BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Data Breaches

Legislation

A draft ''Law to Better Guarantee the Right to Privacy in the Digital Age,'' which has been submitted to the French Senate (8 PVLR 1685, 11/23/09), is scheduled to be reviewed in the coming months by an internal committee before being put to a vote in the full assembly of senators. Among other things it would clearly identify an internet protocol address as personal data, create an obligation to notify the French data protection authority of data breaches, and impose data security requirements. It would double monetary penalties for violations of the Data Protection Act and would require data controllers to obtain the prior consent of data subjects for data processing, including the use of cookies, except if a legal exception applies. The measure is likely to be amended, but there is a clear indication that privacy and data protection are on the political agenda in France, meaning that the measure could possibly be enacted in 2010, the author writes.

French Senate Proposes Amendments to the Data Protection Act

BY OLIVIER PROUST

Olivier Proust, of Hunton & Williams LLP in Brussels, is a member of the Paris Bar. He can be reached at oproust@hunton.com.

Introduction

On Nov. 6, French senators Yves Détraigne and Anne-Marie Escoffier submitted to the Senate a draft proposal for a ''Law to Better Guarantee the Right to Privacy in the Digital Age.''[1] This bill aims to reinforce the protection of privacy by introducing new

 ISSN 1538-3423

provisions to the Data Protection Act.[2] It follows a report[3] on the same topic issued earlier this year by the Senate, which observes that in recent years the right to privacy has been confronted with the development of ''new digital memories.'' Owing to fast advances in various technologies (e.g., Bluetooth, RFID, GPS, nanotechnologies), individuals nowadays can be easily tracked and traced in time and space, which poses new threats to the right to privacy. Should this new bill be adopted by the French Parliament, the proposed changes would have an impact on the data processing activities of organizations and on their duty to comply with data protection requirements.

Clarification of the definition of personal data

The bill would clarify the definition of personal data by introducing a new paragraph under its current definition, stating that in particular, personal data constitutes ''any address or number identifying a terminal equipment connected to a network.'' The purpose of this paragraph would be to clearly identify an internet protocol (IP) address as personal data. Despite recent court decisions in France against the recognition of an IP address as personal data,[4] the Senate considers that an IP address is undoubtedly a means of identifying indirectly internet users, like a telephone number or a postal address. Traffic data (including IP addresses) would thus be treated in the same way under data protection law as any other category of personal data.

Increasing obligations for data controllers

Obligation to appoint a DPO in large organizations

An important change in the proposed bill would require large organizations in which more than 50 employees have access to, or process, personal data to appoint a data protection officer (DPO). Recent statistics published by the French Data Protection Authority (CNIL)[5] indicate that over 5,000 organizations, mainly in the private sector, have appointed a DPO since the measure was introduced in France in 2004.[6] The appointment of a DPO exonerates organizations from having to notify the CNIL of their data processing activities. [7]. Furthermore, a DPO develops a ''privacy culture'' within organizations and raises the level of compliance with privacy and data protection requirements. Indeed, the bill states that a DPO is in charge of ''ensuring independently compliance with the provisions of the law and of informing all the people working for the organization of the necessity to protect personal data.'' Organizations appointing a DPO must notify the CNIL and the Works Council. The DPO must also maintain a list of the data processing activities that are carried out by the organization, which is kept available to any person requesting access to this list.

Obligation to notify the CNIL in case of data security breach, data security requirements

The proposed bill would specify the existing obligation for data controllers to implement adequate security measures to protect the security and confidentiality of personal data. Article 34 of the French Data Protection Act, in its current wording, states that the data controller must take ''useful precautions'' to preserve the security of the data. Under the proposed wording of the bill, this article would state that ''data controllers must implement adequate measures, with regard to the nature of the data and the risks of the data processing, to preserve the security of the data, in particular to protect the data processed against any breach accidentally or unlawfully causing the destruction, loss, alteration, disclosure, communication, storage, processing or unauthorized access to personal data, particularly when the processing contains transmissions of data over a network, as well as any other unlawful form of processing.''

In addition, in case of a data security breach, data controllers would have to notify the CNIL of this breach ''without delay.'' If the breach is likely to impact the personal data of one or more individuals, the CNIL may require the data controller to notify these individuals as well. The content, form and conditions of this notification would be further explained in an implementing decree adopted by the State Council (''Conseil d'Etat'') following an opinion rendered by the CNIL. This new measure would therefore anticipate implementation of the data security breach requirements contained in the ePrivacy Directive.[8] However, it would go beyond the ePrivacy Directive, which only covers breach notifications for telecommunications companies and internet service providers.

Reinforced rights of the data subjects

More transparency of the data processing activities

The proposed bill would require data controllers to provide notice to the data subjects of their data process-

[1] ''Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique,'' submitted by Yves Détraigne and Anne-Marie Escoffier, senators, recorded by the Senate Presidency on Nov. 6, is available, in French, at http://www.senat.fr/leg/ppl09-093.html.

