Regulatory Enforcement: Around the World in 90 Minutes

Global Privacy Summit
Friday, March 7, 2014

www.privacyassociation.org
Welcome and Introductions
Program Outline

I. U.S.
II. EU
III. Canada
IV. Mexico
V. Questions & Answers
U.S.

Alysa Z. Hutnik

Partner
Kelley Drye
US Consumer Privacy Regulatory Round-Up

What Happened and What’s Next

IAPP Global Privacy Summit
March 7, 2014

Alysa Z. Hutnik
Overview

• Past Year’s Enforcement Trends
  – Privacy Disclosures
  – Data Security Breaches

• What can we expect going forward?

• Practical Takeaways
Disclosure Enforcement Actions

“The failure to disclose, or adequately disclose, these facts, in light of the representation made, was, and is, a deceptive practice.” – HTC Complaint
Disclosure Enforcement Actions

HTC

5. The subsequent screen notifies you whether the app will require access to your personal information or access to certain functions or settings of your device. If you agree to the conditions, tap OK to begin downloading and installing the app.

Path

What Personal Information Do We Collect?

We actively collect certain information you voluntarily provide to us, such as when you create an account and profile, send us an email or post information or other content to our site.

We automatically collect certain information when you use our site and our services, such as your Internet Protocol (IP) address, your operating system, the browser type, the address of a referring site and your activity on our site. We treat this information as personal information if we combine it with or link it to any of the identifying information mentioned above. Otherwise, it is used in the aggregate only.

We may also automatically collect certain information through the use of "cookies" or web beacons.

www.privacyassociation.org
46. Therefore, Defendants’ representations as set forth in Paragraph 44 of this Complaint are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

49. Therefore, Defendants’ acts and practices as described in Paragraph 47 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).
Data Security Enforcement

AG Gansler Reaches Settlement with CVS Pharmacy over Improper Disposal of Patient Records, Inappropriate Sale of Expired Products

Drug store chain will pay $250,000 penalty, implement new training and safety measures; Consumers to get coupon if expired items found
What Can We Expect Going Forward?
2014 Focus

“The Commission calls on companies providing mobile services to work toward improved privacy protections. . . .”

- Final FTC Privacy Report, March 2012

www.privacyassociation.org
Do Not Track

“Consumers still await an effective and functioning do-not-track system, which is now long overdue.” – Chairwoman Ramirez
Children’s Online Privacy: COPPA

The Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business

Protecting Kids’ Privacy Online
The COPPA Rule

Updating COPPA to Protect Kids
FTC Seeks Comments on Proposed Changes

www.privacyassociation.org
Continued Discussion on U.S. Approach to Data Security and the Changes Needed

“The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to customers when there is a security breach.”

- Prepared Statement of the FTC Before the House Commerce, Manufacturing and Trade Subcommittee (Feb. 5, 2014)
Practical Takeaways
What Can We Learn?

• Due Diligence Upfront Goes Far
  – Identify data that will be collected
  – Identify business need and all additional uses of data
  – Identify and understand data sharing and purposes
  – Assess all statements for accuracy, from user guide to advertising and privacy policy, about data use and protection
  – Data security assessments of all types of PII/data associated with devices for all intended and unintended uses

• Preparation and Advocacy in Event of Crisis/Investigation
Your Presenter

Alysa Z. Hutnik
PARTNER
Advertising/Privacy & Information Security
(202) 342-8603
ahutnik@kelleydrye.com
www.adlawaccess.com
US Health Information Privacy & Security Regulatory Update

David Holtzman

Vice President, Privacy & Security Compliance Services
CynergisTek, Inc.

www.privacyassociation.org
Today’s Presenter-David Holtzman

- Vice President of Privacy & Security Compliance Services, CynergisTek, Inc.

- Subject matter expert in health information privacy policy and compliance issues involving the HIPAA Privacy, Security and Breach Notification Rules

- Over 10 years of experience in developing, implementing and evaluating health information privacy and security compliance programs

- Former senior advisor for health information technology and the HIPAA Security Rule, Office for Civil Rights
CynergisTek, Inc.

