MAYER·BROWN

Article

Development and Revision of Global Data Privacy and Security Laws

The collection, use and transmittal of private data by companies and organizations is on the rise globally; unfortunately, so is the misuse and theft of this data. Faced with new technological developments and increased globalization, existing data protection rules are proving insufficient to address all of the security and privacy concerns being raised. In response, governments around the world are adding or revising laws and regulations meant to respond to these increased risks and to require those who collect, store and use this data to take greater responsibility for its protection.

We review existing and propose rule changes in the European Union, the United States, Hong Kong, Mainland China and Vietnam

European Union

In Europe, the general principles of data privacy are provided in Directive 95/46/EC, which governs the protection of individuals with regard to the processing of personal data and the free movement of such data (the "Data Protection Directive"). The Data Protection Directive was approved in 1995. One of its major purposes is to remove potential obstacles to the flow of personal data and to ensure a high level of data protection within the European Union.

The EU Commission now intends to revise its current data privacy regime in order to better reflect recent technical developments. The revision of the Data Protection Directive aims to provide a more harmonized level of data protection throughout the 27 EU Member States. The Commission has announced it will provide a systematic and comprehensive data protection framework.

In recent publications and press statements, Ms. Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner, has introduced the Commission's concept for the future EU data privacy framework. It consists of five principles:

- **The "right to be forgotten"**
  Data subjects will have the formal right to revoke consent given to process their personal data. Hence, users may request at any time that data processors delete their data.
- **Transparency toward data subjects**
  Data subjects must be informed, in detail, about the use of their personal data by data processors, and must also be informed of their rights with regard to data privacy. The EU Commission intends to enact new legislation providing for more transparency toward data subjects, e.g., obligating companies to publish data privacy statements on their websites.
- **Privacy by design**
  New technical developments have to observe data privacy requirements at an early development stage, thus permitting the introduction of data protecting hardware and software.

- **Responsibility for the use of personal data** Companies are to be held responsible for protecting the personal data they use. Data controllers must safeguard against data loss, data theft or data transfer not permitted under EU data privacy laws. Data subjects must be informed of data loss. The German model to establish internal data protection officers to supervise the use of personal data and advise on data privacy requirements is mentioned as an example for future internal data privacy control. Additionally, companies are to be held responsible for the personal data they process, regardless of where this data is physically stored. Providing commercial services to EU citizens or to persons or entities located in the European Union shall be subject to EU data privacy laws.
- **Independent data protection authorities** The Commission has voiced the opinion that efficient data privacy rules require strict and effective supervision. EU data privacy authorities must have a sufficient degree of independence and cooperate throughout the entire European Union.

The EU Commission has announced that it is going to introduce its new draft data privacy legislation in several months.

United States

Although it is unclear whether comprehensive privacy legislation will be enacted in 2011, potentially significant bills regarding data security and the collection and use of personal information have been introduced, and several Congressional hearings have been held, as a result of a number of high profile data security breaches. A high-level overview of two of the recent privacy and data security bills introduced in Congress is set forth below.

THE COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011 (S. 799) (SEN. KERRY/SEN. MCCAIN)

The Commercial Privacy Bill of Rights Act of 2011 (Kerry-McCain Act) would create a new disclosure-based privacy regime for any entity that collects, uses, transfers or stores "covered information" concerning more than 5,000 individuals during a 12-month period *and* (i) is subject to regulation by the Federal Trade Commission (FTC) under the Federal Trade Commission Act (FTC Act), (ii) is a common carrier subject to regulation by the Federal Communication Commission (FCC) or (iii) is a non-profit entity. Insured depository institutions (banks), which are not subject to jurisdiction of the FTC, would be excluded from the coverage of this legislation. However, many other financial institutions would be covered to some extent.

The Kerry-McCain Act attempts to harmonize its coverage with the existing federal privacy laws. As a result, existing federal privacy laws would continue to apply, and covered entities would remain subject to their requirements. Thus, a financial institution covered by the Gramm-Leach-Bliley Act (GLB Act) would continue to comply with the applicable provisions of the GLB Act. To the extent that the particular conduct or behavior was not subject to regulation by the GLB Act, the financial institution would be required to comply with the provisions of the Kerry-McCain Legislation. This qualified exemption would require most financial institutions to comply with the GLB Act, other federal privacy laws and the Kerry-McCain Act. This would often require institutions to make difficult determinations about the proper coverage of specific conduct under the various privacy laws.

The type personal information covered by the Kerry-McCain Act extends beyond those types covered by the GLB Act and other privacy laws. For example, it includes geographic location and IP addresses, if associated with a person, and "sensitive personal information." Sensitive personal information is broadly defined as information that carries a significant risk of economic or physical harm if inappropriately disclosed or compromised. The subjective nature of this definition would make compliance difficult.

