While there have been a number of administrative rulings from the French Data Protection Authority (the “CNIL”) in 2012, the most significant is that the entry into force of data breach notification rules for providers of publicly available electronic communications services. Decree n°2012-436 of March 30, 2012 (the “Decree”) implements the amended e-Privacy Directive (Directive 2009/136/EC amending Directive 2002/58/EC), which had previously been made by the Ordinance of August 24, 2011, amending Section 34 of the French Data Protection Act of January 6, 1978. The CNIL also provided guidance on compliance with these new rules (see http://www.cnil.fr/dossiers/internet-telephonie/telecom-pratique/article/la-notification-des-violations-de-donnees-a-caractere-personnel/).

Under the new notification rules, providers of publicly available electronic communication services (such as internet service providers and telecom operators) must notify the CNIL of “any breach of security leading accidentally or unlawfully to the destruction, loss and alteration, disclosure or unauthorized access to personal data, processed in the context of providing electronic communication services to the public” without delay.

Importantly, there is no de minimis threshold that would exclude minor or less serious breaches from the notification obligation.

The new requirements only apply to information breaches that arise while a telecoms provider is providing electronic communication services. So while the breach of an HR database located in the cloud could give rise to notification and liability under the rules, the breach of the same database on the employer's internal servers would not give rise to a notification obligation to the employer under the statute. Indeed, unlike the case in other EU countries, there is no notification requirement for general data breaches under the Decree.

The breach must involve personal data, such as a breach of an ISP’s customer database containing customer email addresses or billing information, or breaches of a mobile operator’s online store for customer credit card numbers.

The notification must be made by registered mail addressed to the CNIL. The provider must specify the type of data breach and the consequences flowing from the breach, including an estimate of the number of people affected by the breach and the remedial steps proposed to remedy the breach.

Also, the provider must provide details of protective measures, such as encryption, applied to the data and estimate of the impact of the data.
New EU Rules on e-Invoicing in Effect

By Katherine Jonckheere, Associate, Lorenz

Will this be the year for electronic invoicing – or e-invoicing – in Europe? As of January 1, 2013 all EU countries must comply with the provisions set forth in Council Directive 2010/45/EU on invoicing rules (the "Directive"). Although e-invoicing is nothing new, its adoption has remained sluggish with an estimated 5% of all invoices between businesses in the EU being exchanged electronically. The new Directive aims to simplify invoicing rules throughout Europe in an attempt to help businesses reduce costs and increase competitiveness. Its transposition into national legislation is a key action point under the Digital Agenda for Europe, a flagship initiative for the ‘Europe 2020’ growth strategy.

One of the foremost changes brought by the Directive is that paper and electronic invoices are now to be afforded the same legal status. It follows that previous requirements for electronic invoicing imposed by national legislators such as the mandatory use of an advanced electronic signature or Electronic Data Interchange (“EDI”) are no longer valid. From now on, businesses can decide for themselves how to ensure the invoice’s authenticity, integrity and legibility from the moment of issuance to the end of the archiving period. While this may still be achieved through the use of the aforementioned technologies, a broader range of solutions and protocols will now be considered as lawful; a simple email with a PDF attached should do the trick.

This is certainly good news for SMEs – e-commerce businesses especially – since they can now choose what best works for them and move towards more automated business processes with greater ease. One notable barrier to the widespread adoption of e-invoices remains though, in the requirement by which the use of electronic invoicing is subject to acceptance – implicit or explicit – by the recipient. It is justified by the technical means needed to receive an electronic invoice; much unlike the ubiquitous postal address, individuals and companies are not (yet) required to register an email address for the purpose of official correspondence.

The Directive stipulates that the European Commission shall present by the end of 2016 an overall assessment report on the impact of the new invoicing rules. By then, the requirement of customer acceptance may well return to the discussion table.

Endnotes:
4 Ibid.

Brazil's New Law is Not Tough Enough to Fight Electronic Crimes

By Professor Renato Opice Blum - Attorney, Economist and President of the IT Advisory Board of Fecomercio

After fifteen years of discussion, Brazil’s government has enacted a law that typifies computer-related crimes and covers important issues such as electronic device invasion, unauthorized remote access and interruption of web services. This article analyzes some aspects of the long-awaited Law 12.737/2012.

