PRIVACY ASSOCIATES INTERNATIONAL LLC

International Privacy Update

Robert L. Rothman

September 25, 2013

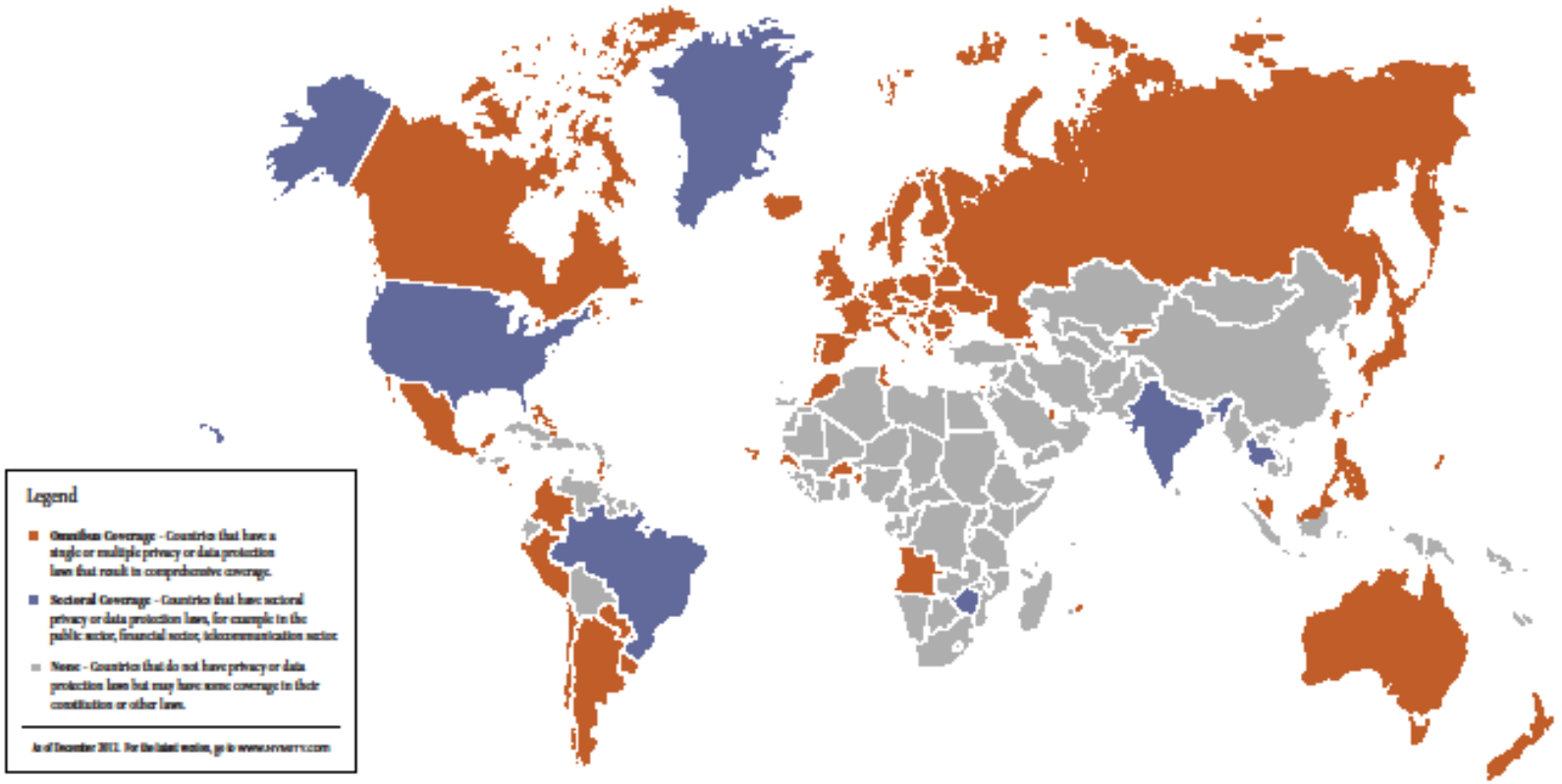
Purpose

- Provide a quick high-level refresher of selected data privacy regulation around the world

- Address selected developments and a major coming attraction in regulation

Overview of Global Privacy Regulation

Sectoral and Omnibus Privacy and Data Protection Laws



Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

Omnibus Law Countries

Albania, Andorra, Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahamas, Belarus, Belgium, Benin, Bosnia & Herzegovina, Bulgaria, Burkina Faso, Canada, Cape Verde, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guam, Guernsey, Hong Kong, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kosovo, Kyrgyz Republic, Latvia, Liechtenstein, Lithuania, Luxembourg, Macao SAR, Macedonia, Malaysia, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Senegal, Serbia, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, Trinidad & Tobago, Tunisia, Ukraine, United Kingdom, Uruguay

Sectoral Law Countries

Brazil, Dubai, Greenland, India, Singapore, Thailand, United States, Zimbabwe

Regional Privacy and Data Protection maps available at:
WWW.NYMITY.COM

The Sectoral Approach

Sectoral Approach

- Complex
- Different definitions for different laws and regulations
- Enforcement by different agencies
- USA best example

