Morrison & Foerster Client Alert.

February 27, 2012

Hong Kong Privacy Law Update: New Legislation and User Guidelines

By Gordon Milner and Eric Tyler Dickinson

Hong Kong has one of the oldest privacy laws in the world, and The Office of the Hong Kong Privacy Commissioner has recently been very active in shaping the ongoing evolution of Hong Kong's data privacy regime. The past few weeks have seen the Privacy Commissioner publish detailed commentary on the forthcoming update to the key privacy statute and two new sets of guidelines aimed at data users.

(A) The Personal Data (Privacy) (Amendment) Bill

The Personal Data (Privacy) Amendment Bill (the "Bill") was introduced into Hong Kong's Legislative Council on 13 July 2011 following public concerns arising from several highly-publicised scandals involving the sale of personal data without the knowledge or consent of individuals. As a result, there have been calls to update the law and to increase enforcement authority of the Privacy Commissioner.

In brief, the Bill seeks to regulate direct marketing and the sale of personal data as follows:

- Before personal data can be used for direct marketing or sold to a third party, the data user must notify the individual clearly specifying: (i) the type of personal data which may be used for direct marketing or otherwise sold, (ii) the classes of persons to whom the data may be provided, and (iii) the types of goods or services which might be marketed to the individual.
- The individual may at any time decline to allow such use or sale of his/her personal data. The entity seeking to use the personal data must provide an opt-out mechanism for this purpose.
- The entity must wait 30 days after the notice is provided to the individual before selling the data or commencing direct marketing so as to provide the individual with sufficient opportunity to opt out prior to such activities taking place.
- Under the Bill, non-compliance with these direct marketing and data sale provisions would be a criminal offence.

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

- The Bill would also introduce a new offence for persons who obtain personal data from an individual without his/her consent, and subsequently disclose the personal data in order to (i) obtain any form of gain, (ii) cause loss to the individual, or (iii) cause psychological harm to the individual.

The Privacy Commissioner has criticized the Bill in several recent statements. In particular, in comments published in December, the Commissioner voiced concerns that the 'opt-out' approach taken in the Bill would effectively create a system of "delayed notification and deemed consent", as the majority of individuals are unlikely to take the necessary steps to proactively opt-out of a proposal to sell or use their personal data in direct marketing campaigns. The Commissioner has instead argued that such sale and direct marketing use of personal data should be subject to the 'opt-in' consent of the individuals concerned. However, this approach now appears unlikely to be incorporated into the Bill, which passed the Bill committee stage in January and looks set to become law later this year.

(B) New Guidance Notes

The Privacy Commissioner also published two new Guidance Notes on its website (www.pco.org.hk). While such Guidance Notes are not legally binding, they are illustrative of best practices and, if followed, will provide a presumption that the entity has complied with the Hong Kong Data (Privacy) Ordinance (the "Ordinance").

(1) Guidance on Personal Data Erasure and Anonymization

Under the Ordinance, entities are responsible for deleting collected personal data when the entity no longer needs the information. This Guidance Note recommends the following best practices:

- Entities should have a data retention policy specifying when and how personal data should be destroyed;
- Paper records containing personal data should be shredded in a cross-cut fashion so that individual sheets cannot be reconstructed;
- Personal data stored in digital form should be erased by use of advanced data deletion software, such as those conforming to U.S. Department of Defense deletion standards (DoD 5220.22-M) – simply deleting files or reformatting hard drives is considered unreliable because data deleted through these means may remain retrievable; and
- When outsourcing data deletion services, parties should enter into a contract specifying security requirements, erasure standards, and a mechanism to ensure that all personal data has been completely destroyed.

The Guidance Note also notes that in lieu of destroying useful (but not necessary) personal data, an entity can take steps to anonymise it instead. Anonymisation must be so complete, however, that the relevant individuals can never be re-identified.

(2) Guidance for Entities on the Collection and Use of Personal Data through the Internet

This Guidance Note seeks to help website owners and operators comply with each of the Ordinance's six data privacy principles. Key recommendations include the following:

- **Collection**. Personal data should be collected in a transparent fashion. The identity of the website operator must be made clear. If the website collects personal data through an online form, mandatory items should be clearly labeled. If cookies are required, this should be clearly stated on the website.

- **Retention**. The website should have a policy setting out the retention period of the personal data collected, and a mechanism to ensure deletion of both online and offline data after such period.
- **Use**. When displaying personal data on a website, there should be a statement limiting its use. Website operators should also consider whether the display of anonymised data would serve as an adequate substitute for the display of actual personal data.
- **Protection**. Adequate technological safeguards should be adopted to prevent the leakage or theft of personal data. Such safeguards should include access codes, encryption, and firewalls. All personnel involved in the handling of personal data should be adequately trained and made familiar with the requirements of the Ordinance.
- **Transparency**. A privacy policy statement should be made accessible by link on any page where personal data is collected.
- **Access**. Individuals should be able to easily access all of their personal data which is handled by, or stored on, the website. They should be able to correct any inaccuracies directly relating to their personal data.

Copies of both Guidance Notes are available via the Privacy Commissioner's website (**www.pco.org.hk**).

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for eight straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.