The law limits the characterization of device invasion to cases in which an “infringement of security mechanisms” occurs, excluding computer devices without protection mechanisms from the enforcement. Moreover, “security mechanism” and “computer device” (only hardware, what about software?) are not defined by the law, raising doubts about the legal framework in certain cases.

See, Brazil's New Law Not Tough Enough, page 3
New Data Breach Notification Obligations

breach on the affected individuals. With this information, the CNIL will assess whether the security and remedial measures are “appropriate” in light of the gravity of the data breach. If the CNIL notifies the provider that the security measures are inappropriate, or if the CNIL fails to respond within two months of the filing, the provider will be required to notify the individuals affected by the breach.

The CNIL may require that the provider notify affected individuals directly in the event of a “serious breach”. The notification must specify the nature of the data breach and the provider must recommend specific measures designed to reduce the adverse consequences of the data breach on the affected individuals.

Non-compliance can result in the following criminal sanctions: five years imprisonment and/or a 300,000 euro fine.

Brazil's New Law Not Tough Enough

Furthermore, since the conduct “to invade” gives the idea of “entering forcefully”, cases of inappropriate acquisition of data through social engineering techniques and other means (e.g. disclosure of password by the owner to third parties) theoretically would not be included in the newly born classification. This is because such actions would not constitute violation, but merely unauthorized access.

Additionally, it is possible to foresee a broad debate about who would be the “owner of the dispositive” invaded – expression used to designate the victim. The legal text seems to refer only to the owner, not clarifying if an eventual possessor or user could also be protected.

It is also important to mention that, concerning the penalization of disclosure of industrial secrets obtained by invasion, there is an apparent duplicity of legal prediction: the improper disclosure was already considered crime by the Protection of Industrial Property Law (Law 9.279/96).

The new law comprises many other interesting topics, however the sentences imposed appear to be too soft, allowing the enforcement of the conditions of Special Courts’ proceedings. This when the international trend is precisely the opposite: recently it became news the fact that the State of California (USA) condemned to ten years of prison a hacker accused of stealing pictures from celebrities through the web - in addition to the payment of a compensation for the sum of 76,000 U.S. dollars.

Obviously, we are not advocating the sudden increase of Brazil’s prison population just to punish computer crimes. Nevertheless, it is hard to understand how the creation of a law after so many years of debate can establish punishments with such a weak deterrent effect.

For these reasons, it seems lenient to punish such conduct with the concession of benefits directed to minor crimes. If technology achieved a relevant role in the daily life of the Brazilian citizen, the law should follow this change, recognizing in practice its gigantic potential to affect people’s lives – for better or, unfortunately, for worse.
Electronic Eavesdropping by Government v/s Citizens’ Right to Privacy

By Faisal Daudpota Senior Partner, Daudpota International

“The Judge while passing an order for the issuance of warrant shall ensure that ... the issuance of the warrant shall not unduly interfere in the privacy of any person or property”

The above extract from Section 10(2) of the ‘Investigation for Fair Trial Act, 2012’ (IFTA’12), which will soon be signed by the President of Pakistan and will then become a law open to constitutional challenges also, and in my humble view IFTA’12 offends Article 14 (concerning protection of privacy) of Pakistan’s Constitution.

IFTA’12 establishes a compliance regime as to issuance of two kinds of warrants, namely: (1) Warrant of Surveillance, and (2) Warrant of Interception. Both these warrants (surveillance or interception) can be issued by a Judge of a High Court, and shall enable select law enforcement agencies to carry out: (a) Interception and recording of telephonic communication of the suspect with any person, (b) Video recording of any person, persons, premises, event, situation, etc., and (c) Interception, or recording, or obtaining, of any electronic transaction including but not limited to e-mails, SMS, etc.

Unfortunately IFTA’12 does not afford many safeguards to meet the guarantees as to protection of privacy of Pakistan’s citizens under the Constitution and laws of Pakistan. Further, Pakistan’s superior Courts have acknowledged in Riaz v Station House Officer, Police Station Jhang City & Others (PLD 1998 Lahore 35) that, issuance of house search warrant, after all, makes an inroad into the Constitutional guarantee of fundamental right of privacy of the home. Enjoyment of this right, no doubt has been made subject to law; but at the same time it has been described as inviolable.

