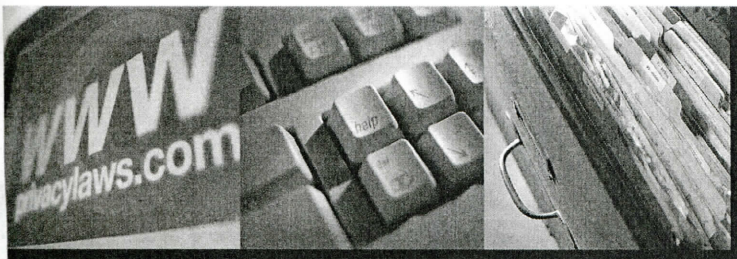

25 YEARS
PL&B ANNIVERSARY
1987-2012

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The US FTC's privacy enforcement role challenged

Company claims that the FTC lacks authority to regulate data security standards. **Robert Belair** and **Kim Phan** discuss.

The Federal Trade Commission (FTC) is the *de facto* US privacy and security regulatory agency. In the past 10 years, the FTC has brought more than 40 separate enforcement actions related to privacy and data security. All of the companies involved in these actions have agreed to settlements.

On 26 June, however, the FTC filed a complaint in a federal district court in Arizona against hotel group Wyndham Worldwide Corporation and three of its subsidiaries (Wyndham)[1] arising from a series of data breaches that may have exposed Wyndham's customers' personal information. Surprisingly, rather than agree to a settlement, Wyndham decided to fight declaring that, "We intend to defend against the FTC's claims vigorously."

This unprecedented litigation challenges the FTC to prove in court

Continued on p.3

Singapore adopts Personal DP Act for the private sector

The Act has so many exemptions, it is only a 'known unknown'. There is no relief for outsourcing, however. **Graham Greenleaf** analyses the Act's scope and principles.

Singapore's legislature enacted the Personal Data Protection Act on 15 October 2012, making it the 10th jurisdiction in Asia to enact a data privacy law. It is the fourth in the ASEAN (Association of South East Asian Nations) region, after Malaysia (2010, but likely to be in force January 2013), the Philippines (enacted and in force 2012) and Vietnam (in force 2011, although limited to the consumer sector). ASEAN has seen the most intense developments in data privacy laws of any part of the world in 2012.

This article explains the scope of Singapore's Act, and its data privacy 'General Rules'. An examination of the Act's enforcement measures will follow in the next issue. The Act also

Continued on p.5

Issue 120 **December 2012**

Yomiuri, 2012). It is expected that a new Bill would undergo some revisions, but those who are close to legislative developments see little reason to expect that any of the above-identified deficiencies will be remedied in the short term. Japan's bureaucratic juggernaut, once set on a path, rarely changes course no matter how compelling the reasons to do so (Kerr, 2001). Japan's data privacy laws are likely to stay in hibernation, and out of touch with global and regional developments for some time to come (Murata and Orito, 2008; Orito and Murata, 2013).

The main glimmers of hope that this situation can be improved from a privacy perspective come from politics and civil society. The expansion of the Jukinet system a decade ago was both a bruising experience for politicians exposed to protests from civil society, and the protesters raised constitutional objections which, although they lost in the Jukinet cases, might be revived on stronger grounds against My Number. However there is no sign of such civil discontent this time.

Implementation of this data matching system also raises the question of whether a country can remain compliant with the OECD privacy Guidelines if it abandons the 'finality' principle (use and disclosure only for the purposes of collection) across such a large part of its public sector, rather than making more specific exceptions to these principles. There are no means of testing this.

AUTHORS

Professor Graham Greenleaf, UNSW and Visiting Fellow, Meiji University, Tokyo, Professor Kiyoshi Murata, Director, Centre for Business Information Ethics (CBIE), Meiji University, Tokyo and Prof essor Andrew Adams, Deputy Director, CBIE. Valuable information has been provided by Prof Fumio Shimpo, but responsibility for content and opinions remains with the authors. This article is also an outcome of the research project Kakenhi (B) 24330127.

Nigeria's Data Protection Bill: Too many surprises

The Bill is likely not to fulfil the adequacy standard of the EU Data Protection Directive. **Alex B. Makulilo** reports.

Over the last ten years there has been a growing trend by African countries to implement comprehensive data protection legislation. Until now eleven countries: Cape Verde, Seychelles, Burkina Faso, Mauritius, Tunisia, Senegal, Morocco, Benin, Angola, Gabon and Ghana have adopted such laws. South Africa is about to pass its legislation on data protection following lengthy deliberation on its Bill. Other countries in Africa with either data privacy Bills or draft Bills include Ivory Coast (Côte d'Ivoire), Kenya, Madagascar, Mali, Niger and Nigeria. As most of the countries which have so far adopted data protection are relatively weak economically and politically, the spotlight will increasingly be put on Nigeria as one of the most economically and politically significant countries in Africa still without a data protection law. It is also significant that Nigeria is a member of the Economic Community of West African States (ECOWAS). As such, it has an obligation to adopt a data protection law in conformity with the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, a sub-regional data privacy framework.