Examples of Federal Laws

- **Cable Communications Policy Act**
- **CAN-SPAM Act**
- **Children's Online Privacy Protection Act**
- **Computer Matching and Privacy Protection Act**
- **Consumer Credit Reporting Reform Act**
- **Driver's Privacy Protection Act**
- **Electronic Communications Privacy Act (ECPA)**
- **Electronic Funds Transfer Act**
- **Electronic Signatures in Global and National Commerce Act**
- **Employee Polygraph Protection Act**
- **Fair and Accurate Credit Transaction Act (FACTA)**
- **Fair Credit Reporting Act (FCRA)**
- **Family Educational Rights and Privacy Act**
- **Federal Trade Commission Act**
- **Financial Services Modernization Act (aka Gramm-Leach-Bliley)**
- **Foreign Intelligence Surveillance Act**
- **Freedom of Information Act**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Identity Theft and Assumption Deterrence Act**
- **Privacy Act of 1974**
- **Privacy Protection Act of 1980**
- **Right to Financial Privacy Act**
- **Telecommunications Act**
- **Telemarketing and Consumer Fraud Act**
- **Video Privacy Protection Act**
- **Video Voyeurism Prevention Act**

Selected ***Areas*** of State Legislation

- Identity theft protection
- Security breach notification
- Social security number protection
- Marketing
- Behavioral tracking
- Spyware and adware
- Radio frequency identification devices
- Insurance
- Vehicle data event recorders
- Background checks

The Omnibus Approach

Omnibus Approach

- Privacy legislation applicable to “personal information” in whatever context
- Often a government privacy bureaucracy in place at the national or provincial level to administer the law
- Even countries with omnibus laws may have other privacy laws
- European Economic Area (EU plus EFTA) best example
  - Laws promulgated pursuant to ePrivacy Directive, particularly for providers of electronic communication services
  - “Cookie” laws

Primary Data Protection Laws in the European Union and the EFTA

Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

EU Members

1. AUSTRIA: Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000 – DSG 2000)
2. BELGIUM: Law of December 8 1992 on the protection of privacy in relation to the processing of personal data
3. BULGARIA: Law for Protection of Personal Data
4. CYPRUS: The Processing of Personal Data (Protection of Individuals) Law 138 (I) 2001
5. CZECH REPUBLIC: Act 101 of April 4, 2000 on the Protection of Personal Data
6. DENMARK: The Act on Processing of Personal Data
7. ESTONIA: Personal Data Protection Act
8. FINLAND: Personal Data Act (523/1999)
9. FRANCE: Act n° 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties
10. GERMANY: Federal Data Protection Act
11. GREECE: Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data
12. HUNGARY: Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest

    Act No CXII of 2011 on Informational Self-Determination and Freedom of Information (Effective January 1, 2012)
13. IRELAND: An Act to give effect to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th Day of January, 1981, and for that purpose to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. [1988 Act]

    An Act to give effect to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, for that purpose to amend the Data Protection Act, 1988, and to provide for related matters. [2003 Act]
14. ITALY: Personal Data Protection Code – Legislative decree n° 196 of 30 June 2003
15. LATVIA: Personal Data Protection Law
16. LITHUANIA: Law on Legal Protection of Personal Data
17. LUXEMBOURG: Law of 31 August 2002 on the Protection of Persons with regard to the Processing of Personal Data
18. MALTA: Data Protection Act (CAP 440)
19. NETHERLANDS: Personal Data Protection Act
20. POLAND: Act on the Protection of Personal Data

    Act of 29 October 2010 amending the law on the protection of personal data.
21. PORTUGAL: Act 67/98 of 26 October – Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)
22. ROMANIA: Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data
23. SLOVAKIA: Act No. 428/2002 Coll. on Protection of Personal Data
24. SLOVENIA: Personal Data Protection Act
25. SPAIN: ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
26. SWEDEN: Personal Data Act (1998:204)
27. U.K.: Data Protection Act 1998

EFTA

1. ICELAND: Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 of May 10, 2000
2. LIECHTENSTEIN: Data Protection Act of 14 March 2002
3. NORWAY: Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)
4. SWITZERLAND: Federal Act on Data Protection (SCD) of 19 June 1992

Directives

1. General Directive

   Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
2. Directive on Privacy and Electronic Communications

   Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
3. Data Retention Directive

   Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
4. Telecoms Package and Cookie Directive

   Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

EEA Approach

- Protection “floor” set by EU Data Protection Directive 95/46/EC - actual laws and implementation details vary among states making compliance sometimes difficult
- National or provincial privacy bureaucracy to administer the law – DPA
- Requires a legal basis to “process” personal information, even domestically

EEA Approach

- “Personal information” is any information related to an identified or identifiable living natural person
- “Process” is “any operation …which is performed upon personal data…such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- Mandatory registration of databases containing personal information
- Cannot transfer personal information to a country with inadequate data protection laws unless a legal basis exists

Available Legal Bases to Allow for Domestic Processing of Personal Information

- Data subject gives unambiguous consent.
- Processing necessary for performance of contract to which data subject is party.
- Processing is necessary for compliance with legal obligation to which controller is subject.
- Processing is necessary to protect vital interest of data subject.
- Processing is necessary for performance of task carried out in public interest or exercise of official authority.
- Processing is necessary for purposes of the legitimate interests pursued by controller or by the third party/ies to whom data are disclosed, except where such interests are overridden by the interest for fundamental rights and freedoms on the data subject that require protection.

