Privacy Requirements in a Worldwide Context

Yves LE ROUX CISM CISSP
Chair of the ISACA Privacy Task Force
CA Technologies
Yves.leroux@ca.com
• What is privacy?
• Different types of privacy => different types of requirements
• Multicultural issue: Starting from EU to Worldwide
• Some new developments: Cloud, Mobile, BYOD, Big Data
• Seven types of privacy
  – the person (physical body)
  – behaviour and action
  – communication
  – data and image
  – thoughts and feelings
  – location and space
  – association (including group privacy).

Source: “European data protection: coming of age?” edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet
<table>
<thead>
<tr>
<th>Type of privacy</th>
<th>Whole body imaging scanners</th>
<th>RFID-enabled travel documents</th>
<th>Unmanned aircraft systems</th>
<th>Second-generation DNA sequencing</th>
<th>Human enhancement technology</th>
<th>Second-generation biometrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy of the person</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of behaviour and action</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of data and image</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of thought and feelings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of location and space</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Privacy of association</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
The OECD Privacy Guidelines 1980

Organisation for Economic Co-operation and Development (OECD) 34 countries

• Eight basic principles:
  – Collection Limitation Principle
  – Data Quality Principle
  – Purpose Specification Principle
  – Use Limitation Principle
  – Security Safeguards Principle
  – Openness Principle
  – Individual Participation Principle
  – Accountability Principle
9 September 2013 OECD Privacy Framework published “Basic Principles” of the guidelines remain intact

New concepts introduced:

- Privacy management programmes
- Data security breach notification
- Privacy enforcement authorities
- Transborder flows of personal data
- National implementation
- International co-operation and interoperability
- Improving the evidence base for policy making

FOCUS ON THE EUROPEAN UNION
The right to privacy or private life is enshrined in:

- The Universal Declaration of Human Rights (Article 12),
- The European Convention of Human Rights (Article 8) and
- The European Charter of Fundamental Rights (Article 7 and 8).
Directive 95/46/EC of 24 October 1995

- This Directive applies to data processed by automated means and data contained in or intended to be part of non automated filing systems.
- The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful.
• The guidelines relate to:
  – the **quality** of the data
  – the **legitimacy** of data processing
  – special **categories** of processing
  – **information** to be given to the data subject
  – the data subject's **right of access** to data
  – **exemptions and restrictions**
  – the **right to object** to the processing of data
  – the **confidentiality and security of processing**
  – the **notification** of processing to a supervisory authority
The issue with a Directive

• Directives bind Member States as to the objectives to be achieved within a certain time-limit, while leaving to the national authorities the choice of form and means.

• Directives have to be implemented in national legislation in accordance with the procedures of the individual Member States.
European Union
28 countries
24 official languages
28 different national legislations
Under the current Data Protection Directive 95/46/EC, a company operating in more than one EU country will have to deal with several Data Protection Authorities (‘DPAs’) with very different powers (up to one per Member State).

This leads to uncertainty for business and situations where different rules can apply in each Member State for the same operation.

There is no system to reconcile different DPA decisions apart from a non-binding discussion in the so-called Art 29 Committee, which brings together EU DPAs.
<table>
<thead>
<tr>
<th></th>
<th>Denmark</th>
<th>France</th>
<th>Germany</th>
<th>Italy</th>
<th>The United Kingdom</th>
<th>Data Protection Directive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial notification</td>
<td>X 135 euro</td>
<td>X</td>
<td>Only processing of personal data permanently to third party</td>
<td>Only some specified processing 150 euro</td>
<td>X 50 euro</td>
<td>X</td>
</tr>
<tr>
<td>Annual notification</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>X 50 euro</td>
<td>--</td>
</tr>
<tr>
<td>Exemptions from notification</td>
<td>Medium</td>
<td>Some</td>
<td>High</td>
<td>High</td>
<td>Some</td>
<td>X</td>
</tr>
<tr>
<td>Simplification of notification</td>
<td>--</td>
<td>X</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>Appoint data protection official</td>
<td>--</td>
<td>Voluntary, replaces notification</td>
<td>Obligatory, replaces notification</td>
<td>--</td>
<td>Voluntary, replaces notification</td>
<td></td>
</tr>
<tr>
<td>Detailed security regulations for the public sector</td>
<td>X</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Prior checking of specific processing operations</td>
<td>X</td>
<td>X</td>
<td>Prior checking is the responsibility of the data protection</td>
<td>X</td>
<td>A possibility, but no processing are made subject to prior checks</td>
<td>X</td>
</tr>
<tr>
<td>Authorisation of transfer to third countries</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
International Transfers