• Founded in 2003, based in Austin, Texas

• Authority in healthcare information security management, regulatory compliance, IT audit and advisory services, business continuity management, security technology selection and implementation, and secure IT infrastructure architecture and design solutions

• We offer extensive portfolio of consulting solutions in these core areas
Omnibus Rule Expanded HIPAA

- HITECH Privacy & Security
  - Business associates (BA)
  - Marketing & Fundraising
  - Sale of protected health information (PHI)
  - Right to request restrictions
  - Electronic access

- HITECH Breach Notification

- HITECH Enforcement

- GINA Privacy

- Other Modifications
  - Research
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations
Business Associates

• BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule
  – Liable for Security Rule violations

• BAs must comply with use or disclosure limitations expressed in its BA agreement and those in the Privacy Rule
  – Criminal and civil liabilities for violations

• BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities

• Subcontractors of a BA are now defined as a BA
  – BA liability flows to all subcontractors
HIPAA Breach Notification

• New standard – impermissible use/disclosure of (unsecured) PHI presumed to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:

  – Nature & extent of PHI involved
  – Who received/accessed the information
  – Potential that PHI was actually acquired or viewed
  – Extent to which risk to the data has been mitigated
Breach Notification to HHS

• 800+ reports involving a breach of PHI affecting 500 or more individuals
  – Theft and Loss are 64% of large breaches
  – Laptops and other portable storage devices account for 36% of large breaches
  – Business Associates own 36% of large breaches

• 100,000+ reports of breaches of PHI affecting less than 500 individuals
## OCR Privacy and Security Rule Compliance/Enforcement

(April 2003 – December 2013)

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Filed</td>
<td>90,000</td>
</tr>
<tr>
<td>Cases Investigated</td>
<td>32,000</td>
</tr>
<tr>
<td>Cases with Corrective Action</td>
<td>22,000</td>
</tr>
<tr>
<td>Cases Resolved through Civil Monetary Penalties &amp; Resolution Agreements</td>
<td>17</td>
</tr>
<tr>
<td>Amount of Civil Monetary Penalties &amp; Resolution Agreements</td>
<td>$ 19.6 million</td>
</tr>
</tbody>
</table>
HIPAA/HITECH Audit

• Audits of 115 entities in 2012
  – 61 Providers, 47 Health Plans, 7 Clearinghouses

• Total 979 audit findings and observations
  – 293 Privacy
  – 592 Security
  – 94 Breach Notification

• Percentage of Security Rule findings and observations double what was expected

• Smaller entities struggle with all three areas
Meaningful Use Audits

- CMS goal to audit 5% of physicians or hospitals receiving payments for Medicare EHR incentive program
  - Contractor audits for meeting Meaningful Use goals
  - Targeted EHR adoption reviews

- States perform audits on participants in the Medicaid EHR Incentive Program

- CMS or States could seek recoupment if audits finds ineligibility for MU payments
State AG’s Enforcement of HIPAA

- HITECH Act gave State Attorney General jurisdiction to bring an action in federal court on behalf of state residents to:
  - enjoin defendant from further violation; or
  - obtain damages (of $100 per violation)

- If HHS has already instituted an action against defendant, State AG may not bring action while HHS action ongoing

- Handful of cases brought by AG’s to enforce HIPAA
State Breach Notification Laws

- 46 states, DC, PR, Guam & VI have enacted laws to notify individuals of security breaches

- Safe-harbor for data that is encrypted

- Variations in state laws
  - Who must comply with the law
  - Definitions of “personal information”
  - What constitutes a breach
  - Requirements for notice
Texas Privacy & Security Laws

• Expansive definition of Covered Entity
• Employee training state & federal protections to PHI
• Patient rights to electronic medical records
• Covered entities must provide patients electronic copies of their electronic PHI within 15 business days
• Breach Notification
  – All who conduct business in state and owns or licenses computerized data that includes sensitive personal information
  – Protects residents of other states where that state does not require a person to notify the individual of a breach of system security
California HIP Laws

• Applies to all “licensed providers”
• Information protected broadly defined
• Individual rights to access and restrictions on use/disclosure
• Breach notification requirements
  – Reporting to Department of Health Services within 5 business days of “detection” of unauthorized access/use/disclosure
  – Reporting to AG when breach affects more than 500 state residents
• State is very active enforcer and has levied numerous penalties
Assuring Information Security

• Perform a Risk Analysis to identify threats & vulnerabilities to the confidentiality, integrity and availability of information

• Reduce risk to an appropriate level
  – Portable or mobile devices are prone to theft
    • Encrypt PHI stored on device
  – Malware attacks unprotected systems/devices
    • Install security patches to software and systems
    • Identify systems or devices that are past end of life and no longer supported by vendor
The European Union

Eduardo Ustaran, CIPP/E

IAPP Board of Directors
Enforcement today (I)

- Independent national regulators
- Core powers
  - Investigative powers
  - Powers of intervention
  - Power to engage in legal proceedings
- Weak sanctions?
Enforcement today (II)

DPA BUDGET AND POPULATION

DPAs annual budget (in euros)

Population
Budget

Population (in millions)

