25 YEARS
PL&B ANNIVERSARY
1987-2012

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Denmark: The end of cloud computing as we knew it?

The Danish DPA was the first European regulator to formally look into the use of cloud computing, and has issued a number of decisions that provide practical guidance. By **Michael Hopp**.

Traditionally, the basic idea of cloud computing is that a customer, by contracting with a cloud provider, hands over its data processing needs to the provider. The cloud provider may store the data where it is deemed most convenient for the provision of the services; hence the data are possibly being transferred between data centers around the world.

In Denmark, the use of cloud computing services by the public administration has been – and still is – a hot issue for the Danish Data Protection Agency (DPA), the service providers and their potential customers. Other parts of the public administration also have a keen interest in cloud computing.

Continued on p.3

Philippines data privacy Bill signed into law: An 'own goal'?

Graham Greenleaf explains the consequences for companies involved in business process outsourcing (BPO).

President Benigno Aquino signed into law the Philippines Data Privacy Act (Republic Act 10173) on 15 August 2012. This is the second full piece of data protection legislation enacted in South-East Asia (ASEAN), following Malaysia's 2010 Act (not yet in force), and is the first ASEAN Act to apply to both a country's public and private sectors. The Malaysian Act, the Singapore Bill and Vietnam's data protection provisions (in its consumer law), all only apply to the private sector. The enactment of a data privacy law of such general scope, and including a National Privacy Commission, by a large, populous and democratic state is a significant step toward data protection and civil liberties in Asia.

Continued on p.5

Issue 119 **October 2012**

Korea rolls back ID legislation

South Korea's Constitutional Court rules on anonymous Internet postings, and new legislation prevents the collection of ID numbers. By **Whon-il Park** and **Graham Greenleaf**.

South Korea's online 'real name' statute – Article 44-5 of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (called the ICN Act) – was enacted in 2007 with bipartisan support. It was in response to such things as posted Internet comments describing fictitious sex scandals and plastic surgery operations concerning celebrities. A number of suicides of celebrities including top star Choi Jin-sil were allegedly linked to such disclosures.

The legislation stipulated that large-scale portal sites with more than 100,000 visitors, on average, a day had to record the real name identities of visitors posting comments. The poster's resident registration number was usually used to verify whether the name given by an Internet poster was his/her real name. One justification for the law was that the poster's details could be disclosed if a victim then wanted to take legal action for defamation or privacy breaches.

One result was that many South Koreans Internet commentators started to use overseas websites which allowed anonymous posting, such as Google and Twitter, and some therefore argued the law discriminated against domestic Internet services. A series of security breaches resulting in leaks of personal data concerning millions of South Koreans from those websites that were required to adopt real-name policy also occurred over the past couple of years. Observers of the Court are reported to have said that both of these considerations factored in the Court's decision (Lee, Y 2012).

Constitutional Court strikes down 'real name' law

In August 2012 the eight Justices of South Korea's Constitutional Court unanimously held that the 'real name' statute was unconstitutional because the public gains achieved had not been substantial enough to justify restrictions on individuals' rights to free speech (Constitutional Court Decision 2010Hun-Ma47, 23 August 2012 – see references below). The combined two cases decided by the Court were brought by individuals who were required to provide their real names in order to make postings, and also by an online Internet publisher required by the law to verify the names of those posting.

The Court considered that the purpose of the Internet real name system was legitimate insofar as it aims to contribute to a sound Internet culture by preventing users from posting illegal or defamatory messages on Internet bulletin boards, and collecting data to identify who did so. However, the system requiring the operator of the Internet bulletin board to verify the real name of its users and block their posting if their names fail to be verified was held by the Court to be over-restrictive beyond the extent necessary to attain the said purpose, and accordingly in violation of the principle of less restrictive alternatives, and in violation of freedom of speech, for the following reasons:

1. Where incidents of posting illegal messages occur, the illegal posters may be identified by investigating the IP addresses, and the victims may be sufficiently remedied by deleting, and blocking the dissemination of, illegal messages, and/or by means of ex post damages or criminal punishment.
2. As the users of the bulletin board include not only the person who intends to post messages but also the person who merely accesses the board and is unlikely to write a wrongful posting, and the scope of application of the real name system depends on the calculation of the number of users, the system is in disregard of the characteristics of the Internet and seems to allow the enforcement authority to act in an arbitrary manner.
3. The period for the information and communications service providers to retain the real name verification data is six months from the closing of the posting of messages. So such data may be maintained indefinitely until such messages are deleted and the posting has been closed.

