Best Practices in Global Data Privacy Issues

Presenters

Eduard Goodman, J.D., LL.M., CIPP

Chief Privacy Officer/ Identity Theft 911

- First American attorney to receive his Master of Laws (LL.M.) in International Business and Trade Law at Erasmus University Rotterdam, the Netherlands
- Member of the State Bar of Arizona and 2008-2009 Chair of its E-Commerce and Technology Practice Section
- Privacy by Design (PbD) Ambassador for the Information and Privacy Commissioner of Ontario, Canada (PbD program)

Introduction

- Data Protection and Privacy as a global trade issue
- Overview and summary of core Regional Privacy Regimes and approaches
- Brief overview of emerging regional privacy areas
- General Best Practices in Data Privacy (From a Global perspective)

Data Protection and Privacy as a global trade issue

Privacy as a Right

the United Nations Universal Declaration of Human Rights, article 12, states:

*"No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honor and reputation.* ***Everyone has the right to the protection of the law against such interference or attacks**."*

Data Protection and Privacy as a global trade issue

Privacy as a Right

Article 8 of the European Convention on Human Rights:

"***Article 8 – Right to respect for private and family life*** *…Everyone has the right to respect for his* ***private*** *and family life, his home and his correspondence…*"

Data Protection and Privacy as a global trade issue

Privacy as a Right

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
(Key Principles for National Application):

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Accountability Principle

Data Protection and Privacy as a global trade issue

The importance of analyzing the regional differences in approaches to Data Protection and Privacy:

- Differences in categorization and treatment of data types in different regions
- Differing cultural views and treatment of Privacy

Overview and summary of core Regional Privacy Regimes and approaches

North America

- United States
- Canada
- Mexico

Overview and summary of core Regional Privacy Regimes and approaches

U.S. Approach to Privacy

The U.S approach to Privacy protection can be looked at in a few different ways:

① **Protection from Government vs. Protection from third parties**

② **Protections provided by Federal Laws vs. Protection provided by State Identity Theft and Breach Notification Statutes**

③ **Statutory Protection vs. Common Law Protection**

Overview and summary of core Regional Privacy Regimes and approaches

United States

Privacy Defined

(Classic U.S. Context)

*"The makers of our Constitution… conferred, as against the government, **the right to be let alone** - the most comprehensive of rights and the right most valued by civilized men."*

--Louis Brandeis, U.S. Supreme Court Justice,
Dissent in *Olmstead v. U.S., 277 U.S. 438, 478 (1928)*.

Overview and summary of core Regional Privacy Regimes and approaches

United States

Privacy Defined

(Modern Context)

"*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*"

--Alan Westin Professor of Public Law & Government Emeritus, Columbia University

Overview and summary of core Regional Privacy Regimes and approaches

Canada-

- Federal-
  - Office of the Privacy Commissioner of Canada

- Provincial-
  - Office of the Information and Privacy Commissioner
  - Ombudsman
  - Freedom of Information and Protection of Privacy Act Review Office
  - The Commission d'accè s à l'information du Québec (the CAI)

Canada-

- Federal

1. Privacy Act, R.S.C., 1985, c. P-21
   - *Public Sector*

2. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [a.k.a. PIPEDA]
   - *Private Sector*

– *No Federal health related data protection/privacy regulations*

Overview and summary of core Regional Privacy Regimes and approaches

HOSPITALITYLAWYER.COM PRESENTS THE GLOBAL CONGRESS 2011 ON LEGAL, SAFETY & SECURITY SOLUTIONS IN TRAVEL AUGUST 25-28, 2011 HOUSTON

Canada-

- Provincial

1. **Public Sector**- *Unique/Specific Regulations in each Province*

2. **Private Sector**- *Either*:
   a) PIPEDA applies (7 Provinces); or
   b) Provincial legislation that has been found to be substantially similar to PIPEDA applies. (3 Provinces)

