Beijing District Court's attitude may even suggest that those who would like to claim privacy protection before Chinese court should come with clean hands.

On this uncertain note, legislative intervention may be the best solution to clear the present legal ambiguity. While Xuzhou City of Jiangsu Province in 2009 has enacted its law to prohibit the disclosure and dissemination of personal information on the Internet without authority from the concerned individuals, it is hoped that the Wang Fei Case will provide an impetus for the implementation of the Proposed Personal Information Protection Act.

AUTHOR

Anne S.Y. Cheung, Department of Law, University of Hong Kong.

REFERENCES

1. *Wang Fei v. Zhang Leyi, Daqi.com and Tianya.com*, Beijing Chaoyang District Court, No. 10930 (2008), available at www.chinacourt.org:80/html/article/200812/18/336418.shtml (in Chinese).
2. Bai Xu & Ji Shaoting, "Human Flesh Engine": An Internet Lynching?, XINHUA NEWS, July 4, 2008, available at http://news.xinhuanet.com/english/2008-07/04/content_8491087.htm.
3. For a copy of the writ of summons, see http://cache.tianya.cn/publicforum/content/no11/1/539720.shtml (in Chinese).
4. Chaoyang District Court, Beijing to Ministry of Information Industry, Proposal for Stricter Supervision of the Internet, Dec. 18, 2008, available at Chinalaw@hermes.gwu.edu discussion board (in Chinese).
5. Decree No. 291 of State Council, promulgated by State Council, 25 September 2000, effective on 25 September 2000, available at www.lawinfochina.com, Approved by State Council, 11 December 1997, promulgated by the Ministry of Public Security on 30 December 1997.
6. Promulgated by the Ministry of Information Industry, 6 November 2000, Decree No. 3, effective on 6 November 2000, available at www.lawinfochina.com.
7. Violations may incur an administrative penalty of RMB5000. See article 18(7) on the protection of personal information and article 26 on penalty of Xuzhou City Internet Security Provisions, promulgated by the 7th Meeting of the Standing Committee of the 11th People's Congress of Jiangsu Province, 18 January 2009, to be effective on 1 June 2009, available at www.dffy.com/sifashijian/ziliao/200901/20090122191433.htm (in Chinese).
8. For discussion of the background and a summary of the major points of the proposal, see Graham Greenleaf, China Proposes Personal Information Protection Act, *Privacy Laws & Business International*, February. 2008, p.1 and pp.3-6; and Graham Greenleaf, Enforcement Aspects of China's Proposed Personal Information Protection Act, *PL&B International*, April 2008, p.1 and pp.11-14.

Taiwan proposes amendments to its 1995 Data Protection Act

Scope expanded but no supervisory authority. By **Dennis Tang**.

Taiwan is one of the pioneering states in the Asia-Pacific Region in adopting statutes for protecting personal data. The Computer Processed Personal Data Protection Act was enacted in August 1995 with reference to the OECD Guidelines (1980). The Act, consisting of 45 articles, is divided in 6 chapters: I. General Provisions; II. Data Processing by Public Agencies; III. Data Processing by Non-Public Agencies; IV. Damage Compensation and Other Remedies; V. Penalties; and VI. Supplementary Provisions. In light of the rapid advance of information technology and the ever increasing computerisation of personal data in the past decade, the appeal for overhauling the Act has become stronger and more widespread. In response, the Executive Yuan (the Cabinet) has proposed several amendments to the Act since 2000. Yet none has succeeded in the Legislative Yuan (the Legislature). Following his inauguration in May, President Ma appointed a new Cabinet. Among the bills presented by the Cabinet to the January 2008 re-elected Legislature was the Amendments to the Act (hereinafter the Draft).

The Draft has passed its first reading in the Legislature and is currently awaiting "parties' negotiation" to finalise the text for the second reading.

Major revisions proposed

The highlights of the Draft can be summarised as follows:

1. The scope of application is expanded. First of all, the definition of data is extended, from the computer-processed personal data, to all personal data, i.e., the information relating to identified or identifiable individuals which is either being processed by means of equipment operating automatically in response to instructions given, or any set of information relating to identified or identifiable individuals which is otherwise structured in a way that specific information relating to a particular individual is readily accessible. The title of the Act is to be the "Personal Data Protection Act".

Secondly, by eliminating the "category designation" for the private sector, the actors subject to regulation of the Act are broadened to cover all who actually collect, process or use/disclose personal data (so-called "the public agencies and the non-public agencies", hereinafter, data controllers).