In addition, the real name system is in breach of the proportionality required between protected legal interests, in that the disadvantages imposed on the users of the board and information and communications service providers are by no means smaller than the public interest achieved by the real name system. The reasons why the public interest benefits are limited are:

1. Because freedom of expression, the backbone of democracy, is of utmost importance in the Constitution, the effect of public interest achieved by restricting such freedom should be so overwhelmingly clear that restrictive measures can be justified. However, there is no evidence that the real name system has significantly reduced the defamatory or otherwise wrongful posting of messages.
2. Instead, it has caused the mass-flight of local users to overseas websites, adverse discrimination against domestic information and communications service providers, and enforcement difficulties from arbitrary law enforcement. As a result, it is not effective to attain the public interest as anticipated.
3. New kinds of communication media such as mobile bulletin boards, social networking services, etc. are so widely used that the original real name system is being implemented only within a limited scope of cyberspace, with the public benefit thus reduced.

On the contrary, the Court held, the real name system has produced various adverse effects. Internet users are likely to be discouraged from expressing themselves for fear of punishment arising from their identity disclosure. Aliens and ethnic Koreans living overseas without the resident registration number are prevented from participating in the Internet bulletin boards. The operators of the bulletin boards who find themselves in competition with the above-mentioned new kinds of communication media are treated increasingly in a disadvantageous way. The obligatory maintenance of real name verification data has increased the possibility that such data of the bulletin

board users could be leaked or misused improperly.

The Court concluded that the statute at issue was in violation of the principle of less restrictive alternatives, and in violation of the freedom of speech of both users as well as information and communications service providers in cyberspace, and also the self-determination of personal information of the users.

Court relaxations of Internet restrictictions

Recent Constitutional Court decisions have declared unconstitutional other restrictions on use of the Internet.

Until December 2010, South Koreans could be criminally punished for leaving false information online. For example, in the *Minerva Case*, a blogger with an ID, Minerva, criticised the government economic policy and predicted the collapse of Lehman Brothers with precision in 2008. In early 2009 he was arrested by the public prosecutors under suspicion that he communicated false messages in public to damage the public interest via the Internet. Later he was acquitted by the Seoul Central District Court because the accused did not intend to make false communications nor had any intention to damage the public interest. In December 2010, the same statutory provision, under which the *Minerva* blogger was accused was declared unconstitutional by the Constitutional Court, because such vague and abstract provisions cannot choke up the freedom of expression on the Internet (2009Hun-Ba88).

Until 2011, South Koreans were also prohibited from any form of online electioneering: "distributing or posting, with the intention to influence the election, of documents and pictures the content of which support, recommend or oppose a political party or candidate, or refer to the name of a political party or candidate, during the period of 180 days before the election day", but the Constitutional Court overturned this (2007Hun-Ma1001, see *PL&B International* Feb 2010, p.24).

In short, Korea previously had a very restrictive Internet environment, but this has now been relaxed considerably.

Legislation stops use of ID numbers

The most controversial personal information in Korea is the Resident Registration (RR) number which was previously compulsory in almost all dealings with government and many organisations in the private sector. Abuse of the RR number, even after some initial limitations on its use, still accounted for over 20% of all complaints received by the Korean Internet Security Agency (KISA) (over 7,000 complaints per year), with abuse of all other identification information only about one third of that (KISA/DMC 2007 Annual Report: 22).

