

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Terra Incognita

Auditing for Privacy Workshop: Chairman's Remarks

2007 International Data Protection and
Privacy Commissioner's Conference
Montreal, Quebec, Canada

Workshop # 3 – Audit
Wednesday, September 26, 2007
1:30 – 4:00 pm

Dr. Artemi Rallo Lombarte
Director, Spanish Data Protection Agency

What is Auditing?

- Audit vs. Inspection
 - Audit – initiated by DPA or data controller
 - proactive overview to establish **general compliance**, usually results in recommendations
 - Inspection – in response to a complaint or DPA concern
 - investigation of a **specific area** of suspected breach, can result in sanctions
- Effective enforcement requires both proactive and reactive components
 - In the context of this panel, we'll refer generally to “auditing” – an inclusive idea

Spanish Auditing Process

- **20% Preventive Enforcement**
 - **Systematic audits** – public and private sectors
 - Results in recommendations, but issue a Resolution too
 - Includes non-audit actions: guidelines, consultations, publicity
 - **80% Reactive Enforcement**
 - Law mandates AEPD to **resolve every citizen complaint**
 - Usually resolved with request for voluntary information submission
 - **can search *in situ* or issue subpoenas**
 - fines assessed for violations – based on nature of infraction as minor, serious, or very serious as defined by law
- **Inspection** by IT experts - submit factual report to Legal Department
- **Legal Department** analyzes report, initiates sanction procedures if needed, makes recommendation for Resolution
- **Director** approves Resolution; appealable in court

Collaborative Enforcement: Bilateral Cooperation in the EU

- 2000 – AEPD fines a content provider for posting personal data of police officers on its website
 - No fine to ISP – content removed immediately upon injunction
- 2006 – notification that content still exists on a Dutch mirror site
 - **Collaboration with NL DPA (CBP) to remove content**
 - CBP sent an information request to the Dutch ISP, with attached AEPD Resolution on illegality of data
 - **Immediate removal** of content by ISP

Cooperative strategy and tools

- **Exchange of information** on Spanish action and outcomes
- **Investigation** of site by CBP, factual (whois) and legal analysis
- **Collaborative development of enforcement strategy**
- **Consistent communication** of actions and status

Collaborative Enforcement: Why Synchronized Auditing?

- **Enforcement's goal is to increase compliance**
- Biggest enforcement obstacle is resource limitations
- Synchronized enforcement can harmonize DP practices
 - Information sharing and cooperation to reduce divergence in MS
 - simplify enforcement, use best practices, more efficient enforcement
 - Unified practices to permit self-regulation like BCR
 - diminish enforcement burdens
 - improve compliance sector-wide
- **Vital to refine approach and pursue joint action**

Collaborative Enforcement:

Multilateral Cooperation in the EU

- **Overall positive compliance**, with some areas of concern

Moving forward:

- **Recommendations** to correct gaps in compliance
- Non-participant data controllers should note findings
- Analyze and refine methodology for future actions
 - Continue to coordinate joint enforcement with representative organizations like CEA
 - Properly equip DPAs for effective enforcement
 - Improve survey instrument – clearer questions, more focused
 - Pursue in-depth follow-up investigations to improve compliance, not just take its temperature

Collaborative Enforcement: Cooperation with Third Countries

- Unprecedented enforcement action outside the EU: *in situ* inspections of data transferred to Colombia
- Legal basis: **model contract clause** for international data transfers
 - Where data is transferred internationally, DPA may conduct audits of the importer, using the **same techniques and tools that are available for audits of the exporter** in the DPA's jurisdiction
- Telecom company included clause in contract for Colombian tech support outsourcing
 - AEPD awareness that data might be at risk of misuse or vulnerable to security breaches; **decision to audit *in situ***

Collaborative Enforcement: Cooperation with Third Countries

- Cooperation and **facilitation by exporter** (data controller)
 - Coordinated inspections
 - Served as contact point for audits
 - Audited all involved data importers in Colombia
- 5 days of **auditing in Colombia**
 - 3 inspectors + Inspection Subdirector
 - Document access and examination
 - *in situ* checks of technical systems
 - Access to and evaluation of information stored in the system
 - *in situ* verification of security measures
- Findings: **general compliance** with technical and organizational security requirements
 - Importers saw **audit as a helpful experience** to improve practices

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



Dr. Artemi Rallo Lombarte
Director, Spanish Data Protection Agency
<http://www.aepd.es>

Workshop 3 Panelists

- Mr. Chris Turner
 - Head of Audit and Remedies, Office of the Information Commissioner, UK
- Mr. Joel Winston
 - Associate Director of Privacy and Identity Protection Branch, FTC Consumer Protection Bureau, USA
- Mr. Nicholas Cheung
 - Principal, Assurance Services Development of the Canadian Institute of Chartered Accountants
- Ms. Yim Chan
 - Global Privacy Executive, IBM and Chief Privacy Officer, IBM Canada