BAKER & MCKENZIE

# BakerGPS (Global Privacy Strategy) – Part 23 Webinar

## Big Data and Big Data Privacy: An introduction to the conflict between the commercial value of information and global privacy requirements

**21 May 2013**

# Our Panel Today


## Brian Hengesbaugh

**Partner, Chicago**

T: +1 312 861 3077

E: Brian.Hengesbaugh@bakermckenzie.com



## Samuel Kramer

**Partner, Chicago**

T: +1 312 861 790

E: Samuel.Kramer@bakermckenzie.com



## Anne-Marie Allgrove

**Partner, Sydney**

T: +61 2 8922 5274

E: Anne-marie.Allgrove@bakermckenzie.com



## Amy de La Lama

**Associate, Chicago**

T: +1 312 861 2923

E: Amy.deLaLama@bakermckenzie.com



## Julia Wendler

**Associate, Munich**

T: +49 89 55 238 242

E: Julia.Wendler@bakermckenzie.com

# Agenda

1. What is Big Data?
2. What are the key privacy issues with Big Data?
   - United States
   - Europe
   - Asia-Pacific
3. What are the key commercial contracting issues?
4. Key take aways

# What is Big Data?

# What is Big Data?

"*Big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationships between citizens and governments*."

Big Data: A Revolution That Will Transform How We Live, Work, and Think
by Viktor Mayer-Schonberger and Kenneth Cukier

# What is Big Data? (cont'd)

- Big Data surge is fueled by the extraordinary growth in digital information across mobile applications, social networks, web tracking, search data, smart grids, and a myriad of other applications
- Amount of data in the world is doubling roughly every three years (Martin Hilbert of the University of California)
  - In 2007, the world had more than 300 billion gigabytes of stored data
  - By the end of 2013, stored data in the world should be around 1,200 billion gigabytes (or 1,200 exabytes). Approximately 98% of this data is in digital form
  - Illustration: If 1,200 billion gigabytes of data were placed on CD-ROMs and stacked together, the CD-ROMs would stretch to the moon in five separate piles

# What is Big Data? (cont'd)

- Key characteristics of Big Data:
  - Secondary uses
  - Complete data sets
  - Data consolidation from multiple sources
  - New sources of data

# What Are The Key Privacy Issues?

- Expanding scope of regulated personal data
- Data subject notice and choice
- Data subject rights (access, correction, matching procedures, and automated decisions)
- Disclosures to third parties
- Data de-identification
- Cross-border data transfer restrictions

# Key Privacy Issues with Big Data

# United States

# When Do Privacy Laws Apply?

- Privacy laws – including those in the United States - only apply to information that falls within the scope of personal data (as defined by the relevant law)
- In the context of Big Data, data that has not been de-identified in accordance with applicable laws is subject to all notice and consent, security and other requirements

# When Do Privacy Laws Apply? (cont'd)

- By way of example, the Health Insurance Portability and Accountability Act ("HIPAA") establishes specific and strict standards for de-identification of covered health data or protected health information ("PHI").
- Covered entities (e.g., health care providers, pharmacies, health insurance providers) and/or their service providers that improperly disclose or use PHI that has not been de-identified in accordance with HIPAA can be subject to civil fines and even criminal penalties in certain circumstances.

# De-identification Under HIPAA

- General de-identification standard: PHI is de-identified when "there is no reasonable basis to believe that the information can be used to identify an individual."
- There are two different methods to comply with this standard:
  - The removal of eighteen specified patient identifiers; or
  - Determination by a qualified statistician

# Removal of Eighteen Identifiers

- To meet this requirement, eighteen specified patient identifiers must be removed.
  - The identifiers include, but are not limited to, patient name, location (other than state or 3-digit ZIP codes with populations greater than 20,000), email address, telephone number, Social Security Number.
  - Significantly, the eighteenth identifier that must be removed is “any other unique identifying number, characteristic, or code.”
  - Even after removing all of the designated identifiers, the data controller must not have actual knowledge that the remaining data could be used alone or in combination with other information to re-identify the data subject.

# Professional Statistical Analysis

- To meet this standard of de-identification, a qualified statistician must:
  - Determine that the risk is very small that the PHI could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
  - Document the methods and results of the analysis that justify such determination.
- In performing this analysis, the statistician must take into account available technology and the overall information environment.

# Europe

# De-identification In Europe

EC Data Protection Directive:

"Personal Data shall mean any information relating to an **identified or identifiable natural person**; an **identifiable person** is one who can be identified, **directly or indirectly**, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

- Replacing name with a code number not sufficient
- No definition of de-identified data

# De-identification In Europe (cont'd)

German Federal Data Protection Act:

"Personal Data shall mean any information concerning the personal or material circumstances of an **identified or identifiable natural person**."