Italy, UK, France, Spain, Netherlands, Sweden, Poland, Czech Republic, Denmark, Hungary, Ireland, Finland, Slovenia, Luxembourg, Bulgaria, Romania, Latvia, Estonia, Greece, Iceland, Portugal, Slovakia, Malta

Graphics by MindYour! Privacy

www.privacyassociation.org
Enforcement today (III)

COUNTRIES DOING THE MOST INSPECTIONS

Spain 5.389
Hungary 2.929

NUMBER OF SANCTIONS PER COUNTRY

Spain 572

COUNTRIES WITH THE HIGHEST AVERAGE SANCTIONS
(total amount earned by sanctions / # of total sanctions)

135.650 €
United Kingdom

370 €
Netherlands

1.700 €
Portugal

34.000 €
Spain

8.800 €
Italy

200 €
Romania

Graphics by MindYourPrivacy
Enforcement trends

• Name and shame

Measured scrutiny

Ireland jostles to position itself as EU data protection hub

By Jamie Smyth in Dublin

Ireland is seeking to position itself as the EU’s premier data protection hub for US multinationals, while rejecting claims from some European partners that it operates a light touch regulatory regime.

Ahead of key EU talks this week in Vilnius on the scope of a pan-European data protection regulation, Dublin said on Monday that adopting a “one stop shop” regulatory approach for companies operating across borders was the right move. It also said it had begun an in-depth data protection audit of US technology company LinkedIn, which owns the world’s biggest professional-networking website, to ensure its procedures complied with Irish data protection laws.
Enforcement tomorrow

• Still national regulators

• Greater international cooperation?

• One-stop-shop?

• Massive fines?
  – % of global turnover
Canada

Shaun Brown

nNovation LLP
Canadian Regulatory Update:

OPC (PIPEDA) & CRTC (CASL)
Privacy Commissioner of Canada

• *Personal Information Protection and Electronic Documents Act (PIPEDA)* applies to collection, use & disclosure of personal information in private sector

• Enforced by Privacy Commissioner of Canada (OPC)
  – “Officer of Parliament”; ombudsman model
  – No order-making powers, no penalties
  – Federal Court of Canada can award damages (have been minimal)

• Growing calls for new powers – not likely anytime soon

• Can still make life difficult

www.privacyassociation.org
Recent/upcoming activity

• Increasing focus on new technologies
  – Social media; Google, OBA

• The Internet Sweep
  – “Naming and shaming” in action

• Targeted ads based on sleep apnea violate PIPEDA

• Investigating OBA by Bell Canada

• Increasing focus on accountability
What is CASL?

- Rules for sending Commercial Electronic Messages (CEMs)
- Rules for installation of computer programs
- Prohibition against unauthorized alteration of transmission data
Canadian Radio-television Telecommunications Commission (CRTC)

- Canadian Radio-television Telecommunications Commission (CRTC)
- Role as enforcement agency began with Unsolicited Telecommunications Rules (UTR) in 2008
- Broad investigatory powers
- Ability to impose administrative monetary penalties (AMPs); up to $10 million/violation
- Demonstrated willingness to impose AMPs under UTR
Recap

• Privacy Commissioner: weak powers unlikely to change soon, but becoming more aggressive with “name and shame”

• CRTC:
  – very strong enforcement powers under CASL, which comes into force on July 1, 2014
  – has shown willingness to use powers

• Imbalance between protection of email (and other electronic) addresses and everything else
Contact

Shaun Brown
nNovation LLP
sbrown@nnovation.com
Twitter: @emarketinglaw
613.656.1297

nNovation LLP

www.privacyassociation.org
Mexico

María-Elena Pérez-Jaén Zermeño
Commissioner (DPA Mexico)

Federal Institute for Access to Information
and
Data Protection
(IFAI)
Mexican DP Regulation

Data Protection is a fundamental right (articles 6 and 16 of the Mexican Constitution)

<table>
<thead>
<tr>
<th></th>
<th>Federal</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public sector</strong></td>
<td>Mexican FOIA (IFAI authority)</td>
<td>Several local laws (local authorities)</td>
</tr>
<tr>
<td><strong>Private sector</strong></td>
<td>Federal Law on the Protection of Personal Data Held by Private Parties (DPL) (IFAI sole authority)</td>
<td></td>
</tr>
</tbody>
</table>

www.privacyassociation.org
Mexican Approach

A hybrid approach that includes benefits of general and sectorial models:

<table>
<thead>
<tr>
<th>From the general model...</th>
<th>From the sectorial model...</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP as fundamental right</td>
<td>Implicit consent for 90% of data processing</td>
</tr>
<tr>
<td>Comprehensive Laws</td>
<td>Accountability principle</td>
</tr>
<tr>
<td>Principles, duties and rights</td>
<td>Coexists with self-regulation</td>
</tr>
<tr>
<td>Data protection authority</td>
<td>Facilitation for International Data Transfer</td>
</tr>
<tr>
<td>Violations and penalties</td>
<td>No registry of data controllers is needed</td>
</tr>
</tbody>
</table>
Scope
Mexican DPL

- It applies throughout the national territory. IFAI is the only authority that protects this right in Mexico.