The following analysis identifies some glaring problem areas with Nigeria's Data Protection Bill 2010 (HB.476), tabled in the House of Representatives in 2010, with enactment still pending. My conclusion is that the Bill, with only 12 sections, nevertheless, contains too many surprises which make it a weak standard.

Limited definitions

Some important terminologies and phrases remain undefined, such as "relevant filing system" and "responsible person". Similarly there are terminologies and phrases which, although defined in the interpretation section, are not found within the text of the Bill (e.g. "'sensitive personal data" and "health record"). At the same time the Bill offers certain definitions which are meaningless. For example, "'obtaining' or 'recording', in relation to personal data, includes obtaining or recording the information to be contained in the data". Similarly, "'using' or 'disclosing', in relation to personal data, includes using or disclosing the information contained in the data". The Bill does not define some important terms such as "data processor" and accordingly, no provision in the Bill explicitly covers the activities of data processors in processing personal data.

The Bill's unknown scope

The draft Bill does not state whether it covers the public or private sector or both. The definition of "data controller" in section 10 of the Bill does not either give any indication of such scope. This uncertainty is likely to result in implementation problems. Yet reading the definitions of "personal data" and "data subject" in section 10 of the Bill as well as the explanatory memorandum, it appears that the proposed law is intended to apply to natural persons as it is the case with many pieces of data protection legislation and does not extend to offer protection to legal persons.

Moreover, while most international data protection codes, as well as national legislation, exclude from their application certain types of processing, Nigeria's Bill does not. For example, the Bill does not exclude processing of personal data for public security, defence, state security, activities in the area of criminal law, etc. It also does not exclude processing of personal data by a natural person in personal or household activities. What this means is that creating a list of phone book contacts, for example, may be subject to the Bill.

Perhaps the most interesting point to note is the silence of the Bill on the territorial scope of its application. The Nigerian Bill does not provide protection both for citizens and non-citizens.

Only Nigerian citizens can be afforded constitutional protection for the right to privacy. It is doubtful if the Bill will operationalise the protection of the right to privacy beyond the constitutional limit. This is because under Article 1(3) the Nigerian Constitution is the supreme law and any other law which is inconsistent with its provisions becomes void to the extent of its inconsistency.

WEAKER DATA PROTECTION PRINCIPLES

The Bill contains seven data protection principles roughly similar to those found in international data privacy codes. These principles are stated in Section 1 of the draft Bill: lawful and fair processing, purpose specification, minimisation, information quality, accuracy, processing in accordance with the rights of data subjects, and security. The draft Bill does also contain additional principles on direct marketing and automated decision-making in Sections 4 and 5 respectively. There are also provisions on data subjects' rights of access, objection, rectification, blocking, erasure and destruction (Sections 2, 3 and 7 respectively). However, in many places, the scope and ambit of these principles fall short of the standards of international codes regulating processing of personal data. To make matters worse, the draft Bill does not contain conditions for legitimate processing as is the case with many data protection instruments in this field.

NO REGIME FOR SENSITIVE PERSONAL DATA

Although section 10 of the draft Bill provides for the definition of sensitive personal data, the text of the Bill does not contain a regime for regulating processing of such data. This is in contrast to the standard afforded by international data protection codes as well as national laws in many jurisdictions which offer extra safeguards to this category of data.

NO PRIVACY ENFORCEMENT COMMISSION

This is the most unique feature of Nigeria's Bill on data protection. In contrast to most international codes of data privacy as well as national legislation which incorporates a data protection authority (DPA) to oversee the enforcement of data protection legislation, the Nigerian Bill lacks this important institution. Instead, the Bill makes reference to a court as a place where individuals may enforce their rights. Yet a close scrutiny of the Bill indicates that the court referred in it is not defined anywhere neither is its jurisdiction defined. Nevertheless, a court may only intervene in specific contexts. At least, this is the implication one draws from reading the Bill, which also suggests that beyond those contexts, courts may not deal with privacy breaches.

Indeed, courts are not ordinarily better placed to deal with routine enforcement issues in data protection legislation. Hence omission of a privacy commission weakens the Nigerian Bill significantly to the extent of falling short of international standards. If the Nigerian Data Protection Bill passes into law without a privacy commission it is likely not to fulfil the adequacy standard of the EU Data Protection Directive 95/46/EC.

RESTRICTIONS TO INTERNATIONAL TRANSFERS

The draft Bill restricts in section 1(4) transfer of personal data to a country or territory outside Nigeria unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Surprisingly, the draft Bill does not further stipulate who should carry out the 'adequacy' assessment, how and according to which criteria.

Nigeria's Bill also does not provide for exceptional situations where transfer of personal data may take place even if a foreign country or territory does not ensure an adequate level of protection. Such situations usually include where:

1. The data subject has given consent to the proposed transfer; or
2. The transfer is necessary for the performance of a contract between the data subject and the controller; or
3. The transfer is necessary for the performance of a contract in the interest of the data subject between the controller and a third party; or
4. The transfer is necessary or legally required on important public interest grounds; or
5. The transfer is necessary in order to protect the vital interests of the data subjects; or
6. The transfer is made from a public register.

