Cross-Border Data Privacy and Security Best Practices

Valérie Demont, Sharon R. Klein, Anand Mehta, Supratim Chakraborty | November 28, 2012

Pepper Hamilton LLP
Attorneys at Law

We will be starting momentarily…

Pepper Hamilton LLP
Attorneys at Law

Listen to the audio portion of today's webinar by dialing:

North America Toll-Free: +1.866.322.1348

International Toll: +1.706.679.5933

India Toll-Free: 180030705400

Mumbai Local: 2230985770

Audio Conference ID #: 73463532

Pepper Hamilton LLP
Attorneys at Law

Technical Support Numbers

If you experience technical difficulties, hit *0 on your telephone keypad and an operator will assist you.

Or you can dial:

For Web Support:
North America:
+1.877.812.4520 or
International
+1.706.645.8758

For Audio Support:
North America:
+1.800.374.2440 or
International:
+1.706.645.6500

Pepper Hamilton LLP
Attorneys at Law

Cross-Border Data Privacy and Security Best Practices

Click this icon to view the slide in full screen mode.

Hit the 'Escape' key to return to the normal view.

Valérie Demont, Sharon R. Klein, Anand Mehta, Supratim Chakraborty | November 28, 2012

Pepper Hamilton LLP
Attorneys at Law

Cross-Border Data Privacy and Security Best Practices

Valérie Demont, Sharon R. Klein, Anand Mehta, Supratim Chakraborty | November 28, 2012

Click the printer icon to download/print the slides.

Pepper Hamilton LLP
Attorneys at Law

Cross-Border Data Privacy and Security Best Practices

Feel free to submit text questions throughout the webinar

Valérie Demont, Sharon R. Klein, Anand Mehta, Supratim Chakraborty | November 28, 2012

Pepper Hamilton LLP
Attorneys at Law

Freeh Association.

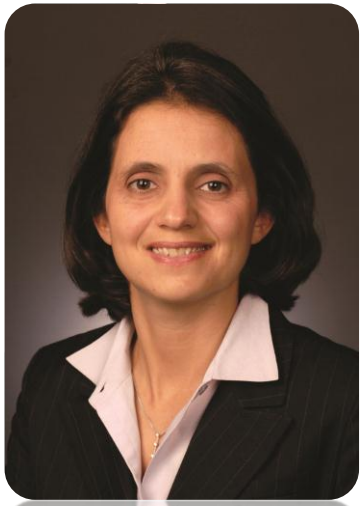
The Freeh Group is now part of Pepper Hamilton LLP.

We are pleased to announce that
The Hon. Louis J. Freeh
and the lawyers of Freeh Sporkin & Sullivan, LLP
have joined Pepper Hamilton LLP
and Pepper Hamilton LLP has acquired
Freeh Group International Solutions, LLC

August 28, 2012

Pepper Hamilton LLP
Attorneys at Law

Moderator: Valérie Demont



+1.212.808.2745
demontv@pepperlaw.com

- Partner in the Corporate and Securities Practice Group of Pepper Hamilton LLP, resident in the New York office
- Practice leader for the U.S.-India Practice Group
- Focuses her practice primarily on U.S. and cross-border mergers and acquisitions, capital markets, corporate finance and securities matters
- Has been involved in numerous transactions for corporations and private equity funds in the U.S., Europe, Canada and Asia.

Pepper Hamilton LLP
Attorneys at Law

Speaker: Sharon R. Klein

+1.949.567.3506
kleins@pepperlaw.com

- Partner in the Corporate and Securities Practice Group of Pepper Hamilton LLP, and the partner in charge of the firm's Orange County office
- Handles a variety of corporate and intellectual property matters, in particular, helping information technology and telemedicine clients grow and succeed
- An active member of HIMSS (Healthcare Information and Management Systems Society) and writes and speaks frequently on issues such as licensing, privacy security, confidentiality, telemedicine, outcomes/disease management and managed care. She is a board member of the *Privacy and Security Law Journal*.

Pepper Hamilton LLP
Attorneys at Law

Speaker: Anand Mehta

+91 22 6636 5000
anand.mehta@khaitanco.com

- Partner and a qualified advocate and company secretary with Khaitan & Co.
- Specializes in corporate acquisitions and mergers, India entry strategies, corporate & commercial laws, anti trust, contract and securities laws
- Assisted several clients including some Fortune 500 companies to establish and expand their India operations including forming joint ventures and other strategic alliances
- Has actively participated in commercial negotiations for several multinational clients. His forte, apart from mergers and acquisitions includes employment, real estate, variety of IP matters, including those involving trademark, copyright, rights of privacy and trade secrets.

