Privacy and Information Security Law

Randy Canis

CLASS 14 pt. 1

International Privacy Law
International Privacy Law

- Europe – omnibus privacy laws
- US – sectoral privacy laws

A. THE OECD PRIVACY GUIDELINES

Organization for Economic Cooperation and Development (OECD)

- 34 member countries including US
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) of 1980
  - Guidelines "establish eight key principles for the protection of personal information. It creates a non-binding framework that is intended to influence policymakers about privacy throughout the world."
Personal Data under OECD

- “Personal data” is defined as “any information relating to an identified or identifiable individual (data subject).”

8 Principles

1) Collection Limitation
2) Data Quality
3) Purpose Specification
4) Use Limitation
5) Security Safeguards
6) Openness
7) Individual Participation
8) Accountability

Self-Regulation and International Data Flow

- Guidelines stress self-regulation
  - “A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.”
2013 Guidelines

• 2013 guidelines update but do not replace previous guidelines
• Establishment of privacy enforcement authorities

Data Controller

• Required to establish a privacy management program
• A data controller is “a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.”

B. PRIVACY PROTECTION IN EUROPE
Europe v. US

• “Continental Europeans are consistently more drawn to problems touching on public dignity, while Americans are consistently more drawn to problems touching on the depredations of the state.”

European Convention on Human Rights

• “[W]as intended to bring violations of human rights to the attention of the international community.”
• “The Court’s judgment is binding upon the member state against which the application was brought.”

ECHR Article 8

Article 8 — Right to Respect for Private and Family Life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
Breach of Confidence Tort (England)

• “(1) the information must have ‘the necessary quality of confidence about it’;
• (2) the information ‘must have been imparted in circumstances importing an obligation of confidence’; and
• (3) there must be an ‘unauthorised use of that information to the detriment of the party communicating it.’”

European Union Data Protection Directive


EU Charter of Fundamental Rights – Article 7

• Everyone has the right to respect for his or her private and family life, home and communications.
EU Charter of Fundamental Rights – Article 8

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Controlled Data Usage

• “The Directive also gives individuals substantial rights to control the use of data about themselves. These rights include the right to be informed that their personal data are being transferred, the need to obtain ‘unambiguous’ consent from the individual for the transfer of certain data, the opportunity to make corrections in the data, and the right to object to the transfer.”

Article 25

• “The Directive extends privacy safeguards to personal data that are transferred outside of the European Union. Article 25 of the Directive states that data can only be transferred to third countries that provide an ‘adequate level of data protection.’ As a result, implementation focuses on both the adoption of national law within the European Union and the adoption of adequate methods for privacy protection in third party countries.”
Implementation of Directives

• “Directives are a form of EU law that is binding for Member States, but only as to the result to be achieved. They allow the national authorities to choose the form and the methods of their implementation and generally fix a deadline for it. Therefore, the rules of law applicable in each Member State are the national laws implementing the directives and not the directive itself. However, the directive has a ‘direct effect’ on individuals: it grants them rights that can be upheld by the national courts in their respective countries if their governments have not implemented the directive by the set deadline. A directive thus grants rights rather than creates obligations, and they are enforceable by individuals rather than by public authorities.”

20

Article 2 Definitions

• (a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); 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;

• (b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, 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;

21

• (c) “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

• (d) “controller” shall mean the natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

• (e) “processor” shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

22
Article 2 Definitions

- (f) “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
- (g) “recipient” shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- (h) “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Posting Information = Processing of Data

- “The Lindqvist court found that Mrs. Lindqvist’s posting of her website on the Internet constituted the processing of data. It found that she had illegally processed personal information as well as health information. It read the Directive’s provisions about personal data about health to extend even to a mention of a foot injury.”

Google Spain SL v. AEPD

- 2014 European Court of Justice
- Issue
  - Availability of search engine results for a real-estate auction associated with attachment proceeds for recovery of social security debts from 1998
“26. As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 Lindqvist).”