3. ***Medical Data**
   a) 4 Provinces have laws governing the privacy of health related data
      - ***Alberta*** *[Health Information Act (HIA)]*
      - ***Manitoba*** *[Personal Health Information Act (PHIA)]*
      - ***Ontario*** *[Personal Health Information Protection Act (PHIPA)]*
      - ***Saskatchewan*** *(Health Information Protection Act (HIPA)]*

Overview and summary of core Regional Privacy Regimes and approaches

Mexico-

- Federal Privacy Law:
  - LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES
  - (*LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES*)

Overview and summary of core Regional Privacy Regimes and approaches

Mexico-

- Went into effect July 5th, 2010
- *Supervisory authority provided by the:*
  - *Instituto Federal de Acceso a la Información y Protección de Datos*
  - (a.k.a. "the Institute for Access to Information and Data Protection")
  - *Lays out eight (8) core principles that data controllers must abide by*

Overview and summary of core Regional Privacy Regimes and approaches

Mexico-

8 core principles for data controllers to abide by under the regulation:

1. Legality,
2. Consent,
3. Notice,
4. Quality,
5. Purpose limitation,
6. Fidelity,
7. Proportionality, and
8. Accountability

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- The European Union is REALLY a treaty organization or more accurately, a "Confederation" of sovereign and distinct member nations who have agreed by treaty to delegate certain competences to common E.U. institutions or bodies.
- Comprised of 27 separate and distinct sovereign member nations comprising a single "economic zone" ensuring free movement of people, goods, services and capital.
- 16 member nations utilize the same currency.
- 23 official and working languages (with roughly 150 regional and minority languages)
- 27 distinct legal systems, almost all of which are based on the civil law system (with the exception of the U.K.)
- 27 distinct, yet overlapping histories

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- European Union Countries
  - Continental Europe
  - The U.K.
- E.U. Candidate Countries
  - Croatia
  - Former Yugoslav republic of Macedonia
  - Iceland
  - Montenegro
  - Turkey
- "Other" European Countries

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
  - (Commonly referred to as the Data Protection Directive)
- *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector*
  - (Commonly referred to as the E-Privacy Directive)
- *Directive 2009/136/EC amending Directive 2002/22/EC & Directive 2002/58/EC*
  - *(*Commonly referred to as *the "NEW" E-Privacy Directive)*

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- *Directive 95/46/EC (*the Data Protection Directive)
  - ***Transparency (Articles 10 &11)-*** There is a duty to inform the data subject when his/her personal data is processed.
  - ***Legitimacy (Article 6(b))-*** Personal data may only be processed for specific legitimate reasons and can't be further processed in a way inconsistent with those specified purposes.
  - ***Proportionality (Articles 6; 8; and 14) -*** Personal data can only be processed if the processing is considered adequate, relevant and not excessive in relation to

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- *Directive 2002/58/EC (the E-Privacy Directive)*
  - ***Updates Directive 97/66/EC*** concerning the processing of personal data and the protection of privacy in the telecommunications sector
  - ***Builds on Directive 95/46/EC*** and its principles
  - ***Application (Article 1(2))***- Covers both individuals and legal persons.
  - ***Cookies (Article 5(3))*** – "Opt out" (**meaning the consumer must be able to opt out of receiving cookies.*)
  - ***Data Retention (Article 6)***-Requires service providers to erase/anonymize data when no longer needed.
  - ***Spam (Article 13)*** "Opt in"

Overview and summary of core Regional Privacy Regimes and approaches

Europe/E.U.

- *Directive 2009/136/EC (the "NEW" E-Privacy Directive)*
  - ***Updates 2002/58/EC*** – still limited to communications providers.
  - ***Breach Notification (Article 3)***- Amends Article 4 of *Directive 2002/58/EC (the E-Privacy Directive* creating a data breach notification obligation for telecom/ISP related breaches.
  - ***National Implementation*** - May 25th of this year.