Processing Must Comply with the Certain EU Directive Principles

- The principles:
  - Notice
  - Onward Transfer
  - Choice
  - Security
  - Data Integrity
  - Access
  - Enforcement
- Much law surrounds the implementation of these concepts in each member state

Available Legal Bases to Make the Personal Information Transferable Outside the Country

- The transfer is to an entity in a country with “adequate” privacy laws (small number – does not include US)
- Data subject consents
- Transfer is made pursuant to a standard clause contract drafted by the EU
- Transfer is made pursuant to ad hoc contracts approved by the appropriate Data Protection Authority
- Transfer is made pursuant to “binding corporate rules” approved by appropriate Data Protection Authorities
- Transfer made to the US to a Safe Harbor company (technically an adequacy determination)
- Transfer is necessary for performance of a contract with the data subject
- Transfer is necessary on public interest grounds
- Transfer is necessary to protect the vital interests of data subject
- Transfer is made from a public register

Data Protection Laws of Asia Pacific

Legend

- No Law
- Data Protection Law

As of March 2013. For the latest version, go to www.nymity.com

Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

Asia Pacific Countries

1. Australia
Privacy Act 1988 (Cth)

2. China
Decision on Strengthening the Protection of Network Information

3. Hong Kong
Personal Data (Privacy) Ordinance

4. India
Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

Information Technology (Intermediaries Guidelines) Rules, 2011

5. Japan
Act on the Protection of Personal Information (Act No. 57 of 2005)

6. Malaysia
Personal Data Protection Act 2010

7. New Zealand
Privacy Act 1993

8. Philippines
Data Privacy Act of 2012

9. Singapore
Personal Data Protection Act 2012

10. South Korea
Personal Information Protection Act

11. Taiwan
Computer-Processed Personal Data Protection Law
Personal Information Protection Act

Regional Privacy and Data Protection maps available at:
WWW.NYMITY.COM

Asia-Pacific

- Sophisticated generally European-like omnibus laws in:
  - Australia
  - New Zealand
  - Singapore
  - HK
- Sectoral laws in other countries, particularly regulating the telecommunication sector
- Japan has had comprehensive law since 2003
  - Law itself very high level and purports to be omnibus
  - Implementing regulations by various Ministries in different sectors quite detailed and prescriptive

China

- At the end of 2012, the National People's Congress issued a law regulating the collection and use of personal electronic information
  - Organizations collecting personal electronic information must publish policies regarding their data practices
  - Individuals must be informed of the purpose, method, and scope of data collection
  - Organizations must obtain individuals' consent prior to collecting personal electronic information
  - Organizations must implement measures to protect individuals' personal electronic information against theft, loss, and damage
  - Organizations must refrain from selling or illegally disclosing personal electronic information
  - Organizations must take immediate remedial measures if personal electronic information is compromised.
  - Organizations must refrain from sending commercial electronic communications to a recipient's landline, mobile phone, or email address without consent