“33. It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).”

“57. As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller’s establishment on the territory of a Member State, in this instance Spanish territory.”
In the light of all the foregoing considerations, ..., the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased. …

In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.
Supervisory Authority

- Article 28 – each Member State is required to establish a public authority to monitor application of laws and regulations
- Supervisory Authority needs to have investigative powers, intervention powers, and the power to engage in legal proceedings

Notification Requirement

- “Obligation to Notify the Supervisory Authority. Under Article 18, the ‘controller’ (the entity determining the purposes of the data processing) must notify the ‘supervisory authority’ before carrying out any partly or wholly automatic processing operation. If certain conditions are met, Member States may enact rules exempting controllers from notifying the supervisory authority (or simplifying the notification).”

European Data Protection Supervisor (EDPS)

- “In 2001, the European Community promulgated Regulation No. 45/2001, which established data protection rules for the processing of personal data by Community institutions. This regulation also established the European Data Protection Supervisor (EDPS) as an independent supervisory authority with responsibility for monitoring the processing of personal data by Community institutions. The EDPS has a further role in advising European institutions and national supervisory authorities on new legislation, new technology, and international developments. Finally, the EDPS has legal authority to intervene in actions before the European Court of Justice.”
C. INTERNATIONAL TRANSFERS OF DATA

Balancing

- Cross-border information flow v. individual privacy

International Flow of Personal Data

- "Article 25 governs when Member States may permit the flow of personal data to other countries. This provision has particular relevance for the United States, because it governs the level of privacy protections other countries must have in place for data transfers to occur".
Article 7

- Processing restrictions
  - Explicit consent
  - Performance of or entry into a contract
  - Compliance with a legal obligation
  - Protection of vital interests
  - Public interest or exercise of official duties
  - Balancing of the legitimate interests of controller

Article 25(1)

- The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Article 25(2)

- The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
Derogations/Exceptions

- “Transfers of personal data to a third-party country that does not ensure an adequate level of protection under Article 25(2) may still take place on condition that the data subject has unambiguously consented, the transfer of data is ‘necessary in order to protect the vital interests of the data subject,’ or the transfer serves ‘important public interest grounds.’ There are several additional exceptions.
- A Member State may also authorize transfers of personal data to third countries without an adequate level of protection where protection of the privacy and individual freedoms ‘result from appropriate contractual clauses.’”

Blocking

- “Pursuant to Article 25 of the EU Directive, transfers of personal data about European citizens can be blocked if third party countries (such as the United States) do not provide ‘an adequate level of protection.’”
- “The European Directive requires the national supervisory authorities in each of the Member States and the European Commission to make comparisons between European data protection principles and foreign standards of fair information practice. The European Directive further requires that foreign standards of fair information practice be ‘adequate’ in order to permit transfers of personal information to the foreign destination.”

US Safe Harbor Enactment

- “In 1998, the U.S. Department of Commerce began negotiations with the EU Commission to formulate a ‘safe harbor’ agreement to ensure that the United States met the EU Data Directive’s ‘adequacy’ requirement in Article 25. In July 2000, the negotiations yielded the Safe Harbor Arrangement as well as other supportive documents elaborating on the principles, such as letters and a list of Frequently Asked Questions.”
- Safe Harbor agreement approved by the Commission in 2000.
Safe Harbor Principles

• Notice
• Choice
• Onward Transfer
• Security
• Data Integrity
• Access
• Enforcement

Notice

• “An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.”

Choice

• “An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.”
Choice

- "For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive."

Safe Harbor Certification

- Comply with safe harbor privacy principles and FAQs
- Publicly disclose privacy policies
- Subject to FTC (or other gov’t org) for compliance enforcement

Schrems v Data Protection Commissioner

- Office of Advocate General
- September 2015
Schrems v Data Protection Commissioner

- "Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. That decision provides a legal basis for the transfer of personal data from the European Union to undertakings established in the United States that adhere to the safe harbour principles."