- Regulates the legitimate, controlled and informed processing of personal data held by private parties, except:
  - Credit reporting companies (other legislation)
  - Individuals → personal use, without purposes of disclosure or commercial use, i.e. personal list of contacts.

- Ensures privacy and information self-determination.

DPL (Data Protection Law)
DPL Content

**Principles and obligations**
1. Legality
2. Fidelity
3. Purpose
4. Proportionality
5. Quality
6. Notice
7. Accountability
8. Consent

**Rights**
1. Security
2. Confidentiality

**Proceedings**
1. Rights Protection
2. Verification
3. Sanctioning

ARCO
1. Access
2. Rectification
3. Cancellation
4. Objection

DPL (Data Protection Law)

www.privacyassociation.org
IFAI's faculties

Informative  Regulations  Verification

Preventive  Resolutions  National and international cooperation
Proceedings before IFAI

• Rights Protection

• Verification

• Penalties Imposition
Penalties (enforcement)

- Warning
- Fines from \( \sim \$500 \text{ USD} \) – \$1,650,000 \text{ USD} \\
- Repeated occurrences, additional fine
- Violations in processing sensitive data, sanctions may be doubled
Sanctions imposed in 2012-2013

IFAI imposed 17 economic sanctions (fines) totaling $4,445,868.00 USD.

The most sanctioned firms were a banking institution and a private education school. The most frequent offending behaviors were:

- Lack of information regarding Privacy Notice,
- Lack of attention and response to ARCO rights requests,
- Conducting undue transfers of personal data,
- Disclosure of personal data without the consent of the owner, and
- Use of personal data without the consent of the owner.
Sanctions by sectors (2012-2013)

- Health services and social assistance: 17%
- School services: 18%
- Financial services and insurance: 41%
- Retail: 6%
- Leisure, Culture, Sport and other services: 6%
- Electronic information processing: 6%
- Mass media information: 6%
Resolutions are available in Spanish at:

http://consultas.ifai.org.mx/SesionesspDP
Conciliation

• Mexican DPL stipulates conciliation as an alternative to dispute resolution, as part of the rights protection procedure.

• In 97 cases, 70 accepted conciliation, with 68 settlements.

• Financial and Health services were the sectors with the highest number of settlements.
IFAI’s Policy

• Promote prevention

• Develop tools to facilitate data controllers to comply with their obligations

• Promote self-regulation
Guides and Tools

- Privacy Notice Guidelines and Self-Regulation Guidelines
- Recommendations on Data Protection Security
- ABC Privacy Notice Guide
- Privacy Notice model for video surveillance
- Privacy notice in video
- Privacy Notices Generator (*GAP* in Spanish)
Privacy Notices Generator (GAP)

We assist you to create Privacy Notices

Free of charge

Access your Username and password...

Available in the following website:
http://generador-avisos-privacidad.ifai.org.mx/users/login

www.privacyassociation.org
Privacy Notices Generator: some figures

<table>
<thead>
<tr>
<th>Information</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of times users have logged in</td>
<td>68,026</td>
</tr>
<tr>
<td>Total registered users</td>
<td>15,313</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company size</th>
<th>Total Privacy Notices created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro</td>
<td>9,281</td>
</tr>
<tr>
<td>Small</td>
<td>4,586</td>
</tr>
<tr>
<td>Medium</td>
<td>684</td>
</tr>
<tr>
<td>Large</td>
<td>614</td>
</tr>
<tr>
<td>Not concluded</td>
<td>4,027</td>
</tr>
<tr>
<td>Total</td>
<td>19,192</td>
</tr>
</tbody>
</table>

www.privacyassociation.org
What’s next?

• Data Controllers Handbook for Compliance with Protection of Personal Data Obligations

• Comparative Chart of International Standards and Safety Measures Established by the DPL

• Guide to Guarantee a Secure Destruction of Personal Data

• Guide for Cloud Services Contracting

• Digital Citizenship Website

www.privacyassociation.org
Thank You

María Elena Pérez-Jaén Zermeño
IFAI Commissioner
mariaelena.perezjaen@ifai.org.mx

www.ifai.org.mx
http://www.portaltransparencia.gob.mx/pot/
www.infomex.org.mx

Phone: +52 (55) 5004 2400

www.privacyassociation.org
Questions
&
Answers