The Kerry-McCain Act would require the FTC to issue rules requiring entities to provide notices that include information practices regarding collection, use, transfer and storage of information and specific purposes for those practices. It also would generally

categorize the use of information as unauthorized, unless expressly authorized or within an enumerated exception. Individuals must opt-in to allow the collection and use of sensitive personal information, as well as for certain limited transfers or uses of personal information. An opt-out requirement would cover most other uses of personal information. The FTC would have enforcement and rulemaking authority under the Kerry-McCain Act. No private right of action is provided, but state Attorneys General could also enforce the legislation. The legislation would preempt certain state privacy laws. However, certain state laws are expressly protected, including state laws regarding health or financial information, data breaches and fraud.

The Kerry-McCain Act was referred to the Senate Committee on Commerce Science and Transportation on April12, where it is still pending.

SECURE AND FORTIFY ELECTRONIC DATA ACT (SAFE DATA ACT) (REP. BONO-MACK) (H.R. 2577)

The SAFE Data Act would require businesses to establish and implement policies and procedures regarding information security practices and to notify individuals if their electronic personal information is subject to unauthorized access. Under the SAFE Data Act, the FTC has enforcement and rulemaking authority. The coverage of the Act is generally limited to those persons over which the FTC has authority pursuant to Section 5(a)(2) of the FTC Act. Similar to the Kerry-McCain Act, this limitation means that insured depository institutions are excluded from the requirements of the SAFE Data Act. There is also an exemption from the security and notice requirements for entities covered by GLB Act and HIPAA.

Under the SAFE Data Act, the FTC would have one year from the date of enactment to issue regulations requiring businesses to establish and implement policies and procedures regarding information security practices. These policies and procedures must include the following: a security policy with respect to the collection, use, sale and maintenance of personal information; identification of an officer or individual with responsibility for information security; a process for identifying and assessing any reasonably foreseeable vulnerabilities in the system; a process for taking preventative and corrective action to mitigate against any vulnerabilities identified; and a process for disposing of data whether in electronic or paper format.

In the event of the discovery of a breach of security involving personal information in an electronic form, a business must, without unreasonable delay, notify law enforcement (unless the breach did not involve unlawful activity), the FTC and each individual whose information has been acquired or accessed as a result of the breach. Notice to the individuals would be required as promptly as possible, but no later than 45 days following the discovery of a breach. Notice to individuals would not be required if the business determines that there is no reasonable risk of identity theft, fraud or other unlawful conduct. If the information was encrypted, there is a presumption that no reasonable risk exists. The SAFE Data Act also requires businesses to offer credit monitoring services or quarterly consumer reports to consumers for up to two years if there is a risk of identity theft. Credit monitoring is not required if the information subject to the breach of security only involves the consumer's name and address with credit or debit card number.

While the SAFE Data Act does not create a private right of action, the FTC would have the authority to impose substantial civil money penalties ($11,000 per violation up to $5 million). Furthermore, state Attorneys General would also have the authority to enforce the Act's provisions to enjoin further violations, compel compliance or obtain civil penalties. The SAFE Data Act would preempt state laws imposing requirements on information security practices or requiring notification in the event of a breach of security involving personal information.

The SAFE Data Act was introduced formally on July 19 by Representative Mary Bono-Mack and was approved by the House Subcommittee on Commerce, Manufacturing, and Trade by a voice vote.

Hong Kong

The Constitutional and Mainland Affairs Bureau of the Government of Hong Kong SAR (the "Bureau") published the Report on Public Consultation on the Personal Data (Privacy) Ordinance (the "Consultation Report") in October 2010, following a late 2009 public consultation on proposed amendments to the Personal Data (Privacy) Ordinance.

The Consultation Report identifies more than 30 proposed changes. Some of the key proposals are set out below:

- To make it a criminal offense for a data user to sell personal data without the data subject's consent
- To make it a criminal offense for a person to disclose personal data obtained from a data user for profit or malicious purposes without the data user's consent
- To make it a criminal offense for a data user who previously complied with the directions in an enforcement notice, to subsequently do the same act for which the enforcement notice was previously issued by the Privacy Commissioner of Personal Data (PCPD)
- To impose a heavier penalty on data users for repeated non-compliance with enforcement notices issued by the PCPD
- To introduce specific requirements on data users regarding the collection and use of personal data for direct marketing purposes
- To introduce a voluntary privacy-breach notification system
- To strengthen supervision of data processors and data processing sub-contracting activities by requiring them to use contractual or other means to ensure that their data processors and sub-contractors, whether located in Hong Kong or overseas, comply with the requirements under the Personal Data (Privacy) Ordinance

The Bureau has invited the public to comment on the proposals set forth in the Consultation Report. In effect, the Bureau is conducting a second round of consultation on the detailed changes. It remains to be seen how these proposals will be implemented.

People's Republic of China

Unlike many other jurisdictions, the PRC does not have a single comprehensive code of legislation dealing with the protection of privacy and personal data. The laws and regulations relating to privacy and personal data are scattered in various pieces of legislations. In 2008, a draft Personal Information Protection Law (the "Draft Law") was proposed to the relevant PRC legislative authorities, however, the contents of that Draft Law are not publicly available and it is unknown if and when the Draft Law might be passed.

Below is a summary of the main legislation in the PRC regarding the protection of privacy and personal data.