Thirdly, the Act, for the first time, carries trans-boundary effects, that is, the Act also applies when a data controller collects, processes or uses/discloses personal data of a citizen

outside the territorial jurisdiction of Taiwan

2. Density of regulation is heightened. The Draft makes various efforts, with various degrees of success, to crystallise the underlying information privacy principles. For example, "the personal information relating to health care, gene, sexual life and criminal records" are differentiated from others and subject to more stringent requirements of data management. Such (sensitive) information is not to be collected, processed or used/disclosed, unless one of several enumerated conditions is met (section 6).

The Draft (section 8-I) for the first time stipulates the items which a data controller shall inform a data subject when collecting the data from the subject directly ("fair notification requirement"). The Draft (section 9-I) further requires that a data controller, before using/disclosing personal data stored, shall inform the data subject of the information source when the data were not collected from the data subject in the first place.

In addition, a new provision (section 11-IV) prescribes that a data controller shall, voluntarily or upon request of the data subject, erase or suspend collecting, processing or using/ disclosing any personal data where the data were collected, processed or used/disclosed in a way in violation of the Act.

One may reasonably infer from such a provision that a data controller shall inform the data subject of any breach of law during data management process ("breach notification obligation"). The Draft (section 20) regulates for the first time direct marketing based upon personal data by requiring a private data controller (the so-called "non public agency") to provide the data subject an opt-out choice when conducting direct marketing in the first place.

3. The administrative supervision is strengthened

In order to prevent various abuses of personal data management, the Draft (section 22) strengthens administrative supervision by authorising local governments to conduct administrative inspection on site, without obtaining a search warrant from the court, and to take all necessary measures for seizure.

4. Class action introduced.

The Draft widens courses for remedies by providing that 20 or more of the victims in a same breach-of-law event may authorise a certified non-profit association or foundation to bring class action for damage compensation. Relevant revisions involve seven sections (sections 34-39 & 51).

5. Penalties refined.

The Draft (section 40) imposes different penal liabilities for breaches of law because of with or without intention of profiting. The Draft (section 28-IV) raises the damage compensation ceiling for a similar breach-of-law event, from NT$20 million, to NT$50 million. The representatives or managers of a private data controller (the so-called "non public agency") shall, in principle, simultaneously be subjected to the same amount of administrative penalties imposed upon the data controller for breaches of law (section 49).

Brief comments on the draft

There are many defects in the Act. To name just a few fundamental ones:

1. **The logic is ambiguous and the order of provisions is confusing.** To be logical and comprehensible, the author urges a reshuffle of the chapters: I. General Provisions; II. Data Subject Rights; III. Data Protection Obligations; IV. Information & Privacy Commissioner; V. Penalties for Breaches; and VI. Supplementary Provisions.
2. **The key concepts are not clearly defined or fully clarified.** The Draft aims to regulate the "collection, processing and use" of personal data (section 1). However, the definition of "processing" (sections 2-4) is redundant and overlapping. The author suggests drop "transfer" from the definition and redefine it with reference to German Federal Data Protection Act (*Bundesdatenschutzgesetz* section 3-IV). Besides, the definition of "use" (sections 2-5) shall be supplemented with, "including the mere disclosure to a third party," after the original "means the use of collected personal data for the purposes other than processing." As to the meaning of "personal data", the Draft ought to be revised to follow the UK legislation by incorporating "filing systems" into the concept of "data" and then redefine both, so that the Act's scope of application will not be overly entrenched. Moreover, the Draft ought to be revised either to follow the EU-style legislation by adopting "data controller" as an upper concept for the actors subject to the Act, both in public and private sectors, or to redefine "public authority" as well as "private organisation". Finally, for the sake of clarity, a "party" in the Act should be correctly re-named as (data) "subject" (sections 2-9).
3. **The contents of right to information privacy have not been unambiguously announced.** For the sake of public education and judicial enforcement, the Draft ought to have a separate chapter to specify in detail all judicially enforceable rights enjoyed by a data subject, including right of access, right of correction (in a broad sense), right to objection (to various data management activities), right for remedies, and concomitant administrative procedure rights.
4. **The obligations of data controllers are not well articulated.** The Draft should, bearing the "information privacy principles" or "data protection principles" in mind, assort and integrate all kinds of data management requirements imposed upon data controllers, of both public and private sectors, into one separate chapter.
5. **A supervisory agency is absent.** The Draft should set up a control agency to supervise the implementation of the Act by both the public and private data controllers. A UK style independent administrative agency ("information and privacy commissioner") for supervising the implementation of both the Freedom of Information Act of 2005 and the Act is probably the most feasible choice.

AUTHOR

Dennis Tang is Director and Research Professor, Institutum Iurispredentiae, Academia Sinica, and Professor of Law, Graduate Institute of National Development, National Taiwan University.
Email: dennis@sinica.edu.tw
Web: http://idv.sinica.edu.tw/dennis