6, 2004, the CNIL’s auditing authority was expanded substantially, and upon completion of an adversarial procedure it now has the authority to issue a warning, a formal summons, a monetary sanction, an order to cease processing, and so on. This was a major change in the powers previously wielded by the CNIL.

Implementing these powers has made it necessary to develop authentic audit and sanction policies: for example, what are the criteria for conducting an audit, in what cases is a monetary sanction justified, how is the amount of such a sanction determined, what publicity should it receive, and so on? The CNIL has now moved out of the experimental stage in the implementation of these powers, and it may be said that its determination to make consistent and systematic use of its powers has attracted the constant attention of the media, those who process data and those who advise them.

The number of articles devoted in recent months to sanctions imposed by the CNIL says a great deal about the changes in the public—and particularly the corporate—perception of its role. Deserving of special note is the impact of the financial sanction—€30,000 [\$43,000]—imposed on foreign-owned Tyco Healthcare, which attracted media attention in the US.

To date, the CNIL has imposed 16 monetary sanctions ranging from €300 to €60,000 [\$430 to \$86,000], and issued 170 summonses, 11 orders to cease or amend processing practices,

and 15 warnings. Thus, it has achieved a 200% increase in activity with respect to sanctions since 2006.¹

The number of audits is also increasing sharply, and this should constitute a major growth area in CNIL activities in the years ahead. In 2006/2007, 213 audits were carried out. A quarter of them were in response to complaints from individuals, or reports posted to the CNIL site by Web users.

The main sectors of activity audited in 2006/2007 were as follows:

- biometrics;
- global positioning;
- the national police database ("STIC");
- commercial marketing;
- private researchers;
- the Navigo online ticketing application introduced by the corporation that runs the Paris subway system;
- recruiting.

3. Biometrics: the CNIL is vigilant, and concerned

The CNIL has always been most attentive to developments in the processing of biometric data. Its vigilance has been stepped up since the new legislation was passed on August 6, 2004, requiring all processing of biometric data to be approved in advance by the CNIL.

Thus, the CNIL examines every proposal, looking at the characteristics of the biometric data used, and the risks entailed for individual freedoms and privacy.

The policy applied by the CNIL in deciding whether to grant approval essentially means that it will authorize the storing of fingerprints in a centralized database only if the technology is justified by a strong security imperative. An example might be control of access to nuclear sites. On the other hand, the CNIL would not authorize the use of biometric devices with a centralized database, which is always open to misuse, to monitor children entering school cafeterias.

The number of cases submitted to the CNIL, the variety of biometric technologies used to identify faces, voices, hands, blood vessels and so on, and the purposes for which biometric devices are being used, are all expanding very rapidly. For example, whereas only 40 applications involving biometric systems were reviewed in 2005, there were 360 in 2006, and 200 applications for approval of biometric systems have already been processed in the first half of 2007 alone. During the same period, moreover, the CNIL has devoted more than 30% of its on-site audits to the inspection of biometric systems, and issued a dozen summonses under its sanctioning authority.

Also in 2006, a number of biometric projects that are national or international in scope were announced. For example, the Ministry of the Interior announced that the forthcoming electronic national identity cards will incorporate biometric data, namely fingerprints. The Ministry has also decided to require all visa applicants to be issued an electronic portrait that includes prints of all 10 fingers, and a photograph: the "VISABIO" project.

¹ A table listing sanctions imposed by the CNIL is appended.

Noting the very rapid spread of biometric devices in the field, the CNIL is nonetheless concerned that the technology will become commonplace under conditions of use that are potentially dangerous for the fundamental freedoms of citizens.

The CNIL's call for vigilance found a significant echo in May 2007 in an opinion on biometrics issued by the *Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé*, a national advisory committee on ethics in the field of health and life sciences, expressing concern that ultimately, and even with a measure of indifference, everyone agrees to be inventoried, observed, surveyed and tracked, often without being aware of it.

The CNIL took the opportunity to point out that technological developments should not come at the expense of human rights. The President of the CNIL has accordingly expressed concern several times in 2007 about the inadequate resources assigned to it for the monitoring of such phenomena as biometrics.

4. The development of “privacy representatives” (*correspondants informatique et libertés* or *détachés à la protection des données*)

A reform that symbolizes the thinking behind the new French privacy legislation, the “privacy representative” (*correspondant à la protection des données personnelles*, *correspondant* or CIL for short) is a successful innovation.

A total of 1,450 organizations have now designated a *correspondant* in France. These appointments have been made by major industrial groups, insurance companies and savings cooperatives, local and territorial communities, associations, hospitals, universities, law firms and small business.

To support the trend towards the appointment of privacy representatives, the CNIL has initiated a large-scale education and communication operation for those concerned. Thus, the largest French corporations and—through the national association of mayors, the *Association des Maires de France*—municipalities have been encouraged to appoint representatives.

The CNIL has also signed partnership agreements with ACFCI (*Assemblée des chambres de commerce et d'industrie*) and the conference of university presidents (*CPU - Conférence des Présidents d'Université*). These partnerships are designed to improve knowledge of the French legislation that protects privacy through awareness activities and the promotion of a privacy culture.

Additionally, the CNIL held six regional gatherings as part of its information and awareness program focusing on the role of privacy representatives.

In order to offer special assistance to CILs, the CNIL has setup a network (*cellule correspondants*) to help them carry out their responsibilities. An e-mail address and a hotline for the exclusive use of CILs have been set up.

The network also offers generalist training including a presentation on the CNIL and its services, what it expects of its privacy representatives, and implementation of the privacy law. Briefings on specific subjects—such as biometrics, human resources, electronic administration, health, local communities and so on—are also available. More than 250 CILs have attended a one-day CNIL training session.

APPENDIX

**TABLE OF MONETARY SANCTIONS IMPOSED BY THE CNIL
(June 2006 to June 2007)**

Date	Name of organization sanctioned	Amount of sanction	Reason
June 2006	CREDIT LYONNAIS	€45,000	Improper entries in records of the central bank Obstructing the work of the CNIL
June 2006	Bailiff firm	€5,000	Improper "notepad" areas Obstructing the work of the CNIL
September 2006	Internet service provider	€300	Spam
September 2006	Consultancy	€500	Failure to respect the right not to be solicited for business
September 2006	Business	€1,500	Failure to respect the right not to be solicited for business
September 2006	Financial establishment	€1,000	Failure to respect the right not to be solicited for business
November 2006	CREDIT AGRICOLE CENTRE FRANCE	€20,000	Improper entries in records of the central bank
December 2006	Two window sales companies	€60,000	Failure to respect the right not to be subjected to telemarketing
December 2006	TYCO HEALTHCARE FRANCE	€30,000	Improper cross-border data transfers Obstructing the work of the CNIL
December 2006	Telemarketing firm	€5,000	Failure to respect the right not to be subjected to telemarketing
March 2007	Telecom operator	€10,000	Refusal to grant access
March 2007	BANQUE DES ANTILLES FRANCAISES	€30,000	Improper entries in records of the central bank
March 2007	Collection agency	€5,000	Failure to declare research data on debtors Excessively long retention of data

March 2007	Telemarketing firm	€10,000	Failure to respect the right not be subjected to telemarketing
May 2007	Real estate company	€15,000	Improper black list of tenants who were slow to pay
June 2007	Private investigation firm	€50,000	Improper collection of data on debtors Collection of sensitive data Excessively long retention of data