Under Korea's new Personal Information Protection Act of 2011, unique identifiers, including RR number, passport number, driver's license number and alien registration number specified by Presidential Decree, may not be processed unless (i) the same consent is obtained as for sensitive data processing or (ii) there is explicit legislative approval (A 24(1)). Alternative means of identification other than the RR number must now be provided by processors where individuals are subscribing to web-based services (A 24(2)). Thus, the new Act now has even tighter requirements on data processors in both public and private sectors, who shall be prohibited from collecting RR numbers except in very narrow circumstances. It applies to ICSPs except where the ICN Act exempts it.

Further, the newly amended ICN Act, which only applies to ICSPs, which came into effect on 18 August 2012, allows the use of RRs only by (i) the authentication agencies, designated by the government for the purpose of provision of alternative ID numbers, (ii) qualified information and communications service providers permitted by the relevant laws, or (iii) information and communications service providers, publicly notified by the Korea Communications Commission, which rely on the collection and use of RR numbers on business (A 23-2(1)). This amendment was caused by a series of massive scale data breach incidents in which RR numbers became a prey to hackers and phishing scammers (see Park, W for information on these incidents).

Conclusions

All of the Constitutional Court's decisions demonstrate the strong role that South Korea's constitutional protections of both privacy and freedom of speech are playing in supplementing and strengthening Korea's data protection legislation. In particular, the Court's use, in the 'real names' decision, of such principles as proportionality and 'less restrictive alternatives' would not be out of place in the approach taken by European courts in the interpretation of the EU Data Protection Directive or European human rights laws. When Korea's new Personal Information Protection Act eventually comes before the courts for interpretation, this decision suggests that it may be given a strong interpretation because of the constitutional context within which it is placed.

AUTHORS

Whon-il Park is Professor of Law, Kyung-Hee University, Seoul, South Korea. Graham Greenleaf is Professor of Law & Information Systems, University of New South Wales, Australia, and JSPS Visiting Fellow, Center for Business Information Ethics, Meiju University, Tokyo.

REFERENCES

1 Constitutional Court Decision 2010Hun-Ma47 ('Real names' decision), 23 August 2012. An official summary of the Court's decision is available on the Court's website at www.ccourt.go.kr/home/bpm/sentence01_list.jsp only in Korean as yet. An English summary by Park, W, including details of the relevant provisions struck down, is available at KoreanLII http://koreanlii.or.kr/w/index.php/2010Hun-Ma47

2 Lee, Y ' 'Real names online' law struck down in South Korea' Seoul , Associated Press, 23/08/2012, at www.theglobeandmail.com/technology/digital-culture/social-web/real-names-online-law-struck-down-in-south-korea/article4495259

3 Park, W, 'Data breach incidents' at http://koreanlii.or.kr/w/index.php/Data_breach_incidents

4 South Korean Constitutional Court 'Prohibition of Internet Use for Political Expression and Election Campaign' (decision) 2007Hun-Ma1001 etc. (consolidated) decided on 29 December 2011.

Korea's DPA faults Google's Terms of Service changes

The ruling may have global implications. By **Graham Greenleaf** and **Whon-il Park**.

The first decision of Korea's Personal Information Protection Commission (PIPC) has borne out the perception that Korea's new Personal Information Protection Act (PIP Act) is "Asia's toughest data privacy law" (Greenleaf and Park, *PL&B International*, June 112, p.1). The PIPC has decided that Google's changes to the Terms of Service (TOS) of over 60 of its services, unifying them in a single TOS, may be in breach of various provisions of the Act. The decision was announced in June by the PIPC Chairman Tae-Jong Park, following a plenary meeting of the Commission.

The PIPC notes that similar results derive from provisions in Korea's Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (ICN Act), which also apply to Google because of its function as an ICSP ('information and communications service provider') under the ICN Act. This article focuses on the position under the PIP Act.

Google's TOS changes, which were effective on 1 March 2012, are considered by the Commission to likely to breach these laws in three ways: (i) they do not specify the purpose of collection clearly enough, and cannot comply with the requirement that personal information may only be collected and used to the minimum extent necessary for the purpose for which it is collected; (ii) they do not comply with the requirement that where personal information is to be used for purposes other than the purpose for which it was collected, it is necessary to obtain additional consents for such uses; and (iii) they do not specify that that personal information will be erased immediately upon the expiration of its retention period or on request from a data subject.