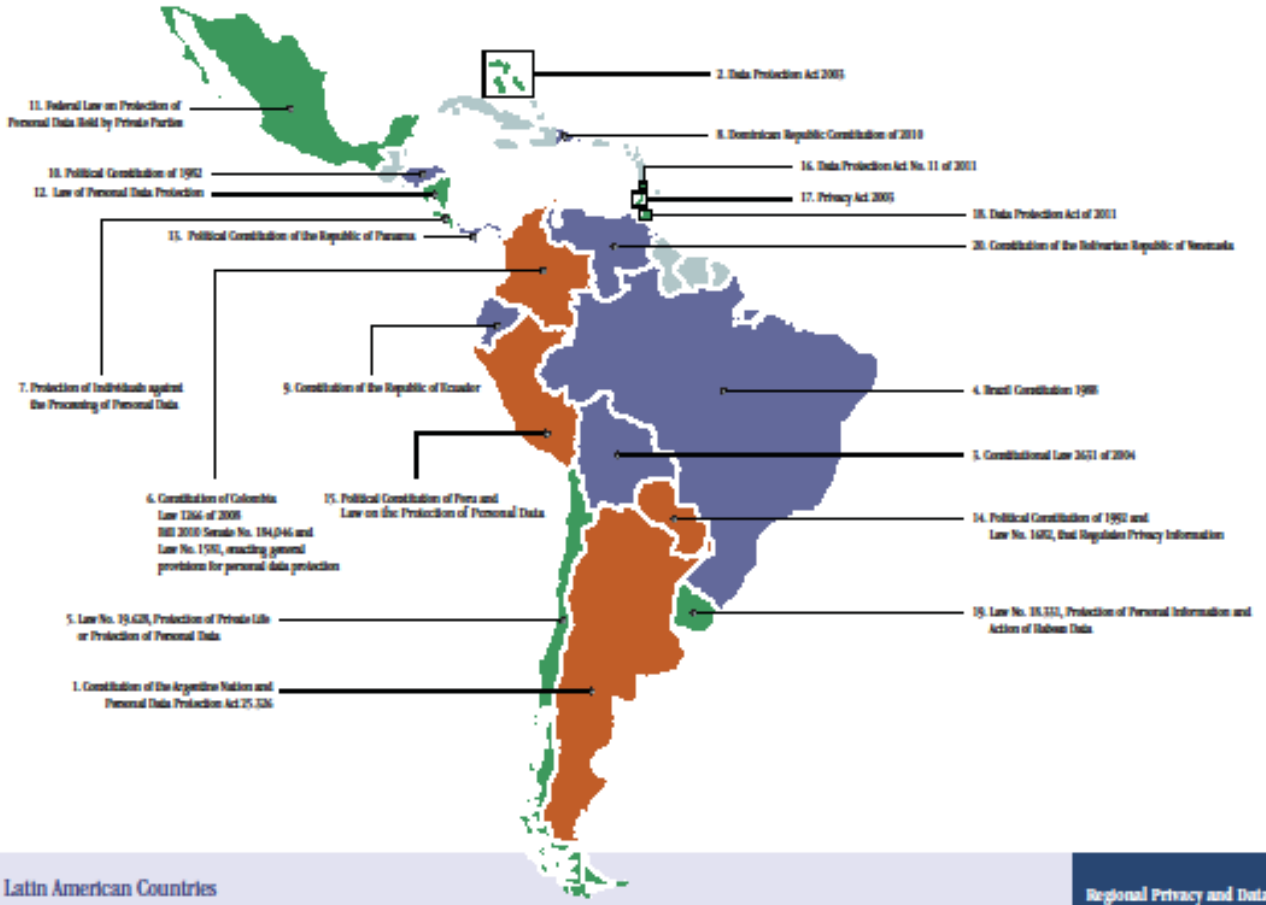
China

- In April, the People's Congress released draft amendments to the country's 20- year old consumer protection law to deal with e-Commerce issues
- In February, Ministry of Industry and Information Technology issued non-binding data privacy guidelines
  - Notify individuals of the purpose and scope of processing prior to collection;
  - Obtain individuals' consent prior to collecting information;
  - Process information only as consistent with the notice given at the time of collection;
  - Provide reasonable security measures to protect personal information;
  - Retain information no longer than as required to meet the purposes for which it was collected
  - Obtain express consent for the processing of sensitive data and for cross- border transfers of any personal information.
- Concepts may lay base for future legislation or current enforcement

India

- India's Ministry of Communications and Information Technology ("Department of Information Technology") implemented the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- Directed at the promotion of outsourcing to India
  - Contain many of the familiar concepts contained in privacy legislation, but no specific privacy bureaucracy established

Data Protection Laws of Latin America



Legend

- No Law
- Habeas Data Laws
- Data Protection Laws
- Habeas Data Laws and Data Protection Laws

As of October 2012. For the latest version, go to www.nymity.com

Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

Latin American Countries

1. **Argentina**
   Constitution of the Argentine Nation, Article 43
   Personal Data Protection Act 25.326
2. **Bahamas**
   Data Protection Act 2003
3. **Bolivia**
   Constitutional Law 2651 of 2004, Article 23
4. **Brazil**
   Brazil Constitution 1988, Article 5(LXXII)
5. **Chile**
   Law No. 19.628, Protection of Private Life or Protection of Personal Data
6. **Colombia**
   Constitution of Colombia, Article 15
   Law 1266 of 2008
   Bill 2010 Senate No. 184,046
   Law No. 1581, enacting general provisions for personal data protection
7. **Costa Rica**
   Protection of Individuals against the Processing of Personal Data
8. **Dominican Republic**
   Dominican Republic Constitution of 2010, Article 70
9. **Ecuador**
   Constitution of the Republic of Ecuador, Article 66
10. **Republic of Honduras**
    Political Constitution of 1982, Article 182
11. **Mexico**
    Federal Law on Protection of Personal Data Held by Private Parties
12. **Nicaragua**
    Law of Personal Data Protection
13. **Panama**
    Political Constitution of the Republic of Panama, Article 44
14. **Paraguay**
    Political Constitution of 1992, Article 135
    Law No. 1682, that Regulates Privacy Information
15. **Peru**
    Political Constitution of Peru, Articles 2 and 200,
    Law on the Protection of Personal Data
16. **St. Lucia**
    Data Protection Act No. 11 of 2011
17. **St. Vincent and the Grenadines**
    Privacy Act 2003
18. **Trinidad and Tobago**
    Data Protection Act of 2011
19. **Uruguay**
    Law No. 18.331, Protection of Personal Information and Action of Habeas Data
20. **Venezuela**
    Constitution of the Bolivarian Republic of Venezuela, Article 28