Schrems v Data Protection Commissioner

- "[T]he principle stated in Article 25(1) is that the transfer to a third country of personal data which is undergoing processing or is intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection of such data."

Schrems v Data Protection Commissioner

- "Under Article 25(6) of that directive, the Commission may find that a third country ensures an adequate level of protection of personal data by reason of its domestic law or of the international commitments it has entered into. If the Commission adopts a decision to that effect, the transfer of personal data to the third country concerned may take place."
14. The safe harbour scheme is based on a solution combining self-certification and self-assessment by private organisations and intervention by the public authorities.

15. The safe harbour principles were developed `in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates`.

17. A United States organisation wishing to adhere to the safe harbour principles is required to state in its privacy policy that it discloses the fact that it adheres to those principles and in fact complies with them and to self-certify by declaring to the United States Department of Commerce that it complies with those principles.

Nature of complaint

- Schrems is an Austrian national who uses FB
- FB Ireland users servers based in the US
- US offers no real protection against State surveillance (as shown after Snowden revelations)
30. In this instance, the Commissioner concluded that Mr Schrems’ complaint was ‘frivolous or vexatious’, in the sense that it was bound to fail because it was unsustainable in law. It was on that basis that the Commissioner refused to investigate the complaint.”

Schrems v Data Protection Commissioner

Mr Schrems brought proceedings before the High Court for judicial review of the Commissioner’s decision rejecting his complaint. … the High Court states that, if the present case were to be approached solely on the basis of Irish law, a significant issue would arise as to whether the United States ‘ensures an adequate level of protection for the privacy and the fundamental rights and freedoms’ of data subjects, within the meaning of section 11(1)(a) of the Data Protection Act. It follows that, on the basis of Irish law, and in particular of its constitutional requirements, the Commissioner could not have rejected Mr Schrems’ complaint, but would have been required to examine that issue.”

Schrems v Data Protection Commissioner

[T]he guarantee enshrined in Article 7 of the Charter and by the core values common to the traditions of the Member States would be compromised if the public authorities were allowed access to electronic communications on a casual and generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individuals concerned and attended by appropriate and verifiable safeguards.”
Schrems v Data Protection Commissioner

• “[I]n order to ensure appropriate protection of the fundamental rights of individuals with regard to the processing of personal data, the national supervisory authorities must have the power, where there are allegations regarding infringement of those rights, to conduct investigations. If, following such investigations, those authorities consider that, in a third country covered by an adequacy decision, there are strong indications of a breach of the right of citizens of the Union to the protection of their personal data, they must be able to suspend the transfer of data to the recipient established in that third country.”

Schrems v Data Protection Commissioner

• “159. Those findings of fact demonstrate, in my view, that Decision 2000/520 does not contain sufficient guarantees. Owing to that lack of guarantees, Decision 2000/520 has been implemented in a manner that does not satisfy the requirements of the Charter or of Directive 95/46.”

Schrems v Data Protection Commissioner

• “In the light of the conditions thus laid down that must be satisfied in order for limitations on the exercise of the rights and freedoms protected by the Charter to be accepted, I find it extremely doubtful that the limitations at issue in the present case may be regarded as respecting the essence of Articles 7 and 8 of the Charter. …”
Schrems Timeline

- 6/25/13 – Complaint filed to Irish Data Protection Authority by Schrems
- 6/18/14 – Irish high court refers complaint to the European Court of Justice (RCJ)
- 9/23/15 – AG opinion suggests the safe harbor invalid [per slides above]
- 10/6/15 – Court of Justice of the European Union (CJEU) invalidates the safe harbor [per slide below]

Court of Justice of the European Union

- Decision 2000/520 is invalid.
- Supervisory authority of member state can examine a claim “concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.”