Brief overview of emerging regional privacy areas

South America

Privacy regimes in force

- **Argentina**
- **Chile**
- **Peru**
- **Uraguay**

Privacy Regimes Currently being Considered

- ***Brazil***
- ***Bolivia***
- ***Columbia***

Brief overview of emerging regional privacy areas

South America

Privacy regimes in force

- **Argentina**
- **Chile**
- **Peru**
- **Uraguay**

Privacy Regimes Currently being Considered

- ***Brazil***
- ***Bolivia***
- ***Columbia***

Brief overview of emerging regional privacy areas

South America

- **Brazil**-
  - No current Privacy Law
    - » governed by Article 5 of the 1988 Constitution
  - No Data Protection Authority
  - Not widely regarded as a privacy friendly country

Brief overview of emerging regional privacy areas

South America

- **Argentina** – *Personal Data Protection Act of 2000 (a.k.a. Habeas Data)*
  - Meets E.U. Data Directive Adequacy Standards ("*EU Adequacy Club Member*")

Brief overview of emerging regional privacy areas

South America

- **Chile** – *Law for the Protection of Private Life (Ley Sobre Protección de la Vida Privada), Law No.19628 of August 30, 1999, (Updated/amended by* Law No. 19.812 in 2002)
  - Should meet E.U. Data Directive Adequacy Standards (But the E.U. hasn't let them into the club!)

Brief overview of emerging regional privacy areas

South America

- **Peru**– the Personal Data Protection Law (*Ley de Protección de Datos Personales, Proyecto de Ley* 4079/2009-PE)
  - Passed the Congress of the Republic of Peru on June 7, 2011
    - » Establishes data processing principles: *legality, consent, proportionality, integrity, security, enforcement and (for cross-border transfers) adequate level of protection*
    - » Creates rights of: *access, correction, inclusion, correction, deletion, objection and opposition*
    - » Establish the National Personal Data Protection Authority within the Ministry of Justice

Brief overview of emerging regional privacy areas

South America

- **Uraguay**–Law No.18,331, of 13 August 2008, on the Protection of Personal Data, "Habeas Data" activity, and the Regulating Decree of 31 August 2009.
  - Granted access to the "E.U. Adequacy Club" in October of 2010

Brief overview of emerging regional privacy areas

Australasia

- Australia
- New Zealand

Brief overview of emerging regional privacy areas

Australasia

- **Australia –** *Privacy Act of 1988*
  - *Covers commonly accepted principles relating to collection, use, disclosure, security and access to personal data*
    - » *Applies to public & private entities*
    - » *Was re-evaluated in 2008 by Australian Law Commission-*
      - *Implementation numerous changes currently underway*
    - » *Enforced by the Office of the Privacy Commissioner*

Brief overview of emerging regional privacy areas

Australasia

- **New Zealand–** *Privacy Act of 1993*
  - *Covers commonly accepted principles relating to collection, use, disclosure, security and access to personal data*
    - » *Currently Evaluating a Credit Reporting Privacy Code*
    - » *Enforced by the Privacy Commissioner (a.k.a. Te Mana Matapono Matapu)*
      - *August 2nd, 2011 issued report on Privacy Reforms*

Brief overview of emerging regional privacy areas

Australasia

- **New Zealand–** *Privacy Commissioner's August 2nd, 2011 issued report on Privacy Reforms recommended:*
  - Breach notification become mandated;
  - Stronger enforcement power
  - A national "Do Not Call" register
  - Regulating surveillance, interception and electronic tracking;
  - Creating the ability to file "class action" complaints;
  - better protect people from publication of offensive or harmful material online;
  - information off-shoring issues;

Brief overview of emerging regional privacy areas

Asia

- India
- China
  - Hong Kong
- Korea

Brief overview of emerging regional privacy areas

Asia

- **India** - *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*
  - *(a.k.a. the Privacy Rules)*
  - *Considered to be most rigorous privacy regime in the world*
    - » *Potentially? Depending upon enforcement*
  - Data Protection Authority of India
    - » *Will enforce the Privacy Rules and*
    - » *Investigate data breaches*