While section 1(4) of Nigeria's Bill may be regarded as providing a higher standard of international data transfer, it is too restrictive. It may not satisfy international data transfer standards.

COMPENSATION AND INJUNCTIONS PLUS OFFENCES

Section 6 of the draft Bill provides for compensation to an individual who suffers damage by reason of any contravention by a data controller. Such an individual is entitled to compensation from the data controller for that damage. The Bill also provides for a number of injunctions with regard to:

1. The right of access to personal data [section 2(10)];
2. The right to prevent processing for purposes of direct marketing [section 4(2)];
3. The right in relation to automated decision making [section 5(5)]; as well as
4. Rights to rectification, blocking, erasure, and destruction [section 7(1)].

Nigeria's Bill also contains offences with regard to a number of practices: unlawful obtaining or disclosing of personal information without the consent of the data controller,

procuring the disclosure to another person, and selling personal data (section 8). Moreover, breaches of certain prohibitions regarding production of certain records (recruitment, contracts for provision of services, payment facilities, etc: section 9) are offences under the Bill.

While all of the remedies mentioned above can be granted by courts, I suggest that the Bill has gone too far. It is unusual for data privacy legislation to contain a hybrid of remedies like this. Also it is interesting to note that those remedies are somewhat uncertain. For example, the Bill is silent on any type of punishment in case a particular offence is proved. This is also the case with compensation. These omissions may have a significant impact on the enforcement of the law once enacted.

Final remarks

In its present formulation, Nigeria's data protection Bill presents a weak standard of data protection legislation in comparison with other jurisdictions in Africa and beyond. It is surprising that Nigeria has even failed to comply with the standard of the sub-regional instrument the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, of which it is a member state. In the event the Bill becomes law without significant modifications, the Nigerian law will undermine the cross-jurisdictional transfer of personal data in the ECOWAS region and across Africa. It may similarly fail to live up to the 'adequacy' standard of the EU DP Directive.

AUTHOR

Alex B. Makulilo is Lecturer at the Open University of Tanzania and PhD graduand, University of Bremen.
Email: kulwath@yahoo.co.uk

Spain makes Google remove personal information from index

The DPA ruling guarantees individuals the right to object to privacy infringements with regard to Spanish Constitutional Court decisions. By **Cristina Blasi Casagran** and **Eduard Blasi Casagran**.

Today Google owns the biggest database in the world. It is not fully clear how big this company is,[1] but some studies state that Google has more than 33 trillion database entries, is subjected to 91 million searches per day, and collects trillions of bytes of data every day.[2]

Although the advantages this search engine offers to the users are unquestionable – e.g. it expands the right of expression and the right of information in the society – it may also raise concerns in terms of data protection and privacy. Particularly, contrary to the idea of how easy uploading and indexing personal information might be, trying to remove information from the net has increasingly become a nightmare for many users.

In this respect, Spain has been one of the top EU Member States as far as the number of cases against Google is concerned. Spain's Data Protection Authority (hereinafter, AEPD), as well the Spanish courts have been (quite successfully) enforcing the right to access, cancel, modify and object to processing of personal information as enshrined in both Spanish and European laws.

However, the AEPD has always had a thorn in its side regarding the index of the Spanish Constitutional Court's (hereinafter, TC) decisions, which were published in Spain's official journal. Regarding those cases, the AEPD has always considered that the TC (and not the AEPD) was the only competent authority to decide whether such information could be removed from the Google Index or not. Surprisingly, this argumentation changed on 31 March 2012. For the first time the AEPD declared itself as competent to examine a case concerning the right to object against Google, particularly with the information requested to be de-indexed was: a) a TC judgment, and b) published in the official journal.

The right to object to the processing of personal data

In Spain, any Spanish citizen has in principle a right to object to the processing of data relating to him/her. This principle was mentioned for the first time in Articles 6(4) and 30(4) of the Spanish Organic Law of Data Protection (hereinafter, LOPD).[3] Subsequently, Articles 34 to 36 of the Regulation implementing the Spanish Organic Law of Data Protection (hereinafter, RLOPD)[4] also developed this principle. Both the LOPD and the RLOPD implement Article 14 of Directive 95/46/EC.[5]

The AEPD has noted that this right permits a user, whose personal data are processed without his/her consent, to object to such processing. The AEPD adds that this request will be possible as long as it does not infringe on the existing laws, and when reasonable grounds on the specific personal situation are demonstrated.[6]

However, the enforcement of the right to object has often become controversial in cases where Spanish citizens request Google to de-index information affecting them. This is, in essence, due to the unclear law with regard to search engines.

Google claims not to be subject to Spanish law

As a general rule, any company is subject to the Spanish jurisdiction - and to the Article 24.5 RLOPD – as long as it has its headquarters or an office processing personal data within Spanish territory.

Google provides two kinds of