• Adequate Countries
  – 27 EU countries and three EEA member countries
  – Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay

• United States - Safe Harbor and Transfer of Air Passenger Name Record (PNR) Data

• Standard contractual clauses

• Binding Corporate Rules
25 January 2012

• European Commission issues two legislative proposals:
  – a Regulation setting out a general EU framework for data protection and
  – a Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.
Key changes in the reform include:

- A single set of rules on data protection, valid across the EU
- Organisations will only have to deal with a single national data protection authority in the EU country
- Right to be forgotten
- Right to portability
- Breach reporting rules (within 72 hours)
- Principle of Accountability – obligation to demonstrate compliance – including internal policies e.g. DPO for >250 employees
- Principle of transparency (e.g. easy access to information on data handling)
- Right to information on data handling practices
- Privacy by default and privacy by design introduced as principles.
- New rules on international transfers (BCRs/Model Clauses for bilateral agreements)
The proposals have turned out to be something of a political hot potato, with many of the proposals receiving political attention throughout Europe. Laws like this in Europe need the consensus of three separate bodies to become law:

– The European Commission (in this case, the proposer of the new laws),
– The European Parliament and
– The Council of the European Union ("the Council").
• EU member states take turns presiding over the Council.
• Ireland has tried to bring some sense to the European Commission's proposals and at the end of May, released a draft compromise text that deals with some of the flaws in the original proposed Regulation.
• Reports from Paris suggest that the Irish compromise would still not be acceptable to France. Belgium, Germany, Italy and Spain may also still have concerns.
• After the Irish Presidency, Lituania has taken over on July 1st 2013.
• In the European Parliament, well over 4,000 amendments have been tabled.

• Ideological and political divisions emerge among European Parliament political groups as they debate amendments on the draft EU data protection bill.

• As a result, the orientation vote on the EU's data protection regulation will take place either in September or October. The vote was originally intended in early 2013.
• Thereafter (depending on progress in the Council of Ministers) Negotiations between European Parliament, Council and Commission (Trilogue)
• Expected adoption in 2015 or even 2016
• Expected enforcement two years after the adoption
OMNIBUS VS. SECTORAL APPROACHES
• An omnibus statute establishes regulatory standards for a large field, which can, in many countries, sweep in the entire public and private sectors.

• In contrast, a sectoral law has jurisdiction over a specific context of information use.

• U.S. information privacy law has taken a sectoral approach while European information privacy law has centered on omnibus laws.
U.S.A.
United States prefers what it calls a 'sectoral' approach to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather than governmental regulation alone. Privacy legislation in the United States tends to be adopted on an ad hoc basis, with legislation arising when certain sectors and circumstances require. The U.S. now has fairly restrictive rules governing the collection and distribution of health and financial data, but few constraints in areas such as online marketing.
ASIA-PACIFIC ECONOMIC COOPERATION (APEC)
• In 2004, the APEC Privacy Framework was endorsed by APEC Ministers.
• In November 2009, an APEC Cross-border Privacy Enforcement Arrangement (CPEA) was endorsed by APEC Ministers. It creates a framework for regional cooperation in the enforcement of Privacy Laws.
APEC Privacy Principles:

- Preventing Harm
- Notice
- Collection Limitation
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- Security Safeguards
- Access and Correction
- Accountability
<table>
<thead>
<tr>
<th>Economy</th>
<th>IAP (Word)</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Canada</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Japan</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Korea</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Yes</td>
<td>2010</td>
</tr>
<tr>
<td>Mexico</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Yes</td>
<td>2011</td>
</tr>
<tr>
<td>Peru</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Philippines</td>
<td>Yes</td>
<td>2009</td>
</tr>
<tr>
<td>Singapore</td>
<td>Yes</td>
<td>2006</td>
</tr>
<tr>
<td>Chinese Taipei</td>
<td>Yes</td>
<td>2011</td>
</tr>
<tr>
<td>Thailand</td>
<td>Yes</td>
<td>2011</td>
</tr>
<tr>
<td>United States</td>
<td>Yes</td>
<td>2006</td>
</tr>
</tbody>
</table>
APEC Cross-Border Privacy Rules System

This voluntary, certification-based system promotes a consistent baseline set of data privacy practices for companies doing business in participating APEC economies. APEC Economic Leaders endorsed the system in November 2011. United States and Mexico are the first participants.
CONCLUSION ON REGULATIONS
More than 90 countries were reported to have adopted data protections laws and the number continues to increase.