Provisions of IFTA’12 therefore, have to be read in the backdrop of Article 14 of the Constitution and accordingly cannot frustrate the inviolable guarantee as to privacy as enunciated therein.

EDPS on Financial Services Consumer Protection

By Katherine Woodcock, Senior Associate, Lorenz

On November 23, 2012, the Assistant European Data Protection Supervisor (“Supervisor”) issued an opinion on the data protection issues in a proposed set of financial services laws (“Opinion”).


- the IM Directive, for violations of the consumer protection requirements on insurance intermediaries and insurance undertakings;
- the UCITS Directive, for violators who pursue UCITS activity without proper authorizations (e.g. in cases of fraud or non-notification of key investor information); and
- the KID Regulation, for breaches of the information requirements for investment product disclosures for retail investors.

See, EDPS on Financial Services, page 5
EDPS on Financial Services

The Opinion emphasizes that these publications should be for clear, well-defined purposes. To this end, it outlines that the purposes and necessity of such publications should be clear and that less-intrusive means (e.g. heavier fines or publication on case by case basis in light of the circumstances) should be considered. Additionally, the recommendation suggests that the Proposals be amended to include adequate safeguards, such as publication only after a final adjudication or that the publication includes that the decision is still subject to appeal and that the individual is presumed innocent until the final adjudication. Finally, the Opinion raises serious concerns about these publications being posted on the Internet. It recommends implementing additional safeguards (e.g. protection from public search engines) in light of the risks associated with such publications on the Internet.

Another core issue in the Opinion is the reporting mechanisms that the UCITS Directive and the IM Directive contemplate. Their reporting mechanisms for the breaches outlined above are, in substance, whistle-blowing schemes. The Supervisor recommends that the Directives specifically provide for the protection of the identity of incriminated persons, unless disclosure is required for investigation under national law or subsequent judicial proceedings (e.g. defamation suit by incriminated person).

Interestingly, in the conclusions to the Opinion there is an additional point with regard to obligations by EU member states to implement “appropriate procedures to ensure the right of the accused person”. This specific recommendation was not included in the main section of the Opinion’s recommendations; however it does mention that the Supervisor is happy to see that both the IM Directive and the UCITS Directive includes this requirement – an oversight perhaps?


Upcoming Events: PEDS Committee at the SIL Spring Meeting

Attending the Section of International Law 2013 Spring Meeting?
If so, catch up with the Privacy, E-Commerce and Data Security Committee!

When: April 23-27, 2013
Where: Hyatt Regency Washington on Capitol Hill, Washington DC

Anjli Garg, Co-Chair of the PEDS Committee and Demetrios Eleftheriou, Senior Advisor and former Co-Chair of the PEDS Committee are chairing and speaking on the panel “More Art than Science: Negotiating Global Privacy and Data Security Language”. The panel takes place on Thursday, April 25 from 4:30 pm until 6:00 pm in Lexington.

Other PEDS-relevant panels include:
- “Harmonization of EU laws: The Rocky Road of Integration on Finance, Privacy and Culture”, Tues. April 23, 11:00 am - 12:15 pm in Congressional A.
- “Lost in the Clouds: How Do You Control the Export of Data to Anywhere when It’s Stored Everywhere”, Wed. April 24, 2:30 pm - 4:00 pm in Lexington.
- “Still Lost in the Clouds: Controlling Company Data on Employees’ Personal Devices in the Age of Readily Available Cloud Storage”, Wed. April 24, 4:30 pm - 6:00 pm in Lexington.
- “Social Media in the Workplace: Employer Interests vs Employee Rights”, Wed. April 24, 2:30 pm - 4:00 pm (room TBA).

Please see the full agenda at http://ww4.aievolution.com/aba1301/index.cfm?do=cnt.page&pg=1005
Committee News

W. Gregory Voss, Professor at Toulouse Business School and Vice-Chair of the PEDS Committee, publishes on the Proposed EU General Data Protection Regulation in the ABA’s Business Law Today.

Full text of the article can be found at: http://apps.americanbar.org/buslaw/blt/content/2012/11/article-02-voss.pdf


About the Committee

Mission Statement:

The Privacy, E-Commerce and Data Security Committee has been established as a resource to assist in the education of international law practitioners on the evolving international laws and practices relating to privacy and data protection, in particular as they relate to global e-business, and to contribute to the development of policy and the promotion of the rule of law in those areas.