PROTECTION UNDER CIVIL LAWS

Infringement of privacy may sometimes be viewed as a civil tort of infringing reputation. In addition to publication of a false statement to lower the standing of another person, or infringement of another person's reputation by way of insult or defamation, a disclosure of the privacy of another person, whether verbally or in writing, also constitutes an act of infringement of the reputation of that person.

The right of privacy has been expressly acknowledged under the PRC Tort Law as one of the civil rights and interests enjoyed by an individual, the infringement of which constitutes an actionable civil tort. An individual whose privacy has been infringed may have a right to demand cessation of such infringement, restoration of reputation, elimination of adverse impact, issuance of an apology and payment of damages (the amount of which does not carry any statutory ceiling), which may include damages to compensate an individual for severe mental distress suffered. A court may also order forfeiture of gains obtained as a result of such infringement.

An individual whose civil rights and interests are infringed as a result of information published on the Internet may notify the Internet service provider (ISP) to take such necessary measures as deletion, blockage or disconnection so as to contain any damage done. Failure on the part of any notified ISPs to take action

may render them jointly and severally liable for any additional damage caused to such an individual. It is important to note that the PRC Tort Law has made it clear that a tortfeasor whose means are insufficient to satisfy both the tortious liability and any administrative or criminal fines is required to first satisfy the tortious liability.

PROTECTION UNDER CRIMINAL LAW

The PRC Criminal Law provides that if government entities or non-governmental entities engaged in finance, telecommunications, transportation, education or medical treatment, or employees of either such entity, sell or illegally provide personal data obtained during the performance of their duties or the provision of their services, and the circumstances are deemed "serious," such entities or employees can be subject to a fine and/or a prison term of not more than three years.

However, the law does not specify what constitutes a "serious circumstance." Considering the increasing misuse of personal information in the PRC, there is a non-official view that such provisions shall apply to all entities that possess the personal information of an individual in the course of providing services.

PROTECTION UNDER LABOR LAWS

Generally, under the Regulation on Employment Service and Employment Management, an employer is obligated to (i) keep confidential the personal data of any of its employees and (ii) obtain a written consent from any employee whose personal data the employer wants to publicize. Although not expressly stipulated, it is generally understood that the above obligations cover the data of former employees as well as job applicants.

Vietnam

Vietnamese law protects rights related to private information. All organizations and individuals have duty to respect private and confidential information. Any breach of this obligation would, depending on the seriousness of the breach, result in an administrative penalty or a criminal sanction. Disclosure of protected information is however possible where:

- It is specifically permitted by the laws;
- The information owner has granted a prior consent to such intended disclosure (in respect of personal information and information of organizations); or
- At the request or in the order of any appropriate state agency in certain cases (for example, as ordered by a competent court).

Specifically, pursuant to Article 38 of Civil Code No. 35/2005/QH11 dated 14 June 2005 (the "Civil Code"), the privacy of an individual is protected by law. The collection and publication of information and data pertaining an individual shall be subject to his/her consent. Exceptions are given to collection and publication of personal information as referred to (i) and (ii) above.

The Civil Code does not specify what constitutes "personal information" or "privacy" pertaining an individual. Thus, the interpretation of whether or not information is considered to be personal would be at the sole discretion of a Vietnamese court.

The same principle is applied to protection of privacy on the Internet.

The confidentiality of private information of organizations and individuals on the Internet is protected by laws (Articles 4.7 of Decree 97 and Part I (3) of Circular 06). ISPs are responsible for the information they upload onto, retain and disseminate through the Internet, and are also under a duty to install and apply technical and professional measures to ensure the safety and security of the information as required by the appropriate state agency (Article 7.2 of Decree 97 and Article 4.3 of Circular 05).

Unless otherwise specifically permitted by law, organizations and individuals that collect, process and use the private information of individuals on the Internet must first secure the individual's permission. The individual must be informed about the form, scope, venue and purpose for the information's collection, processing and use. Additionally, the information must be used only for the purposes as

agreed by the parties, and it can be retained for a certain period of time as provided for by the laws or as agreed by the parties.

Where an ISP retains an individual's private information on the Internet, the individual can request the ISP to check, correct or repeal such information. Private information of an individual must not be disclosed to a third party without the individual's prior consent, or unless specifically permitted by law.

Finally, when personal data is to be transferred abroad from Vietnam, Vietnamese law requires the following:

- Appropriate security measures to ensure that the information transferred is protected; and
- An agreement between the parties specifying the form, scope, venue and purposes of the collection, processing, use and transfer of the personal information. ◆

For more information about this topic, please contact any of the following authors.

Mark Hilgard
mhilgard@mayerbrown.com

Dao Nguyen
dao.nguyen@mayerbrownjsm.com

Sara Or
sara.or@mayerbrownjsm.com

Mark Prinsley
mprinsley@mayerbrown.com

Jeffrey Taft
jtaft@mayerbrown.com

Terrance Tung
terence.tung@mayerbrownjsm.com

Tim Wybitul
twybitul@mayerbrown.com

Andy Yeo
andy.yeo@mayerbrownjsm.com

Atticus Zhao
atticus.zhao@mayerbrownjsm.com