Companies are faced with somehow harmonizing these laws into coherent and workable data protection compliance programs.

To make matters worse, these international laws in many cases appear to combine the most demanding aspects of both the EU and U.S. approaches—stringent requirements and vigorous enforcement.
HOT TOPICS
Workplace Privacy

• In the United States and many third-world countries, workers have very few privacy protections in law.
• European employers are bound by comprehensive data protection acts that limit and regulate the collection of personal information on workers. Employees have legitimate expectations that they are entitled to a degree of privacy in the work environment.
Monitoring at work in Europe

When, for example, you video workers, check telephone logs to detect excessive private use, monitor e-mails or check internet use, workers should be aware of the nature, extent and reasons for any monitoring unless, exceptionally, covert monitoring is justified.
Bring your own device (BYOD) in Europe

• The data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing.

• Data controllers must also remain mindful of the personal usage of such devices and technical measures used to protect personal data must remain proportionate to and justified by real benefits that will be delivered.
Cloud Computing in Europe

- Cloud clients may no longer be in exclusive control of this data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data.
- Article 29 WG Opinion 05/2012 on Cloud Computing Guidelines for clients and providers of cloud computing services
• **Data controller** means the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data.

• **Data processor** means the natural or legal person, public authority, agency or any other body that alone or jointly with others, processes personal data on behalf of the controller.
• The Cloud Client as a controller must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in Directive 95/46/EC.

• The cloud provider is considered as a data processor
• “The imbalance in the contractual power of a small controller with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law”
Businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. This analysis must address the risks related to processing of data in the cloud by having regard to the type of data processed in the cloud.
<table>
<thead>
<tr>
<th>Personal data</th>
<th>Personal data creation</th>
<th>Storage, aggregation</th>
<th>Analysis, productisation</th>
<th>Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volunteered</td>
<td>Mobile phones, smart phones</td>
<td>Apps, OS for PCs</td>
<td>Web retailers</td>
<td>End users</td>
</tr>
<tr>
<td>Declared interests</td>
<td>Desktop PCs, laptops</td>
<td>Apps, OS for mobile phones</td>
<td>Internet tracking companies</td>
<td>Government agencies and public organisations</td>
</tr>
<tr>
<td>Preferences</td>
<td>Communication networks</td>
<td>Apps for medical devices</td>
<td>Internet search engines</td>
<td>Ad exchanges</td>
</tr>
<tr>
<td>...</td>
<td>Electronic notepads, readers</td>
<td>Apps for consumer devices/appliances</td>
<td>Electronic medical records providers</td>
<td>Medical records exchanges</td>
</tr>
<tr>
<td>Observed</td>
<td>Smart appliances</td>
<td>Network management software</td>
<td>Identity providers</td>
<td>Business intelligence systems</td>
</tr>
<tr>
<td>Browser history</td>
<td>Sensors</td>
<td></td>
<td>Mobile operators, Internet service providers</td>
<td>Credit bureaus</td>
</tr>
<tr>
<td>Location</td>
<td>Smart grids</td>
<td></td>
<td>Financial institutions</td>
<td>Public administration</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
<td>Utility companies</td>
<td>Large enterprises</td>
</tr>
<tr>
<td>Inferred</td>
<td>...</td>
<td></td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Follow us: @ISACANews #ISACAEU © 2013 ISACA. All Rights Reserved.
Some issues with Data Brokers

- Information brokers may not offer a method of opting-out
- Information brokers may charge a fee to suppress information from their databases
- Personal information that has been removed from a particular database may be re-posted online at a later date when the company downloads a new batch of information.
Several Global Privacy Enforcement Network (GPEN) members from countries around the world are taking steps currently to ensure that companies meet their obligations related to the privacy of consumers’ personal information.