- No definition of "identifiable person" but definition of "de-identification"

"De-identifying shall mean the modification of personal data so that the information concerning personal or material circumstances can no longer or **only with a disproportionate amount of time, expenses and labor** be attributed to an identified or identifiable person."

# Purpose Limitation In Europe

Rational for purposes limitation: Protection of data subject by setting limits on how data controllers can use the personal data vs. some degree of flexibility for data controllers

- Personal data must be collected for specified, explicit and legitimate purposes (original purpose) and not be further processed in a way incompatible with those purposes (secondary purpose)
  - Unambiguous and clear purpose specification prior to the collection (layered notices)
  - Transparency and predictability for data subject to understand purpose and allow legal assessment of lawfulness

# Purpose Limitation In Europe (cont'd)

- Secondary purpose requires compatibility assessment on a case-by-case basis:
  - Relationship between the original and the secondary purpose
  - Context of data collection and reasonable expectation of data subject – unexpected and surprising use most likely incompatible
  - Nature of personal data (sensitive data) and impact of secondary purpose for data subject (e.g., potential decisions by third parties, exclusion or discrimination of individuals, emotional impacts).
  - Implemented safeguards as "compensator" (e.g., additional information, consent or right to object, de-identification, pseudonymisation)

# Purpose Limitation In Europe (cont'd)

- Processing for incompatible purposes is prohibited even if a new legal ground would justify it (WP 203, April 2, 2013)

- Big Data: Typically opt-in consent required for tracking and profiling for marketing purposes, behavioral advertisement, data-brokering, location-based advertising

# Asia Pacific

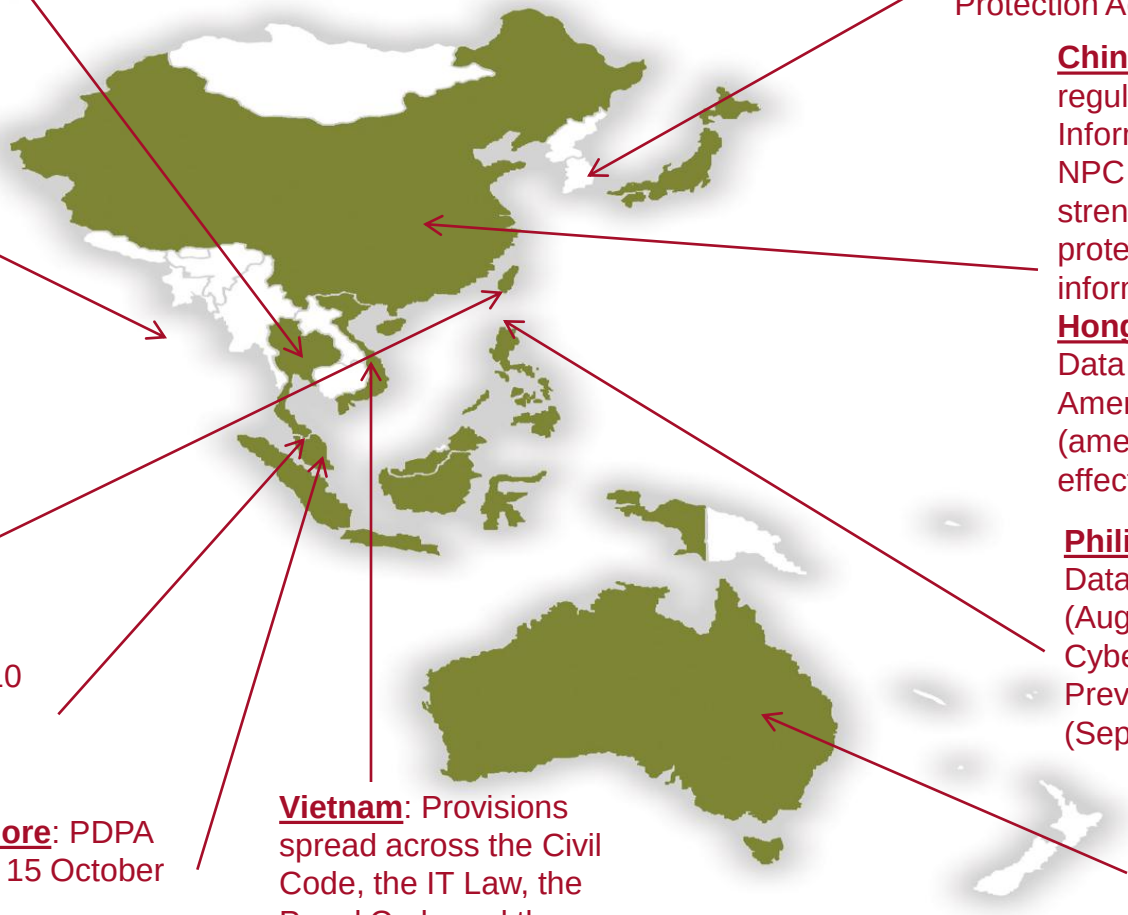
**Thailand**: Draft law sent to Parliament in 2012