D. THE APEC PRIVACY FRAMEWORK
Cooperative Members

- United States, China, Japan, the Russian Federation, China, Australia, New Zealand, Peru, Indonesia, Mexico, Singapore, Thailand, and Vietnam.

Implementation

- Like OECD guidelines
- Allows for exceptions to its principles
  - National sovereignty, national security, public safety, and public policy

Principles

1) preventing harm;
2) notice;
3) collection limitation;
4) use of personal information;
5) choice;
6) integrity;
7) security safeguards;
8) access and correction; and
9) accountability.
Cross Border Privacy Rules (CBPR)

- Voluntary accountability-based system
- Elements
  - (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.
- US, Japan, and Mexico are participating

E. PRIVACY PROTECTION IN NORTH AMERICA

Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000
  - "PIPEDA requires that the individual must consent prior to the collection, use, or disclosure of personal data. See id. sched. 1, §4.3. It also incorporates the OECD purpose specification principle, security safeguard principle, openness principle, accountability principle, and data quality principle, among others. PIPEDA has an unusual structure with its core found in its Schedule 1, which reprints most of the CSA Model Code."
Canada Anti-Spam Law (CASL)

- Effective in 2014
- CASL “prohibits sending unsolicited commercial emails. As a general matter, CASL requires express consent from a recipient before sending commercial emails. CASL does recognize, however, implied consent in situations where sender and recipient have an existing business relationship.”

Mexico

- Mexican Constitution contains an explicit guarantee of privacy in private communications since 1996
- Federal Data Protection Act (FDPA) of 2010
  - Includes Habeas Data
- Privacy Notification Guidelines (2013)
  - Establish requirements for obtaining consent and providing privacy notices before data collection

F. PRIVACY PROTECTION IN SOUTH AMERICA
Argentina

- **Habeas data** – “permits any person to know the content and purpose of the data pertaining to her in public records, or in certain private records”
- Prohibits international transfer of PI to countries without adequate protection

Brazil

- Constitution explicitly protects privacy
- Habeas data

G. PRIVACY PROTECTION IN AFRICA AND THE MIDDLE EAST
Africa

• A number of countries now have data protection laws
• South Africa
  – 1996 Constitution grants a right to privacy
  – 2013 Protection of Personal Information Act

The Middle East

• Some Arab countries mention privacy
• 2002 Dubai law restricts ISPs from disclosing customer data
• Israel
  – Article 7 provides for a right to privacy
  – Privacy Protection Act of 1981
    • Applies to public and private sector
    • Prohibits use of information in a database for purposes beyond for which it was established

H. PRIVACY PROTECTION IN ASIA-PACIFIC
Australia

- Privacy Protection Act of 1988 based on OECD Privacy Guidelines
  - Applies only to the public sector
- Privacy Amendment Act of 2000
  - Applies to the private sector
- Additional amendments became effective March 2014
  - Regulates handling of personal information and credit reporting

Japan

- Personal Data Protection Act effective 2005
  - Personal information may be collected with a purpose of use that cannot be exceeded
  - Right to request disclosure of stored personal information on the user

China

- Protections for privacy include defamation, home intrusion, and correspondence monitoring
- Extensive citizen monitoring
- Yinsi (shameful secret)
- 2011 draft guidelines for information security technology
Hong Kong

- Information privacy statute enacted in 1996
  - Regulates public and private sector
  - Privacy commissioner
- Revisions to Personal Data Ordinance in 2013
  - Consent required prior to use of personal data in targeted marketing

South Korea

- Personal Information Protection Act effective 2012
  - Applies to public and private sector
  - Requires Privacy Compliance officers, notification of data breach, only minimum collect of personal information occur

India

- Constitutional right to privacy
- 2008 IT Security Act
  - First Indian data privacy law
    - Requires establishment of a privacy policy and more
Program Completed

All course materials - Copyright 2015 Randy L. Canis, Esq.