THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
October 2011 • Volume 11 • Number 8

FRANCE—Behavioural biometrics device authorized


By Pascale Gelly, CIPP/E, and Caroline Doulcet

The CNIL has granted an authorization to JVL for its software enabling the identity an individual according to his/her keystroke. The technology can be used to authenticate users in providing access to IT systems and applications. It analyzes the time span during two keystrokes while typing a series of 20 digits minimum.

Biometrics patterns will be encrypted using a strong public algorithm and a key specific to JVL. JVL will have to ensure that no device can be installed to record and simulate the user's keystroke without his knowledge.

The authorization at this stage is granted only for the purpose of demonstration of the tool by JVL to potential customers.

***Pascale Gelly, CIPP/E**, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

***Caroline Doulcet** of the French law firm Cabinet Gelly can be reached at cd@pascalegelly.com.*

Global Privacy Dispatches

FRANCE—CNIL certification process released


By Pascale Gelly, CIPP/E, and Caroline Doulcet

Since 2004, the CNIL has been entitled by the French Data Protection Act to grant seals—labels for products and methods of personal data processing designed in compliance with data protection law. The process must be initiated at the request of professional organisations and institutions.

But the certification process still had to be specified by the CNIL to make the data protection seal effective.

The long-awaited CNIL decision was published in September. It modifies the CNIL's internal rules to determine the data protection seal process.

- A data protection seal committee is created within the CNIL to provide guidelines concerning the data protection certification; to establish the criteria required to obtain a data protection seal, and to evaluate the compliance of products and processes with these criteria
- The creation of a data protection seal can be requested only by a professional organisation or an institution. Such seal will be created if the CNIL deems that it is appropriate for the commission to do so. If such is the case, the CNIL will define the criteria that a product or process must follow to obtain the seal ("*référentiel*");
- Once the criteria have been determined for a type of product or process, a reference document is issued. Products and processes for which it is claimed for the benefit of the seal must follow a procedure of evaluation of compliance with the reference document.
    - An application for a data protection seal can be filed by a single entity or by several entities if the use of the product or process will be gathered by these entities. In this last case, the application must include the commitment of each of these entities to maintain their collaboration for the duration of the seal.
    - The application must include a description of the product or the process and its data protection objectives or guarantees.
    - The CNIL analyses the admissibility of the application within two months and, in principle, communicates its decision to the applicant. Silence within these two months means that the application is rejected (e.g. the application does not contain all the information required).
    - If the application is considered admissible, then the CNIL analyses whether the product or process complies with the criteria of the data protection seal. To do so, the CNIL can submit the product/process to certain tests; ask for the communication of any useful document, or interview any person entitled to provide useful information on the product/process concerned.

- The CNIL takes its decision to grant or not grant the data protection seal in plenary assembly. The decision is based on a report issued at the end of the appraisal process.
- The decision of the CNIL—whether positive or negative—is communicated to the applicant within eight days of the plenary assembly.
- When the data protection seal is granted, the CNIL specifies the conditions of use of the "CNIL seal" by the concerned entity.

The data protection seal is granted for three years and is renewable. Renewal is not automatic. The concerned entity must apply for a renewal six months before the end of these three years.

The data protection seal may be withdrawn if the CNIL gains knowledge of the fact that the product or process is no longer compliant with the criteria of the concerned data protection seal. In such a case, the CNIL notifies the concerned entity, which has one month to take corrective action. If it fails to do so, the data protection seal is withdrawn.

***Pascale Gelly, CIPP/E**, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

***Caroline Doulcet** of the French law firm Cabinet Gelly can be reached at cd@pascalegelly.com.*

Global Privacy Dispatches

FRANCE—Limits to e-mail monitoring


By Pascale Gelly, CIPP/E, and Caroline Doulcet

Employees' rights to privacy in the workplace were reaffirmed by the Supreme Court on 5 July 2011. The decision brings limits to the monitoring of employees' professional e-mailboxes.

A manager of an insurance company was dismissed for having intimate correspondence with another employee and for storing private messages with erotic pictures attached on his professional e-mailbox. The employer argued that the employee knew that these e-mails and attachments would be seen by his assistant and that exchanging personal e-mails within the company's infrastructure was prohibited by internal rules.

Contrary to the Labor Court, the Court of appeal considered the dismissal invalid and sentenced the employer to pay damages to the dismissed employee.

The Supreme Court confirmed the decision of the Court of appeal, pointing out that if a file (it seems the term "file" was used to cover private e-mails and erotic pictures stored on the professional mailbox, as it was the case in the dismissal letter) not expressly flagged as "private" can be opened by the employer, its contents cannot be used against the employee if it appears that it is private.

The Supreme Court decided that the employer's use of private e-mails and erotic pictures stored on the professional mailbox of an employee violates the employee's right to privacy in the workplace.