Regional Privacy and Data Protection maps available at:
WWW.NYMITY.COM

Latin America

- The basis of data protection laws found in the constitutions of many Latin American countries is the principle of "habeas data," which translates essentially to "you should have the data"
  - The principle gives data subjects the right to access and demand rectification or destruction of their personal data
  - Exercised by a petition to a court
- In addition to habeus data laws, there are a series of European-style data protection laws
  - Argentina (2000)
  - Uruguay (2008),
  - Mexico – a fairly business-friendly law – (2010)
  - Costa Rica, Colombia, Peru and Trinidad (2011)
  - Nicaragua (2012)
  - Brazil is now considering its own law
- While many of the concepts in these laws are familiar, details vary significantly
- Many of the laws have fairly onerous provisions
  - With the exception of Mexico, many require express, opt-in consent from the data subject in order to process data – e.g. for marketing purposes
  - Enforcement not always consistent

PAI

Canadian Privacy Laws

Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

Provincial and Territorial Commissioners' Offices

1. British Columbia
Elizabeth Denham
Information and Privacy Commissioner for British Columbia
(250) 387-5629
www.oipc.bc.ca

2. Alberta
Jill Clayton
Information and Privacy Commissioner of Alberta
(780) 422-6860
www.oipc.ab.ca

3. Saskatchewan
Gary Dickson, Q.C.
Information and Privacy Commissioner of Saskatchewan
(306) 787-8350
www.oipc.sk.ca

4. Manitoba
Mel Holley
Acting Ombudsman
Office of the Ombudsman
(204) 982-9130
www.ombudsman.mb.ca

5. Ontario
Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario
(416) 326-3333
www.ipc.on.ca

6. Québec
Me. Jean Chartier
Commission d'accès à l'information du Québec
(418) 528-7741
www.cai.gouv.qc.ca

7. New Brunswick
Anne E. Bertrand, Q.C.
Access to Information and Privacy Commissioner
(506) 453-5965
http://www2.gnb.ca/content/gnb/en/contacts/dept_resolvers.201145.html

8. Prince Edward Island
Maria C. MacDonald
Information and Privacy Commissioner of Prince Edward Island
(902) 368-4099
www.assembly.pe.ca

9. Nova Scotia
Dulcie McCallum
Freedom of Information and Protection of Privacy Review Officer
(902) 424-4684
www.foipop.ns.ca

10. Newfoundland and Labrador
Ed Ring
Information and Privacy Commissioner
(709) 729-6309
www.oipc.nl.ca

11. Yukon
Tim Keogle
Ombudsman and Information and Privacy Commissioner of the Yukon
(867) 667-8468
www.ombudsman.yk.ca

12. Northwest Territories
Elaine Keenan-Bengts
Information and Privacy Commissioner of the Northwest Territories
(867) 669-0976

13. Nunavut
Elaine Keenan-Bengts
Information and Privacy Commissioner of Nunavut
(867) 669-0976
www.info-privacy.nu.ca

Federal Privacy Acts

- PIPEDA*
- Privacy Act

Jennifer Stoddart
Privacy Commissioner of Canada
1-800-282-1376
www.privcom.gc.ca

* PIPEDA - Personal Information Protection and Electronic Documents Act

† All or part of this law is not yet in effect

Note

1. Federal works, undertakings, and businesses are exclusively subject to PIPEDA, regardless of location in Canada.
2. PIPEDA applies in all federal and provincial cross-border transfers of personal information in a commercial activity.

Selected Other Areas

- Canada
  - Personal Information Protection and Electronic Documents Act ("PIPEDA")(2000) Laws
  - Provincial legislation in Alberta, British Columbia, and Quebec often stricter than PIPEDA
  - Has an EU adequacy determination with respect to consumer privacy (but not employee privacy)
- South Africa
  - Protection of Personal Information Bill (POPI) passed by the South African National Assembly on August 20, 2013
  - Largely influenced by the UK version of the EU legislation
  - One year to comply

Changes

- EU approach predominant in the world as a starting point for nations because it is relatively self-contained and can be adapted as a whole
- As such, changes in the EU are extremely influential in the privacy space
- This is true despite the tendency of jurisdictions to frequently modify the implementation of the EU rules
  - Changing technology
  - Individual cultural norms
  - Individual and economic impacts

Selected Recent Developments

Selected Recent Developments

- Proposed EU General Data Protection Regulation
- Snowden, Prism and the Possible Demise of Safe Harbor
- Spread of American-style Breach Notification Laws

Proposed EU General Data Protection Regulation

Proposed EU General Data Protection Regulation

- Regulation intended to replace the current privacy rules established by the Data Protection Directive 95/46/EC
- Will describe the official 2012 proposal
- Numerous amendments, both strengthening and liberalizing various positions, have been suggested by MEPs and others
- European Parliament and the Council of the European Union must adopt legislation jointly
- Widely expected in Europe that "something" will be adapted; widely hoped in the US that those people are wrong
- Have been fairly comprehensive in slides, but in the interests of time will concentrate on some of my "personal favorites" (in red)

Directive vs. Regulation

Article 288 of the Treaty on the Functioning of the European Union

"To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions.

