# Information Security Breaches & The Law

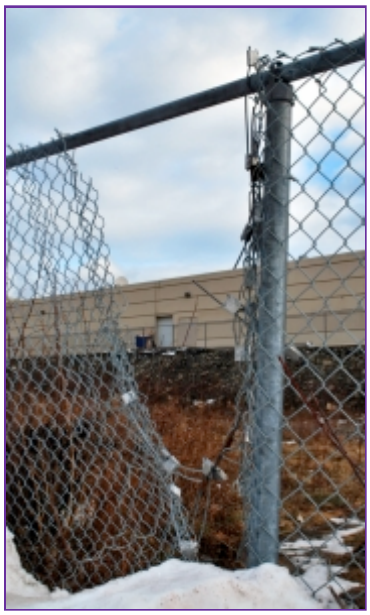
Type here and press enter t

- Home
- About »
- "Security Breaches" Library

## Will France adopt a law requiring the notification of security breaches?

Posted by "Security Breaches" Administrator on 06/08/2010 · Leave a Comment

A bill "*to better guarantee the right to privacy in the digital age*", was presented on November 6, 2009 to the French Senate by two senators, Yves Détraigne and Anne-Marie Escoffier. It was adopted by the Senate, then sent to the National Assembly, France's lower Chamber, on March 24, 2010. (History of the bill) Debates should resume in the Fall.



"Security Breach" (Armdale, Halifax, Nova Scotia, Canada) - Photo by: meddygarnet (2010)

### A bill that implements Directive 2009/136/EC

This bill anticipated the publication on November 25, 2009 of Directive 2009/136/EC amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the

electronic communications sector which added a duty (article 2 (4)(c)) to declare a personal data breach to "the competent national authority" and to the persons likely to be adversely affected by this breach, at least if this breach is *"likely to adversely affect the[ir] personal data or privacy."*

> *"In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.*
>
> *When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay."* (Article 2 (4)(c))

This Directive must be implemented by EU Member States by May 25, 2010. (Article 4 of the Directive.)

The current version of article 7 of the French bill amends article 34 of Act n° 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties, which is France's data protection act ("French Data Protection Act") and makes it mandatory for the data controller to inform the "Data Protection Correspondent" (a person within an organization who could be the controller or assisting the controller), or in the absence thereof, the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés ("C.N.I.L."), of the breach of integrity or confidentiality of such treatment. However, it would not be mandatory to notify individuals affected by the breach, if the data treatment has been authorized by article 26 of the French Data Protection Act, regulating law-enforcement databases.

> *"The data controller implements every appropriate measures, given the nature of data and risks of treatment, to ensure data security and particularly to protect processed personal data against any violation leading to an accidental or unlawful destruction, loss, alteration, disclosure, dissemination, storage, treatment or unauthorized or illegal access.*
>
> *In case of a breach in processed personal data, the controller promptly notifies the "Data Protection Correspondent" or, in the absence thereof, the Commission Nationale de l'Informatique et des Libertés. The controller, in conjunction with the "Data Protection Correspondent" immediately takes all necessary measures to restore the protection of data integrity and confidentiality. The "Data Protection Correspondent" informs the Commission Nationale de l'Informatique et des Libertés about the breach. If the violation has affected the personal data of one or more persons, the controller also notifies those persons, unless this treatment has been authorized under Article 26. The content, form and how the information is disclosed is determined by an Order of the Conseil d'Etat (France's higher administrative Court) after advice taken from the Commission Nationale de l'Informatique et des Libertés. An inventory of all data security incidents is maintained by the 'Data Protection Correspondent'."*

Article 34 of the French Data Protection Act currently in force merely states that:

> *"the data controller shall take all useful precautions, with regard to the nature of the*

> *data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties."*

The data controller has a safety duty, but not a duty to notify about security breaches.

**The bill does not specify how to verify data security**

According to the report Christian Cointat wrote on behalf of the Senate Judiciary Committee, the purpose of the breach notification requirement, which is new under French law, is to encourage the controllers to implement appropriate safeguards (p. 16). This is no easy task: the information report written by senators Yves Détraigne and Anne-Marie Escoffier and published in May 2009, noted that "*data security* ***is in practice difficult to verify****, unless one controls each security system through security attack-tests*" (p. 99) (emphasis in the original text).

However, while data security is *"difficult to verify,"* the bill does not specify what measures might be appropriate to protect it. The deliberation of the CNIL n° 81-94 of July 21, 1981 relating to general measures for computer system security recommended the establishment of such safety measures:

1. Risk assessment as well as a systematic and comprehensive study of data safety for all treatments**;**
2. Efforts to inform and raise awareness among relevant professional groups in order to encourage participation in the implementation of security measures;
3. Very well defined provisions to ensure the security and confidentiality of treatments and information must be included in a reference document regularly updated and constantly monitored for compliance;
4. A clear definition of responsibilities of personnel involved in compliance with safety measures.