CONSEQUENCES IN KOREA

The Commission's opinion, given on 11 June 2012, is that Google must change its TOS in order to comply with these provisions of the Korean law. According to the Commission, Professor Jong-In Im, who is a member of PIPC and chaired the PIPC's Google Subcommittee as a data security specialist, stated that "Google's integrated policy should not become an indulgence to collect and use all types of personal information without limits, and emphasized that the present policy provisions for the comprehensive purpose and the procedure for collective consent, and the insufficient provision for the erasure of the personal information must be corrected as quickly as possible". The PIPC is waiting for Google's response. Mr Young-Min Kim, Director of PIPC's policy review division, has said that "if they continue to delay meeting our request, further action by our organization will be initiated." According to the *Korea Times*, 'The PIPC stated that possible further steps could include administrative and criminal sanctions but the most likely outcome in the long term if Google continues its stance will be a fine up to one percent of its annual revenue". While the legislation does not provide specifically for such a fine, it could result from a fine for an individual breach multiplied by the number of occurrences, under Articles 71.2 and 74(2) of the PIP Act as well as Articles 71.1 and 75(1) of the ICN Act. In addition, the decision of 15-member PIPC, of whom two Commissioners are high ranking judges and seven are lawyers or law scholars, is likely to be given considerable respect by courts.

If Google is in breach of the PIP Act, this also opens up the possibility of both individual actions and collective actions for damages under the Korean law, both through mediation provisions and in the courts (see Greenleaf and Park, 2012 for a summary).

IMPLICATIONS OUTSIDE KOREA

The Korean response to Google's unilateral changes to its TOS is the first clear finding in any Asia-Pacific jurisdiction that Google may be in breach of privacy legislation. Though only stated at this stage of the proceedings to be 'possible' breaches, the PIPC's decision leaves little doubt as to its opinion. The consequences of this Korean decision, and potential further action, outside Korea, could be considerable. Although Korea's legislation is considerably stronger than that required by the OECD Privacy Guidelines, most data privacy laws outside Europe (of which there are more than 40 at present) go considerably beyond the OECD requirements, and are closer to the 'European' provisions of the EU Directive and the Council of Europe Convention 108 (and additional Protocol) (see Greenleaf 2012).

Detailed examination of the PIPC's reasoning, and the terms of the Korean legislation, is needed in order to determine whether the PIPC's findings (and the potential remedial action) are a result of features which are unique to the Korean law, or are they features which are common to at least some other countries' data privacy laws. Each of the three findings concerning breaches are considered in turn, with references given only to the PIP Act.

SPECIFICATION OF PURPOSE AND MINIMAL COLLECTION

In its general statement of the obligations of processors, the Act provides that 'a personal information controller shall make clear the purpose of managing personal information, collect personal information lawfully and legitimately, and limit the collection to the minimum extent necessary to achieve such purpose' (A 3(1)). Only the minimum collection of personal data necessary for the purpose of collection is then allowed, and the processor has the burden of proof to show that it is the minimum (A 16(1)).

The PIPC explained Google's shortcomings under the purpose specification and minimality requirements

as follows:

> Google specified that it collects information "to provide better services to all of our users." Google also stated that "We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads."
>
> Such collection and use of personal information is highly inclusive and may provide a basis for overly excessive collection and use of personal information. Additionally, collection and use of personal information "to provide better services" or "to develop new services" may be used as grounds to justify unlimited collection of personal information in the future as well as the present.
>
> Likewise, to use personal information "to protect Google and our users" is highly likely over-application as it not only failed to have a direct relationship with Google services but also omitted a specific purpose. The provision is rather regression of the previous provision 'to protect the rights or property of Google or our users' in the policy and violates the spirit of the law which requires a collector of personal information to specify the purpose of processing personal information.

The decision then gives specific examples of what may be excessive collection.