In this case, the Supreme Court stressed some important facts—the litigious e-mails and erotic pictures attached had been sent by another employee; the dismissed employee had only stored them in the e-mailbox. He did not share them with anyone or record them on the hard drive of his computer.

***Pascale Gelly, CIPP/E**, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

***Caroline Doulcet** of the French law firm Cabinet Gelly can be reached at cd@pascalegelly.com.*

Global Privacy Dispatches

FRANCE—Online national directory sanctioned for indexing links to social network profiles


By Pascale Gelly, CIPP/E, and Caroline Doulcet

In what appears to be a landmark decision, the data protection authority on September 21 sanctioned the Yellow Pages company for having made available a "webcrawl" functionality along with its usual white pages online directory. This service, which has been suspended, linked the search results made on the white pages with the profiles of the concerned individuals found on social networks and sites like Facebook, LinkedIn, Twitter, Copains'd'avant and others.

A large portion of the 65-million member French society—25 million individuals—including minors and unlisted people—were affected.

The CNIL determined that the activity consisted of an unfair collection of data, as the individuals—especially minors and those not listed—could not be deemed as having knowingly provided their data to the social networks so that it could be used to add value to an online directory.

The privacy notice put on the white pages site did not convince the authority, since it was read by the user of the site doing a search rather than by the people whose names appear in the directory.

The CNIL agreed that the individuals could have been properly informed by the terms and conditions of the social networks. However, the Yellow Pages cannot rely on Facebook terms, which refer to the possibility for profiles to be indexed by third-party search engines. The CNIL is of the opinion that the site is primarily a directory, not a search engine, and that Facebook's terms do not meet the French law's notice requirements.

The data controller had reached an agreement with one of the social networks, TROMBI, so that they added a specific notice on their site, which led the CNIL to the conclusion that providing notice to individuals did not trigger disproportionate efforts.

Among other non-compliances, the CNIL noted that the linked profiles were often outdated—80 percent of Facebook profiles had not been updated for more than four months—and that it was very burdensome for individuals to exercise their rights of rectification and objection.

***Pascale Gelly, CIPP/E**, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

***Caroline Doulcet** of the French law firm Cabinet Gelly can be reached at cd@pascalegelly.com.*

Global Privacy Dispatches

FRANCE—The French Cookie Rule


By Pascale Gelly, CIPP/E, and Caroline Doulcet

The cookie directive was implemented by Ordinance n°2011-1012 of 24 August, 2011, issued by the French government. This ordinance amends the French Data Protection Act.

The Ordinance n°2011-1012 states that cookies (except the ones used only to enable or facilitate the carrying out of the transmission of an electronic communication or which are strictly necessary to provide an online communication service explicitly requested by the Internet user) can be used only if the subscriber or user of an electronic communication service

- has been provided with information concerning the purpose of the cookie or of any similar technology and of the means at his disposal to object to such use and
- has "expressed" his consent after having received the aforementioned information. This consent can result from the "appropriate" settings of his browser or of any other system under his control.

Neither the ordinance nor the French Data Protection Act provide a definition of consent. Hence the ongoing debates about whether consent must be express or can be implied based on inaction (i.e. leave the browser settings as they are) and whether the browser settings accepting or refusing ALL cookies at a time are sufficient to express a valid consent.

The Article 29 Working Party made its position clear in its opinion WP 187 of 13 July 2011, in referring to the definition of consent of the Directive 95/46/EC as a freely given, specific, informed indication of the wish of the data subject to agree to the use of her personal data. It pointed out that the notion of "indication"

- should be interpreted as a kind of signal sufficiently clear to indicate the wish of a data subject and to be understandable by the data controller;
- indicates that an action is needed to express consent and that the absence of behaviour or a passive behaviour cannot be an "indication" among others for browser settings.

The G29 also considered that to be specific, consent must refer clearly and precisely to the scope and consequences of the data processing for which it is given. Moreover, it stressed that consent should be "unambiguous" to legitimize a data processing.

The text of the French ordinance provides us with a few indications. It is stated that the user must have "expressed" his/her consent. An "expression" being an indication resulting from a behaviour, it could mean that consent should result from a positive action. The text also provides that the consent may result from browser

settings. However, these settings must be "appropriate." This precision may signify that consent should not be general but specific (i.e. by taking into account the purpose of cookies).

On this last point, the CNIL has expressed its views in a press release of 19 September. It is of the opinion that the consent of an Internet user must be specific, in compliance with the Directive 95/46/EC and that the use of browser settings accepting all cookies—whatever their purpose—cannot be considered as a valid consent.

Implementing regulations are expected before the end of the year to hopefully clarify the debate.

***Pascale Gelly, CIPP/E**, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

***Caroline Doulcet** of the French law firm Cabinet Gelly can be reached at cd@pascalegelly.com.*