*A **regulation** shall have general application. It shall be binding in its entirety and directly applicable in all Member States.*

*A **directive** shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"*

Compliance-Related Issues

- Breach Reporting
- Consents
- Data Privacy Officers
- Impact Assessments
- Record-Keeping Requirements
- Processor Obligations
- Accountability

Breach Reporting (Art 31, 32)

- Definition of “Personal Data Breach“(Art 4(9)) broader than most US definitions
  - Definition of “Personal Data” also changed (Art 4(2))
- **Processor** must notify the controller "*immediately after establishment of a personal data breach*" (Art 26 (2)(f), Art 31(2)
- **Controller** must notify DPA within 24 hours after the personal data breach has been established
  - Art 31(3) contains a list of information that must be in the notification, most of which the controller will be unlikely to know
  - Required regardless whether the data was encrypted
- **Controller** must notify data subjects without undue delay after notifying the DPA:
  - If breach *"likely to adversely affect the protection of personal data or privacy of the data subject“*
  - Encryption relieves controller of obligation to data subjects

Consent (Art.7)

- Prior draft provision requiring “explicit” consent removed, but still is mentioned in Recital 25
- Consent cannot be relied upon as a basis for processing in situations where there is a *"significant imbalance“* between the position of the data subject and controller. Recital 34 states this includes in the employment context.
- Prior draft provision requiring consent for commercial direct marketing removed
- Burden of proof to show valid consent is on the controller
- If consent is obtained in a document dealing with other matters it must be "distinguishable in appearance" from rest of provisions (Art.7(2))
- Consent of anyone under 13 years of age for *“information society services”* requires parental approval (Art.8(1)). Reduced from 18 years in prior draft.

Data Protection Officer (Arts.35,36,37)

- Mandatory appointment of internal or external Data Protection Officer (DPO) if "enterprise":
  - Employs more than 250 persons; or
  - Is either a controller or processor and core activity involves regular monitoring of data subjects

- DPO must:
  - Be appointed based on privacy expertise and for a period of at least 2 years
  - Not have other duties that conflict with DPO responsibilities
  - Report directly to management
  - Be involved in a timely manner in all issues of personal data protection
  - Be independent and not *"receive any instructions as regards the exercise of the function."*
  - Be provided with sufficient resources, specifically *"staff, premises, equipment."*
  - Not be dismissed unless he/she does not fulfill duties of DPO

- Tasks (Art 37) generally include internal advice and education, compliance monitoring, document maintenance, breach issues, impact assessments, interacting with DPAs, etc.

Impact Assessments Art 33

- Must be carried out by the controller, or processor on its behalf, when the processing operations present "*specific risks*" by virtue of their scope, purposes or nature
- Art 33(2) lists examples of specific risks
- Includes description of processing, assessments of risks to rights of data subjects, measures to address the risks and ensure protection of the personal data and compliance with the regulation
- Must consult with affected data subjects or their representatives regarding the intended processing
- The company DPO must monitor the process (Art. 37(1)(f) and all impact statements must be furnished to DPA in final reg art 34(6)
- Prior draft provision requiring the impact assessment be made public removed

Record-Keeping Requirements Art 28

- In general, record-keeping obligations increased and shifted from DPAs to controllers and processors
- The controller, processor and any EU representative appointed by the controller must each maintain documentation of all processing operations under its responsibility
- The documentation is extensive including, for example, for each processing operation:
  - All the controllers, joint controllers and processors
  - The purposes of processing
  - The legitimate controller interests if processing is being justified by the balancing test
  - Time limits for erasures of data and means of verification
  - Transfers to third countries
  - Full list found at Art 28(2)
- Documentation must be made available to DPA upon request

Processor Obligations Art. 26

- Data processors' legal responsibilities have increased. They now have legal responsibility, regardless of contract (still required), to directly:
  - Maintain documentation of processing operations (Art 28(1))
  - Provide appropriate security (Art 26(2)(c) , Art 30)
  - Notify controllers of breaches (Art 26 (2)(f), Art 31(2)
  - Appoint a DPO (Art 35(1))
  - To obtain controller's consent prior to retaining sub-processor (Art 26(2)(d)
- A processor becomes a joint controller if it processes data beyond controller's written instructions (Arts 26(4), 26(3))
- Processors and controllers have joint and several liability to data subjects in private lawsuits for breach of Regulation, unless one can carry burden of proof that it was not responsible (Art. 77)

Accountability Art 22

- Must be able to demonstrate compliance to DPA (Arts 22(1), 29)
- Mandatory requirement to adopt policies and procedures (Arts 11, 12)
- Need verification/audit mechanism to document compliance with Regulation (Art 22(3))
- Implement security measures appropriate to risks and data (Art 30)
- Need to be able to demonstrate compliance with privacy by design and by default requirements (Art 23)

Issues Relating to Individual Rights

- Right to be Forgotten
- Profiling
- Information Controller Must Furnish
- Portability
- Privacy by Default/Design

Right to be Forgotten Art 17

- Data subjects generally have right to obtain from controller erasure of data and abstention from further dissemination
- Suppression of data not good enough, except in limited circumstances (Art 17(4))
- A controller that has made data public must take all reasonable steps to inform third parties using such data that the individual requests them to erase any links to, or copy or replication of that personal data (Art 17 (2))

Profiling Art 20

- Basic rule: Can't use *"automatic means"* to evaluate natural persons with respect to analyzing or predicting *"certain personal aspects,"* particularly:
  - Performance at work
  - Economic situation
  - Location
  - Health Personal preferences
  - Reliability
  - Behavior
- Exceptions:
  - Consent
  - Performance of the contract
  - Allowed by law

Right of Access Art 15

- Data subjects have right to obtain confirmation of whether a controller is processing their personal information
- If personal data is being processed, controller must provide all the info in Art 15(1), including:
  - Purpose of the processing
  - Categories of data
  - All recipients (or categories of recipients)
  - The period for which the info will be stored
  - Source of data information

Portability Art 18

- If a controller is electronically processing personal data, the data subject has a right to obtain his data in a commonly used electronic format
- If a controller is electronically processing personal data pursuant to either consent or a contract, the data subject can transfer that data and other related information to different controller without hindrance.