The PIPC points out that it considers Korea's 'purpose specification' principle to be similar to that in the OECD Guidelines (and this may be correct), but its decision is one of the first outside Europe to consider the extent to which multiple purposes may be bundled in a statement of purpose of collection. The Korean requirements for minimality of collection equate to the European standard, not the weaker OECD/APEC standards that there be some limits on collection. However, minimal collection is required by the EU Directive and the Council of Europe Convention, so is standard in Europe, and a survey of 33 data privacy laws outside Europe (of 39 existing at the time), 26 followed the European minimality standard (Greenleaf, 2012). So Google's problems with minimal collection are not particular to Korea by any means.

Consent required for collection, change of use

Informed consent is required for any change of use by a processor such as Google (A 18(3)2). Before there can be informed consent, the customer must be informed of the same matters (A 18(3)) as when there is disclosure to a third party: the proposed (changed) uses, the proposed retention period for the data, the fact that consent may be denied, and the consequences of refusal of consent (A 17(2)).

The Korean Act is unusual in that the notifications that must be given before consent is obtained must explicitly separate three types of matters requiring consent, so as to assist data subjects to recognise what requires consent and what does not:

1. Each matter requiring consent must be stated separately, and each consent obtained separately, so that it is possible to consent to one but refuse consent to another (i.e., no 'bundling' of different consents) (A 22(1));
2. Where information is collected which requires consent, it shall be segregated from information which does not require consent (i.e., there should be no misleading bundling of information), and the burden of proof that no consent is required is borne by the processor (A 22(2));
3. If consent is being obtained so as to use information 'to promote goods or services or solicit purchase hereof' then the data subject must be told this, and their consent to this obtained (i.e., data subjects must opt-in to marketing uses of their information, a stronger requirement than in Europe or other laws in the region) (A 22(3)).

Although there is no explicit requirement that consent must be express, the better interpretation of the above provision, and of Article 17(2) of Presidential Decree (concerning methods of consent) is that it must be express. For example, it is difficult to see how the right 'to elect the scope of consent' (A 4.2) could be implemented as implied (opt-out) consent. This is different from some legislation in the region (e.g., Australia) allowing consent to be implied.

Applying these provisions to Google's conduct, the PIPC argued as follows:

> Google listed the personal information that used to be collected for each of over 60 services in their integrated policy en bloc and asked for consent. Thus, it is hard for users to identify for which services their specific personal information is obtained or how it is used, which may lead to the possible misuse and abuse of the information for any purpose other than the intended ones as the personal information sharing between services becomes free.
>
> For this matter, Google specified in their previous policy that "We will ask for your consent before using information for a purpose other than those that are set out at the time of collecting personal information" but they changed it into asking for consent of users before using information for a purpose other than those that are "set out in this Privacy Policy" instead of "set out at the time of collecting personal information" in the present policy. Therefore, giving consideration to the inclusive purpose of the Google Policy pointed out previously, it is deemed that the possibility of using personal information for purposes other than those that are set out in the policy without additional consent procedures for users is increased.
>
> Google stipulated in the policy that they may combine personal information from one service with information from other Google services 'to improve the overall quality of our services' or 'for user experience.' The combination may create a wide variety of new information that may be difficult to predict by users. That Google asked for inclusive consent through the policy is in violation of the relevant Acts and may restrict the choices of individuals. In the previous policy of Google, it was possible "for users to disallow the combination of infor-

mation in some services" for the combination of personal information from one service with information from other Google services or with information provided by a third party, whereas the present integrated policy deleted the provision.

Google's so-called 'tailored content' is a customized service for individuals because of the nature of the service, and the content and the level of the service must be chosen by the individual. Therefore, the tailored content must provide its specific content to individuals and ask for choices of or have consents of individuals rather than obtaining consents en bloc through the integrated policy.

The PIPC's conclusion was as follows:

"Since Google failed to specify details on the types of personal information to be collected, the purpose of collecting personal information by type, and the retention period for personal information when they stated the necessity for obtaining personal information collected for each of over 60 services, and asked for consent en bloc through the integration of the privacy policy, it is possibly in violation of Article 15, Article 18, and Article 22 of the Personal Information Protection Act and Article 22 and Article 26 (2) of [the ICN Act] for consent procedures of collection and use of personal information."