**The bill does not provide for a legal obligation to guarantee data security by contract**

These security measures must also be implemented, according to the CNIL, after

> *"consultation among governments, professional groups, users, builders, engineering firms and hardware and software suppliers in order to clarify which safety measures are being offered, whether they are guaranteed by contract, and to work towards a general improvement in security, which must be taken into account when designing software or hardware products."*

We regret that data security measures taken by companies are not always clearly brought to the attention of users and customers. This is particularly regrettable since the CNIL recommended as early as 1981 that such measures be contractually guaranteed. Indeed, Recital 25 of Directive 2009/136/EC states that

> *"without imposing any obligation on the provider to take action over and above what is required under Community law, the customer contract should also specify the type of action, if any, the provider might take in case of security or integrity incidents, threats or vulnerabilities*." (p. 14)

**The bill provides for a compulsory notification of security breaches to individuals**

The original bill presented in November 2009 only gave the CNIL the power to require the controller to give notice to those affected by this attack, "*if this attack is likely to affect the personal data of one or more individuals.*"

The bill was amended during the parliamentary proceedings in the Senate, and its article 7 now imposes on the controller a requirement to notify individuals whose personal data may have been compromised by a data security breach, unless it is a law-enforcement database, as authorized by article 26 of the French Data Protection Act.

The first law requiring notification of data breaches, the California Security Breach Notification Act, which came into force in July 2003, made it compulsory to provide notification of security breaches to consumers residing in California and affected by them. The law does not require notification to an administrative authority such as the CNIL, even though California has had a government agency since 2000 dedicated to the protection of consumer privacy, the California Office of Privacy Protection.

> *"Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.*" Cal. Civ. Code § 1798.29(a)

**The bill also follows the recommendation of Directive 2009/136/EC to notify individuals of security breaches for all sectors, not only the sector of electronic communications**

Section 2 (4)(c) of Directive 2009/136/EC provides an obligation for the controller to inform the subscriber or individual affected by a breach of personal data if such infringement is *"is likely to adversely affect the personal data or privacy of a subscriber or individual."* The scope of this Directive, however, only concerns providers of electronic communications services accessible to the public.

Yet this is a matter of general interest. Recital 59 of Directive 2009/136/EC expresses regret that the requirements for notification of breaches of personal data contained in the Directive 2002/58/EC

> *"are limited to security breaches which occur in the electronic communications sector*" since *"the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised. (…) The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority*."

Therefore, pursuant to Recital 59,

> *"the Commission (…) should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC, regardless of the sector, or the*

> *type, of data concerned."*

This recommendation appears to have been heard by the French legislature. Senator Christian Cointat's report stresses the need to promote the dissemination of an "IT and freedom" culture, one element of which would be to make notification of security breaches compulsory, regardless of the sector or the type of data involved in the breach, with the exception of data contained in law enforcement databases (p. 16).

**Conclusion**

An amendment to the bill introduced in February 2010 in the Senate by the Government proposed to completely delete its article 7. The government argued that article 7 does not fully implement Directive 2009/136/EC. Indeed, according to the French government, article 7 does not implement the Directive's provisions regarding the penalties that might be brought against the controller who did not inform the persons concerned by the security breach, nor the provisions regarding the requirement for the controller to keep an inventory of the personal data breaches he has found. This inventory requirement was passed by the Senate, but the Senate did not, however, vote for the complete deletion of article 7.

We add that the bill does not implement the provision of Article 2 (4)(c) of Directive 2009/136/EC, which provides that it is not necessary for the provider to notify the subscriber of a breach of personal data if the provider

> *"has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it."*

It will be interesting to follow up how this bill is discussed before the National Assembly in the Fall, provided that the debates make it on to the Assembly's calendar.

**Marie-Andrée Weiss & Cédric Laurant**

(The French version of this article is available here.)



Filed under Comments, ENGLISH · Tagged with security breach notification, United States, security breach, personal data, contractual clauses, unauthorized access, data security, data controller, data confidentiality, France, Commission nationale de l'informatique et des libertés, data breach, California Security Breach Notification Act, California, California Office of Privacy Protection, French National Assembly, French Senate, data protection correspondent, general IT security measures, EU Directive 2009/136/EC, French Data Protection Act, French Data Protection Authority, EU Directive 2002/58/EC, contract, technological protection measures, CNIL deliberation No. 81-94 of July 21 1981, Act No. 78-17 of January 6 1978, Act on Data Processing Data Files and Individual Liberties

La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?

## Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <pre> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

Notify me of follow-up comments via email.