Privacy by Default/Design Art 23

- When determining how data will be processed, and during the processing, the controller must implement appropriate technical and organizational measures to assure compliance with the Regulation.
- The controller must implement mechanisms to ensure that by default only the minimum amount of personal data required for the relevant purpose is collected and it is retained only for the minimum time necessary

International Issues

- International Data Transfers
- International Discovery Demands

International Data Transfers Arts 40-45

- An adequacy determination can be made with respect to a territory within a country (California?) or a *"processing sector"* within a country (Art 41(1))
  - HIPAA?
  - Broad enough for a new Safe Harbor??
- Binding corporate rules require approval of one DPA (subject to the consistency mechanism)
  - Must be approved if all the actions in Art 43 implemented
  - Processor binding corporate rules specifically permitted
- Approval of additional standard data transfer clauses beyond the model clauses possible
  - Will old standard contractual clause agreements be valid for some period?

International Discovery Demands

Prior draft provisions requiring DPA approval to comply with foreign discovery requests eliminated

Legal Issues and Enforcement

- Fines and Enforcement
- Extra-Territorial Application of Regulation

Fines and Enforcement Arts 75-79

- Data subjects have a private right of action against controllers and processors for damages sustained from unlawful processing (Arts 75,77)
- Penalties can be adapted by member states (Art 78)
- Administrative sanctions for specific violations (Art 79):
  - First non-intentional violation: warning
  - Art 79(4) offenses: 250,000 EUR or up to .5% world turnover
  - Art 79(5) offenses: 500,000 EUR up to 1% world turnover
  - Art 79(6) offenses: 1,000,000 EUR up to 2% world turnover

(fines reduced from prior draft)

Extra-Territorial Application of Regulation

Arts 3,25

- Regulation purports to apply to the processing of the personal data of EU residents by a controller outside the EU where the processing is related to:
  - Offering goods or services to the EU residents
  - The monitoring of behavior of the EU residents
- In this situation, the controller has to designate a representative in the one of the EU states where the above activities take place (Art 25)
  - Failure to appoint a representative is an up to 2% of turnover sanction
- Regulation also purports to apply to processing where the national law of a member state applies by virtue of international public law

Snowden and the Possible Demise of Safe Harbor

Snowden and the Possible Demise of Safe Harbor

- Safe Harbor a widely-used basis for eligible US entities to justify the transfer of data from Europe to the US
  - The elements of the self-certification are within the control of the company: no governmental approval required
  - Enforcement by the FTC in the US
  - Less administrative cost than putting complex webs of contracts in place or collecting approvals of European DPAs for Binding Corporate Rules
- Europeans have never liked Safe Harbor, in large part because they have the impression many US companies are not in compliance and the FTC is not sufficiently aggressive in its enforcement activities
- A number of efforts have taken place in Europe to impose additional requirements on exporting data to US Safe Harbor companies
  - Duesseldorfer Kreis
  - Article 29 Working Group Opinion on Cloud Computing , July 2012
  - Public statements by officials
- No legal justification for any additional requirements

Snowden and the Possible Demise of Safe Harbor

- Snowden revelations suggest that the NSA is obtaining information on Europeans from Safe Harbor companies – in violation of the data security and onward transfer principles of Safe Harbor. This has added significant fuel to the fire
  - The EU Parliament claims that PRISM surveillance may have involved a "serious violation" of EU data protection laws, and that the Commission may therefore be obliged to reverse or suspend Safe Harbor
  - The MEP charged with steering the European Commission's proposed data protection reform package through the EU Parliament recommended the EU discontinue the Safe Harbor framework
  - Germany's data protection commissioners wrote a letter asking German Chancellor Merkel to recommend that the EU suspend Safe Harbor
  - EU Vice President Viviane Reding announced plans to conduct a full review of Safe Harbor by the end of this year. Safe Harbor "may not be so safe after all."