[2] Act n°78-17 of Jan. 6, 1978 regarding data processing, data files and individual liberties, available in French at http://www.cnil.fr/index.php?id=45

[3] Report on ''The Right to Privacy in the Age of Digital Memories,'' by Yves Détraigne and Anne-Marie Escoffier, May 27, 2009, available in French at http://www.senat.fr/noticerap/2008/r08-441-notice.html.

[4] See for example, Paris Court of Appeal, April 27, 2007, Anthony G. / SCPP; Paris Court of Appeal, May 15, 2007, Henri S. / SCPP.

[5] See CNIL, ''Les CIL franchissent le cap des 5000,'' press release of Nov. 23, 2009, which is available, in French, at http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/les-cil-franchissent-le-cap-des-5000/.

[6] Act n°2004-801 of Aug. 6, 2004, implementing Directive 95/46/EC of Oct. 24, 1995, available at http://www.legifrance.gouv.fr/./affichTexte.do?cidTexte=JORFTEXT000000441676&fastPos=1&fastReqid=1077588629&categorieLien=id&oldAction=rechTexte.

[7] Please note that appointing a DPO does not exonerate a data controller from his or her obligation to notify the CNIL about activities requiring the prior approval of the CNIL, including data transfers, as stated under Article 22-III of the Data Protection Act.

[8] Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing or personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, approved on Oct. 22, 2009, available at http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML.

   ISSN 1538-3423

ing activities in a ''clear, specific and easily accessible manner,'' prior to carrying out these activities. This means, for example, that organizations would be legally required to post a privacy notice on their websites. The content of this notice would have to be more detailed than what is currently required, since data controllers would have to inform their data subjects about the period of retention for personal data and to clearly identify the contact information so as to enable data subjects to exercise their rights. Data controllers would also have to obtain the prior consent of their data subjects for any data processing activity (including the use of cookies), except if a legal exception applies (e.g., legal requirement, performance of a contract to which the data subject is party, pursuit of a legitimate interest, etc.).[9]

Easier exercise of the data subjects' rights

The proposed bill also aims to facilitate the data subjects' right to object to data processing activities. With a view to clarifying the current wording of the Data Protection Act, the Senate proposes to distinguish between a data subject's right to object to the collection of his/her personal data for commercial purposes and his/her right to request the deletion of personal data, based on legitimate grounds, after the data was processed. The proposed bill would also enable the data subjects to exercise these rights more easily, including by electronic means (e.g., e-mail). Finally, the data subjects would have the right to better understand the purposes of a data processing activity, including to obtain information about the origin of the data processed.

Facilitated civil right of action

In order to facilitate civil actions, the proposed bill would enable the data subjects to file a lawsuit before the civil court in the jurisdiction of their place of residence, as opposed to the place of establishment of the data controller. Therefore, the data subjects would have better access to the judicial system and would be able to defend their rights in court more easily, similar to what is already permitted under consumer protection law.

Stronger enforcement powers for the CNIL

Heavier fines

Under the current law, the CNIL can impose a maximum fine of €150,000 ($215,117) for a violation of the Data Protection Act, or €300,000 ($430,248) in case of a second violation within five years of the first sanction.[10] The Senate's bill proposes to double these thresholds by bringing them respectively to €300,000 ($430,248) and €600,000 ($860,450). The Senate hopes that this will encourage the CNIL to impose harsher sanctions, similar to those pronounced by the Spanish Data Protection Authority.

Intervention in court proceedings

The bill also proposes to enable the CNIL to publish its decisions and penalties regularly, and not only in case of bad faith of the data controller, as it is currently the case[11]. The hearings of the CNIL's restricted committee would also be open to the public, which would establish the CNIL more formally as a judicial body, according to the Senate. In addition, the law currently gives the CNIL the power to refer any violation of the Data Protection Act to the public prosecutor or to render an opinion upon request of a court.[12] The proposed bill would supplement these provisions, granting the CNIL the additional right to produce written observations or to be heard spontaneously in any civil, administrative and criminal court hearing.

Conclusion

In the upcoming months, the proposed bill is due to be reviewed by an internal committee of the French Senate before being put to the vote in the full assembly of senators. During the parliamentary process, the bill is likely to be amended, making it difficult to assess which provisions are most likely to be adopted, if at all. However, there is a clear indication that privacy and data protection are currently on the political agenda in France, meaning that this new law could possibly be enacted in the course of 2010. Organizations may therefore consider that now is a good time to act proactively and to make the structural changes that are necessary to comply with the law.

---

[9] Article 7 of the Data Protection Act.

[10] Article 47 of the Data Protection Act.

[11] Pursuant to Article 46 of the Data Protection Act ''the Commission [CNIL] may make public the warnings that it issues. It may also, in case of bad faith on the part of the data controller, order the publication of any other penalties imposed, in such publications, newspapers or other media as it designates.''

[12] Article 40 of the Criminal Procedure Code.