In May 2013, ten companies received a warning letter from the FTC reminding them to evaluate their practices to determine whether they are consumer reporting agencies, and if so, how to comply with the Fair Credit Reporting Act (FCRA).
If you’ve done nothing wrong...

then you’ve nothing to worry about.
Law Enforcement Access to Personal Information

- Both international governments and the world's biggest tech companies are in crisis following the leaking of documents that suggest the US government was able to access detailed records of individual smartphone and internet activity, via a scheme called Prism.
- This PRISM disclosure was published by The Guardian and The Washington Post on June 6, 2013.
- In the United Kingdom, Government Communications Headquarters (GCHQ) has its own surveillance program TEMPORA

Source: Nimity www.nimity.com
Introduction

U.S. as World’s Telecommunications Backbone

- Much of the world’s communications flow through the U.S.
- A target’s phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can’t always predict the path.
- Your target’s communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011
Source: Tele geography Research
Dates When PRISM Collection Began For Each Provider

- Microsoft: 9/11/07
- Yahoo: 1/14/09
- Google: 6/3/09
- FaceBook: 12/7/09
- PalTalk: 9/24/10
- YouTube: 2/6/11
- Skype: 3/31/11
- AOL: (added Oct 2012)
- Apple: (added Oct 2012)

PRISM Program Cost: ~ $20M per year
PRISM Collection Details

Current Providers
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page:
Go PRISMFAA
“The NSA's filtering programs, code-named Blarney, Fairview, Oakstar, Lithium and Stormbrew, among others, filter and gather information at major telecommunications companies. This filtering takes place at more than a dozen locations at major Internet junctions in the U.S., officials say. The surveillance system is built on relationships with telecommunications carriers that together cover about 75% of U.S. Internet communications. They must hand over what the NSA asks for under orders from the secret Foreign Intelligence Surveillance Court. The firms search Internet traffic based on the NSA's criteria, current and former officials say.”

Source: Wall Street Journal  2013-08-20
The NSA system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say. The NSA's filtering, carried out with telecom companies, is designed to look for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the U.S."

Source: Wall Street Journal   2013-08-20
How the NSA collects your data

**Sources**

- AT&T
- Verizon
- Sprint
- Facebook
- Apple
- Google
- Microsoft
- Yahoo
- AOL

**Telecommunications Cables**

- Patriot Act: Section 215

**NSA**

- Fairview, Stormbrew, Blarney, and Oakstar ("Upstream" Data)
- Mainway (Phone Metadata)
- Nucleon (Phone Content)
- Prism (Internet Content)
- Shelltrumpet & Evilolive (Internet Metadata)
- Marina (Internet Metadata)
- Moonlightpath (Internet Metadata, planned Sept. 2013)
- Spinnaret (Internet Metadata, planned Sept. 2013)

**GCHQ**
Data collected from sources
The NSA gets much of its communication information from companies

- **Phones**
  - The NSA can gather phone-call data.

- **Prism**
  - Stored content from Internet firms, aimed at foreign targets.

- **Internet backbone**
  - Monitors certain streams of Internet traffic, through legal relationships with telecom companies.

Internet data sorted
The NSA filters out the data it needs

- **Filtering System**
  - Companies such as Narus make technology that filters large streams of Internet traffic. The system aims at communications where at least one person is overseas.

Main databases
Data goes into NSA databases.

- **Main databases**
  - Data goes into NSA databases.

- **Information might also go to an analyst for study in real time.**

- **Query programs**
  - Software for analysts to spot links or patterns in piles of data.

- **Analyst**
  - Gives instructions to the filtering algorithms, gets information from databases and studies the data.

- **Reports**
  - Final reports are stored in databases named Maui and Anchory.

- **NSA Processing**
  - Systems including one called Xkeyscore take 'selectors,' such as email addresses sent by analysts, develop filtering rules and send information back.
• The EU's Justice Commissioner has written to the US attorney general, questioning him about America's data surveillance programme, Prism. She was concerned America's efforts "could have grave adverse consequences for the fundamental rights of EU citizens".

• Germany's justice minister has written to British ministers seeking information about allegations of mass surveillance by British intelligence.
CONCLUSION
In Privacy as in others matters, Security People are facing the upheaval and must pilot the security boat to the objectives fixed by the Board.
Privacy Requirements in a Worldwide Context

Yves LE ROUX CISM CISSP
Chair of the ISACA Privacy Task Force
CA Technologies
Yves.leroux@ca.com