Snowden and the Possible Demise of Safe Harbor

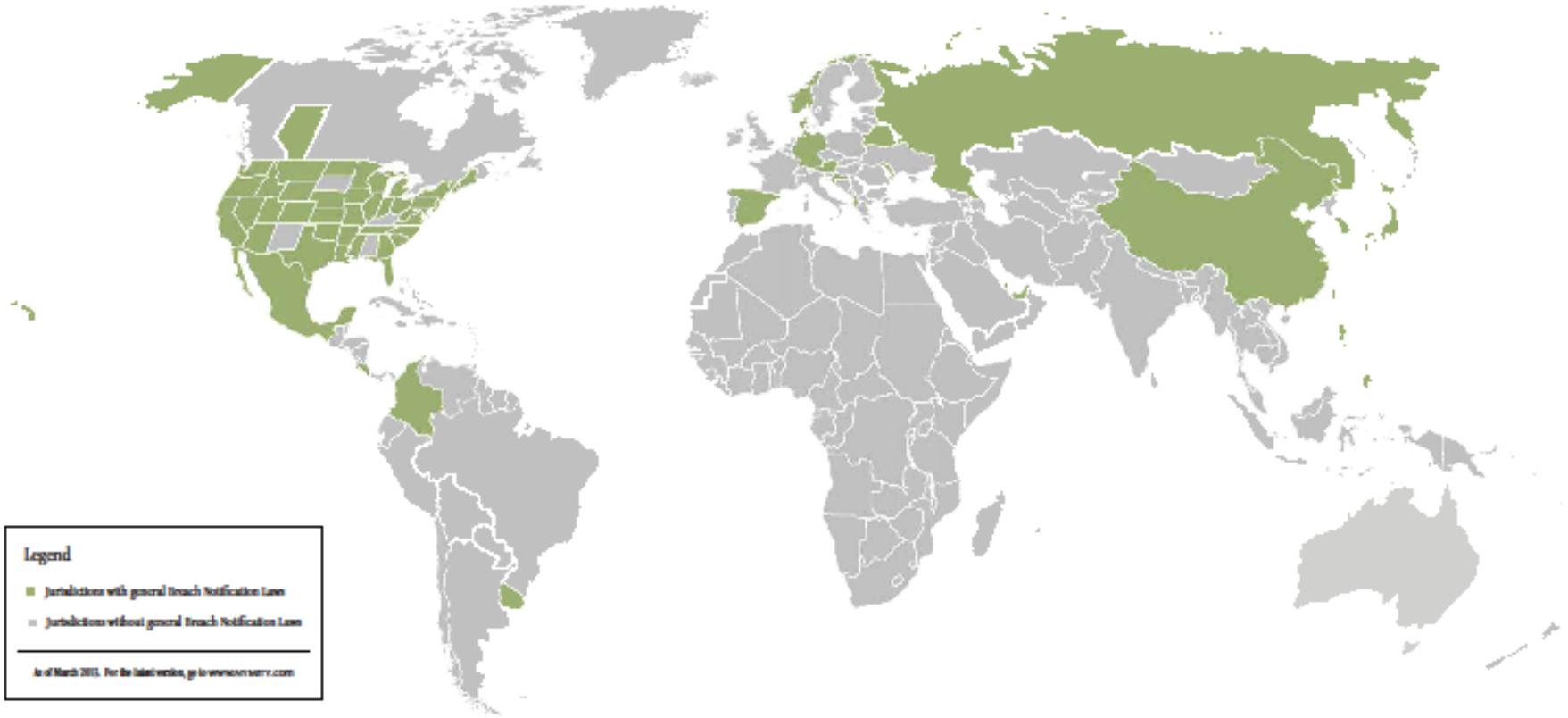
- Because of the substantial contribution that data transfers make to international trade, US wanted to include cross-border data transfer issues in the Transatlantic Trade and Investment Partnership (TTIP) negotiations aimed at establishing a free trade agreement between the U.S. and the EU.
- Europeans resisting: Germany's data protection commissioner is taking the position that the United States data protection framework is lacking and that the Safe Harbor "cannot compensate for these deficits."

Advice for US Companies

- If you are currently a Safe Harbor company, make certain you are in compliance with all the rules: there is strong pressure is on the FTC for enforcement
- If you are taking steps internally so you can become in a position to certify, keep going with your plans: if Safe Harbor goes away the new requirements will not be less strict
- Do not count on Safe Harbor in its current form to be around forever

Spread of American-style Breach Notification Laws

Global Breach Notification Laws



Produced by

NYMITY
innovating compliance

Toronto • Washington DC • Brussels

 WWW.NYMITY.COM

Jurisdictions

Albania
Austria
Belarus
Canada
- Alberta
China
Colombia
Costa Rica
Croatia
Denmark
Germany
Japan
Mexico
Moldova
Norway
Philippines
Qatar
Russia
South Korea
Spain
Taiwan
United Arab Emirates
Uruguay

United States
- Alaska
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

This map does not reflect jurisdictions that have implemented sector-specific breach notification obligations, (e.g. US - Federal, the European Union, or China) or jurisdictions whose data protection authorities or privacy regulators have recommended breach notification as a best practice (e.g., Canada, Australia, New Zealand, United Kingdom, and Ireland).

Regional Privacy and Data Protection maps available at:
WWW.NYMITY.COM

Breach Notification Laws Outside US

- ePrivacy Directive in Europe relating to telecoms requires breach notification
- Proposed EU Regulation provides for breach notification
- Often notice outside the US is first or concurrently to government officials
- May have a significance threshold
- May have broader definition of what constitutes personal information subject to notification than exists in US

Advice to Companies

- Make certain you understand the current breach notification rules in the countries in which you operate
- Design and put in place before a breach occurs a process that provides for compliance in those individual jurisdictions
- Globalize breach processes to the maximum extent possible