The extent to which similar conclusions might be reached in other jurisdictions is more complex, because Korea's consent provision are so precise (they make bundled consent almost impossible; they do not allow opt-out or implied consent but instead require explicit opt-in; and they do not allow notification to substitute for consent). The value of the Korean arguments in other jurisdictions will be very jurisdiction-specific.

Erasure of personal information

The PIP Act requires deletion of personal data after the purpose of processing is complete, or any other retention period completed (A 21). Since retention periods must be specified at the time of collection, this provides another period that must be complied with. The PIPC is very clear about Google's breaches of the legislation in this respect: 'Google failed to specify the retention period of personal information in the privacy policy and to delete the personal information immediately upon user requests for deletion, which violates Article 15, Article 21, Article 36, and Article 37 of the [PIP Act] and Article 29 and Article 30 of the [ICN Act].'

Although it notes that Google has provided more information to Korean users in response to the Korean Communications Commission, it is not satisfied, arguing that Google must change its deletion policies, not merely provide notice or information:

Google provided more detailed information on "retention and erasure of personal information' in "additional information related to personal information for residents in Korea." However, they still failed to specify the period for which personal information is held and used saying that 'we strive to give you ways to delete it' upon receiving a request for erasure from the data subject, and explained only about the Google archive system. It is deemed that Google has to improve the relevant policy provisions including the specification of 'erasure' of personal information instead of 'strive' upon receiving a request from users for the specification of the Acts concerned in Korea and to guarantee 'the right to be forgotten' that is discussed across the globe.

The Korean deletion requirements are more complex than most, and refer clearly to 'deletion' without providing for de-identification as an alternative. Although the OECD Guidelines do not require a deletion principle, a survey of thirty three data privacy laws outside Europe (Greenleaf, 2012) showed that twenty seven did have deletion requirements. Once again, although the Korean provisions are at the restrictive end of the scale, deletion issues could be faced by Google in many jurisdictions.

Can Google deny service to Korean users?

Although it is not mentioned in the PIPC decision, a distinctive Korean principle might cause problems for Google, if (as reported) it takes the approach that any Korean users who don't like the changed TOS will simply have to stop using Google's services.

The Act provides that there must be no denial of services because of a person's refusal to provide legally unnecessary information (A 16(2)). Organisations therefore cannot decline to provide services because a person refuses to provide more than the minimum data allowed to be collected. Such action would be a separate breach of the Act. This principle is reiterated in relation to data subjects who refuse to consent to matters where consent is optional under the Act (A 24(4)), discussed later in relation to consent. These protections to data subjects are more explicit than in legislation found in other countries.

A processor must not deny the provision of goods or services to a data subject who refuses to provide consent under A 22(2) or (3), or 'additional consent' under A 18(2) to allow additional uses or disclosures of personal

REFERENCES

Personal Information Protection Commission (South Korea) Decision 'Comments on Improvements of Privacy Policy of Google Inc.', June 11, 2012, available at www.pipc.go.kr/pds/news/120612.html

General Information on the Personal Information Protection Commission (in English) is at the KoreanLII website http://koreanlii.or.kr/w/index.php/Personal_Information_Protection_Commission

Cho, Mu-hyun (2012) 'Government may take legal action against Google' *Korea Times*, 5 July 2012, at www.koreatimes.co.kr/www/news/tech/2012/07/133_114528.html

Greenleaf, G and Park, W-I (2012) 'Korea's new Act: Asia's toughest data privacy law' *Privacy Laws & Business International Report*, Issue 117, 1-6, June 2012

Greenleaf, G (2012) 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' *International Data Privacy Law*, Vol. 2, Issue 2, 2012, also available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299

information beyond what was consented to at the time of collection (A 22(4)). This does not cover A 22(1), only because A 16(2) already provides that there can be 'no denial' for refusal to provide more than the minimum information a processor is entitled to require.