Subscribe by email to this site

- **Recent Posts**
  - Will France adopt a law requiring the notification of security breaches?
  - La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive
  - Are 'clouds' located outside the European Union unlawful?
  - The Safe Harbor Framework: not a "safe harbor" anymore for US companies? German expert body insists on stronger compliance stance
- **Recent News on Security Breaches**
  - "Consumer View: Staying Safe from Cyber Snoops" (FCC, June 11, 2010) Recent news

reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers' private data accessible. (…)

- "Sécurité des données personnelles : les entreprises ne font pas face" (ITR News, 9 juin 2010) L'étude souligne le fait que, en dépit de ce que croient beaucoup d'entreprises, le fait de respecter la réglementation en vigueur ne suffit pas à assurer une protection efficace des données. En effet, alors que 70 % des sondés affirment (…)
- "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program" (FTC, June 24, 2010) The FTC's complaint against Twitter charges that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had (…)
- "UK headed for data breach disclosure law within four years" (siliconcom, July 16, 2010) "According to lawyers at law firm Field Fisher Waterhouse, legislation requiring organisations to notify the relevant authorities as well as individuals affected in the event of a serious security breach will be introduced across Europe."
- "Survey: 87 per cent of UK businesses favour mandatory disclosure of data breaches" (Secure Business Intelligence, July 6, 2010) 87 per cent of organisations believe that data breaches should be revealed when sensitive data about the public is exposed. Revealed, but to whom?
- "Putting a Private Detective in Your Laptop" (New York Times, June 16, 2010) "According to a study by the Ponemon Institute, 12,000 laptops are lost each week in American airports (…) You can keep an eye on your devices and not leave them visible and unattended, but they might best be protected with some software."
- "Credit Card Hackers Visit Hotels All Too Often" (New York Times, July 5, 2010) Hotels are a favorite target of hackers. A study released this year by data-security consulting company SpiderLabs found that "38 % of the credit card hacking cases last year involved the hotel industry".
- Ponemon Institute: First Annual Cost of Cyber Crime Study (ArcSight, July 26, 2010) "The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount (…
- Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (FTC, July 27, 2010) "The FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash that contained consumers' personal information such as pharmacy labels and job applications. (…)
- Data Breaches Easy To Avoid, Report Finds (eWeek Europe, July 28, 2010) "Data breaches are on the decline with the overall number of breaches investigated last year down from the previous year. This is according to…Verizon's 2010 Data Breach Investigations Report, in collaboration with the US Secret Services."

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 California Office of Privacy Protection California Security Breach Notification Act Canada cloud computing Commission nationale de l'informatique et des libertés confidentiality contractual clauses data breach notification statute data controller data security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities European Union external audit Facebook France German Federal Data Protection Act Germany identity theft integrity material breach personal data PIPEDA preemption Privacy Commissioner of Canada Safe Harbor Framework Safe Harbor self-certification security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Blog Authors**
  - 

  - 
  - 
- **Disclaimer & Comments Policy**
  - Disclaimer & Comments Policy
- **Authors' upcoming talks & conferences on information security & legal issues**
  - Cédric Laurant: II Congresso Crimes Eletrônicos e formas de proteção (2nd Congress on Cybercrimes and Protection Measures) Federação do Comércio do Estado de São Paulo

(Sao Paulo Chamber of Commerce), Sao Paulo, Brazil – Sept. 27-28, 2010
- Cédric Laurant: "Legal Developments and Relevant Court Decisions in Latin America" High Technology Crime Investigation Association (HTCIA) International Conference (Atlanta, GA-USA – Sept. 20-22, 2010)

- **Tweets (last 10)**

  - Will France adopt a law requiring the notification of #security_breaches? New blog posting http://bit.ly/cyZcC2 #in - tweeted 15 minutes ago
  - "La France va-t-elle se doter d'1 loi rendant obligatoire les notifications des violations de sécur.?" New blog posting http://bit.ly/9DJS36 - tweeted 2 days ago
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 1 week ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 1 week ago
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive. New blog posting at http://bit.ly/aOG3cY #in - tweeted 2 weeks ago
  - "Are 'clouds' located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 2 weeks ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog posting. http://lnkd.in/ShwMWj - tweeted 3 weeks ago
  - "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 3 weeks ago
  - FTC's proposed consent agreement with #Twitter: company misrepresented its security measures. http://bit.ly/cF8LNk - tweeted 1 month ago
  - Your "private" tweets are... public! #Twitter prone to security breaches, FTC says in consent agrmt. Com'ts requested. http://bit.ly/axKpnV - tweeted 1 month ago

- **Subscribe to this blog by e-mail**

  Enter your e-mail address here to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!

- 

- **Counters**

- 


Information Security Breaches & The Law ·

Blog at WordPress.com. Theme: Structure by Organic Themes.