Brief overview of emerging regional privacy areas

Asia

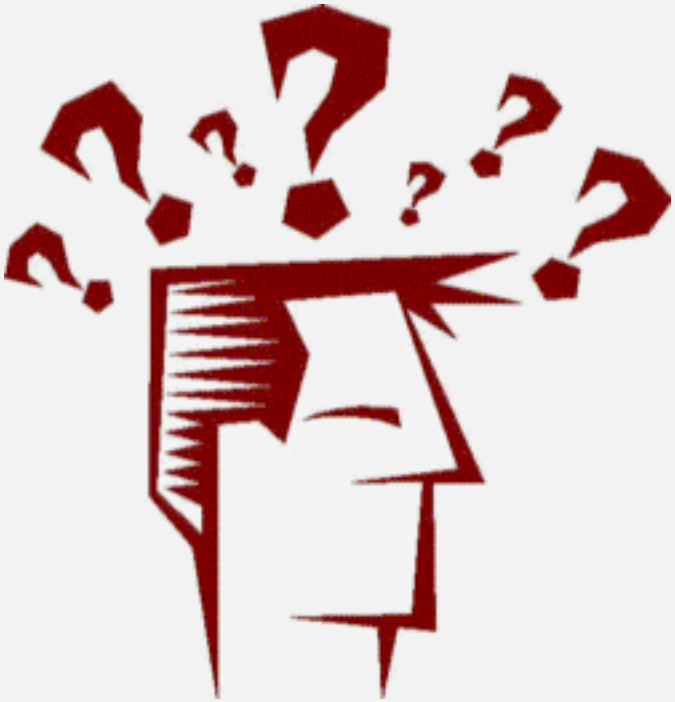
- **China**- No Overarching Privacy regime (YET?)
  - Currently early drafts of a data privacy/security rule are emerging
- ***Hong Kong***- *the Personal Data (Privacy) Ordinance (a.k.a.* "The Ordinance")
  - Enforced by the Office of the Privacy Commissioner for Personal Data, Hong Kong

Brief overview of emerging regional privacy areas

Asia

- **Korea** - *Personal Information Protection Act (a.k.a. "PIPA")*
  - *Enacted March of 2011*
  - *Requires consent for collection, use or disclosure of personal information by individual, company or government agency*
  - *Collective mediation/class action litigation*
  - *More to come as additional regulations are added*

How do I get my head around all of this??



General Best Practices in Data Privacy (From a Global perspective)

Figure out the applicable entity's "data footprint"

- What type of data is collected?
- From Whom?
- From where?
- For what Purpose?
- Who can access that Data?
- Where is data being stored, processed, etc. ?

General Best Practices in Data Privacy (From a Global perspective)

Examine regional, national, state/provincial and even municipal privacy requirements

- Is your industry regulated?
- Is privacy in the applicable jurisdiction regulated?

General Best Practices in Data Privacy (From a Global perspective)

Security

- Technical
- Administrative
- Physical

General Best Practices in Data Privacy (From a Global perspective)

Develop a "privacy framework" that governs the general practices of your business from a:

- Philosophical standpoint;
- business standpoint; and
- operational standpoint

General Best Practices in Data Privacy (From a Global perspective)

Integrate a Privacy by Design (PbD) Approach to products and services:

- 1. Proactive not Reactive;
- 2. Privacy as the Default Setting
- 3. Privacy Embedded into Design
- 4. Full Functionality -Positive-Sum, not Zero-Sum
- 5. End-to-End Security — Full Lifecycle Protection
- 6. Visibility and Transparency — Keep it Open
- 7. Respect for User Privacy — Keep it User-Centric

Conclusion/Closing

- Meeting Privacy goals from a multi-jurisdictional standpoint is possible.
- We have more in common when it comes to privacy than we have differences.
- Privacy can't be an enterprise level afterthought
- Privacy is here to stay…

Thank you

Eduard Goodman, J.D., LL.M., CIPP

Chief Privacy Officer/ Identity Theft 911

EGoodman@IDT911.com

480-355-4940