Conclusions

A short article such as this can only explain the Korean decision, and cannot suggest in any detail what might be analogous reasoning in other jurisdictions outside Korea. However, given the global effect of Google's changes to its Terms of Service, this decision should be read carefully in all jurisdictions, particularly those that go beyond the bare OECD requirements – and that means in most jurisdictions.

In the Asia-Pacific, Latin America or Africa, there are no equivalents to the relatively uniform standards set by the EU's privacy Directive. Nor is there any equivalent to the EU's 'Article 29' Working Party of data protection authorities (DPAs) with its long experience of joint decisions on matters of policy, which is now developing into cooperation on common issues of enforcement. Global corporations such as Google can exploit the differences between the laws of countries outside Europe, and the weak cooperation of their DPAs, to 'divide and conquer'. Concerted efforts at cooperation between DPAs outside Europe, a willingness to learn from the approaches of those of their members who have the courage (and the statutory provisions) to confront a globally powerful company, and the solidarity to support them in doing so, is needed if the pitchforks of privacy protectors are to prevail against the resources of their common opponents.

AUTHORS

Whon-il Park is Professor of Law, Kyung-Hee University, Seoul, South Korea. Graham Greenleaf is Professor of Law & Information Systems, University of New South Wales, Australia, and JSPS Visiting Fellow, Center for Business Information Ethics, Meiju University, Tokyo.

Brazil: A pioneer for digital rights?

Internet Bill of Rights to be voted on at Congress as the Ministry of Justice amends its draft data protection law. In the meantime, the Marketing Association lobbies for self-regulation. **Julia de Oliveira** reports.

Two key texts look set to radically change the digital state of affairs in Brazil: an Internet Bill of Rights is rumoured to be voted on shortly at Congress; and the draft data protection bill is being amended following public consultation.

The Internet Bill of Rights is big news for Internet users in Brazil. As to the draft data protection bill -– if it becomes law, the existing sectoral approach to privacy protection will shift and Brazil will be more in line with the European Union's approach to privacy and data protection.

Fragmented regulation bolstered by the proposals

As previously discussed (*PL&B International* Dec 2009, p. 7 and *PL&B International* April 2010 p.7) Brazil has a weak and fragmented system of personal privacy protection. The Brazilian Constitution of 1988 outlines the constitutional privacy rights relating to an individual's right to their image. The *Habeas Data* model, which provides for access to data as well as rectification, originated in Brazil: an irony since most South American countries have now overtaken Brazil by enacting data protection laws with stricter personal privacy protection than *Habeas*. Consumer protection laws add weight to the limited constitutional and habeas data rights.

The Brazilian Internet Bill of Rights

Despite its recognised weak privacy protection model, Brazil is quite possibly set to revolutionise and set a precedent for Internet regulation – to pioneer in the area of digital rights – with the rumoured imminent voting on the *Marco Civil da Internet*, the Brazilian Internet Rights Bill.

The *Marco Civil* is an interesting development for two reasons: firstly because it is the comprehensive codification of the civil rights of Internet users in Brazil, which is in itself unique and unprecedented since other countries do not have such a codified bill of rights for Internet users. The text covers issues such as ISP liability, equality in access to the Internet, data retention and court orders required for disclosure of communications data. It outlines several principles which govern the Internet such as freedom of speech, equality and net neutrality.

Secondly, the *Marco Civil* creates new enshrined privacy principles in legislation. The text contains two references to "privacy" and two to the "protection of personal data": It firstly mentions privacy and the protection of personal data as one of the underlying principles of the Internet (Article 3) and then it goes on to specifically mention the privacy of communications and free speech as rights of Internet users (Article 8). The Article 8 reference to privacy sits in tandem with one to freedom of speech.

Draft data protection law

The noticeable absence of a data protection law in Brazil is not necessarily a disadvantage since it is in the enviable position of being able to look at the decades of development of data protection laws across the globe while refining its proposed privacy legislation.

It comes as no surprise then that the Ministry of Justice's proposal for a data protection law, first developed in 2010 and now under revision following public consultation in 2011, seems to draw inspiration from the Canadian and EU data protection laws. Aspects of the EU's new proposed data