**India**: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

**Taiwan**: PDPA 2010 in effect from 1 October 2012

**Malaysia**: PDPA 2010 (date for coming into force yet to be set)

**Singapore**: PDPA passed 15 October 2012



**Vietnam**: Provisions spread across the Civil Code, the IT Law, the Penal Code and the Telecommunications Law.

**South Korea**: Personal Information Protection Act 2011

**China**: Provisions regulating Internet Information Services/ NPC Decision on strengthening the protection of internet information

**Hong Kong**: Personal Data (Privacy) Amendment Ord (amendments in full effect on 1/4/2013)

**Philippines**: Data Privacy Act (August 2012) Cybercrime Prevention Act (September 2012)

**Australia**: Amendments come into effect in March 2014

# Asia Pacific Overview

| | Australia | China | Hong Kong | India | Indonesia | Japan | Malaysia | Philippines | Singapore | South Korea | Taiwan | Thailand | Vietnam |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Comprehensive data protection law in force | ✓ | | ✓ | | | ✓ | | ✓ | ✓[1] | ✓ | ✓ | | |
| Comprehensive law has passed but is not yet in force | | | | | | | ✓ | | | | | | |
| Draft comprehensive law has been proposed | | | | ✓ | | | | | | | | ✓ | |
| Regulations/ Guidelines | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓[2] | ✓ | ✓ | ✓ | ✓ |

[1] 12 and 18 month sunrise period for substantive provisions
[2] Proposed for consultation

# Where We Are Now?

| | Australia | China | Hong Kong | India | Indonesia | Japan | Malaysia | Philippines | Singapore | South Korea | Taiwan | Thailand | Vietnam |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Distinguishes between data collection and data processing | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓^ | ✓ | ✓^ | ✗ | ✓ | ✗ | ✗ |
| Registration/notification requirements | ✗ | ✗ | ✓^ | ✗ | ✗ | ✗ | ✓^ | ✗ | ✗ | ✗ | ✗ | ✓ (certain industries) | ✓ (certain industries) |
| International data transfer specifically regulated | ✓ | ✓ | ✓^ | ✓ | ✗ | ✗ | ✓^ | ✗ | ✓^ | ✓ | ✓ | ✓ (certain industries) | ✗ |
| Mandatory breach notification | ✗ | ✓ (certain industries) | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ (certain industries) | ✓ | ✓ | ✓ (certain industries) | ✓ |
| Criminal sanctions | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓^ | ✓ | ✓^ (certain offences) | ✓ | ✓ | ✓ (certain industries) | ✓ |
| Privacy Officer required | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓^ | ✓ | ✓ (public institutions) | ✗ | ✗ |
| Exemptions for employee data | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓^ (certain cases) | ✗ | ✗ | ✗ | ✗ |
| Workplace surveillance laws | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Recent, upcoming, or proposed reforms | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

^ **Provision has been enacted but is not yet in force**

# Key Commercial Contracting Issues

# Commercial Contracting

- Protection of databases
  - US
    - No protection for “sweat of the brow”
    - Selection, coordination and arrangement
  - Australia
    - Labor, skill and judgement
  - UK
    - Copyright and Rights in Databases Regulation 1997

# Commercial Contracting (cont'd)

- Licensing: Contract to regulate data use with counterparty
  - Scope of use
  - License type
  - Territory

# Commercial Contracting (cont'd)

- Regulating Compliance
  - IT security
  - Confidentiality
  - Consequences of termination

# Commercial Contracting (cont'd)

- Don't forget the boilerplate
  - Assignment
  - Jurisdiction and Governing Law
  - Export Controls

# Key Take Aways

# Key Take Aways

- Stay close to the business
- Enhance privacy notices / consents
- Improve controls on data usage and information management
- Enhance policies and procedures on third party disclosures
- Consider de-identification
- Address cross-border data transfer restrictions

Baker & McKenzie

# BakerGPS (Global Privacy Strategy) – Part 23 Webinar

## Big Data and Big Data Privacy: An introduction to the conflict between the commercial value of information and global privacy requirements

**21 May 2013**