Pepper Hamilton LLP
Attorneys at Law

Speaker: Supratim Chakraborty

+91 22 6636 5000
supratim.chakraborty
@khaitanco.com

- A corporate lawyer and member of the corporate and commercial law team with Khaitan & Co.
- Focuses his expertise on corporate and commercial transactions such as mergers, acquisitions, joint ventures and general corporate law advisory
- Advised eminent clients in relation to information technology laws in India including data protection and data privacy related issues. Before joining Khaitan & Co., Supratim was as an associate in an eminent law firm in Mumbai.

Pepper Hamilton LLP
Attorneys at Law

KHAITAN &CO
Advocates since 1911

U.S. India Webinar
Cross-Border Data Privacy and Security Best Practices

Anand Mehta
Supratim Chakraborty

| Mumbai | 28 November 2012

News Flash

- June 2012 - Website of a multinational internet corporation was reportedly hacked and more than 453,000 login credentials were stolen
- February 2012 - Website of an Indian subsidiary of a US software giant was reportedly hacked and login IDs and passwords of users were stolen
- May 2011 - Website of a major news channel was reportedly hacked and stolen personal details were published on a file sharing website
- April – June 2011 - Network of a major video game company was reportedly intruded and details from approximately 77 million accounts were stolen

…and the list goes on…

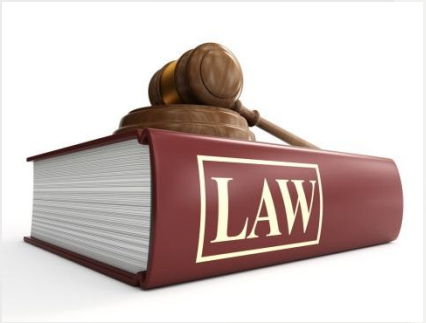
Celebrating a Century

Changed Global Scenario

- Technology has made it possible to collect, copy, process and transfer data at the press of a button
- Risk and actual instances of misuse of data has increased, resulting in heightened attention from all global organizations for protection
- Data Privacy and protection has to be dealt by most companies from multiple jurisdiction standpoint, applying territorial laws

Celebrating a Century

The Law



Indian Legal Framework and Development

- Article 21 of the Constitution of India protects life and personal liberty which includes the Right to Privacy
- Information Technology Act ("**IT Act**") has made a beginning
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("**Privacy Rules**") framed under Section 43A of the IT Act provides framework for protection of data
- Press Note dated 24 August 2011 clarifying some of the provisions of the Privacy Rules
- Nine National Privacy Principles proposed by a panel working on new legal framework for India

Celebrating a Century

IT Act

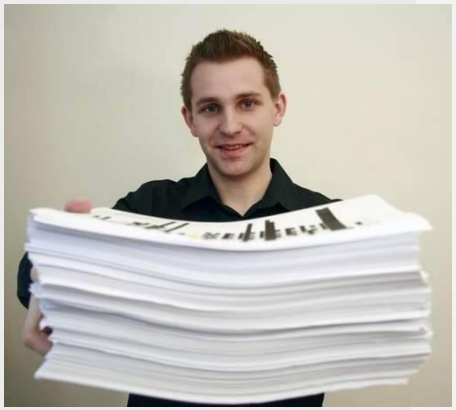
Relevant Provisions

- Section 43 A – Civil Remedy:
  - Relates to any body corporate possessing, dealing or handling any **sensitive personal data or information** in a computer resource
  - Where such body corporate is negligent in implementing and maintaining **reasonable security practices and procedures**
  - Causes wrongful loss or wrongful gain to any person
  - Liable to pay **damages by way of compensation** to the affected person

- Section 72 A – Criminal Remedy:
  - Relates to any person providing **services under lawful contract** wherein personal information is accessed
  - There is intent or knowledge of wrongful loss or wrongful gain being caused through disclosure of such personal information
  - Disclosure is made **without the consent of the person** concerned **or in breach of a lawful contract**
  - Liable to be **punished with imprisonment** up to **3 years**, or with **fine** up to **INR 0.5 Million**, or with **both**

Celebrating a Century

Privacy Rules

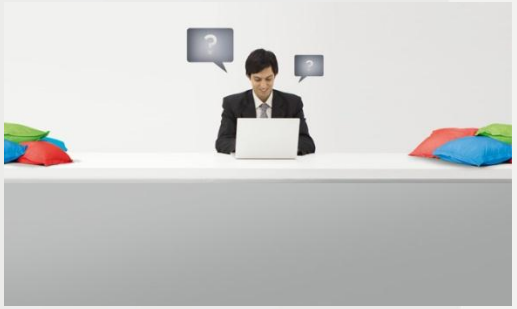


Key Definition

- Sensitive Personal Data or Information ("**SPDI**") — personal information relating to:
  - password
  - financial information such as bank account or credit card or debit card or other payment instrument details
  - physical, physiological and mental health condition
  - sexual orientation
  - medical records and history
  - biometric information
  - any detail relating to the above as provided to body corporate for providing service
  - any information received under above by body corporate for processing, stored or processed under lawful contract or otherwise

Celebrating a Century

Privacy Rules – What To Do

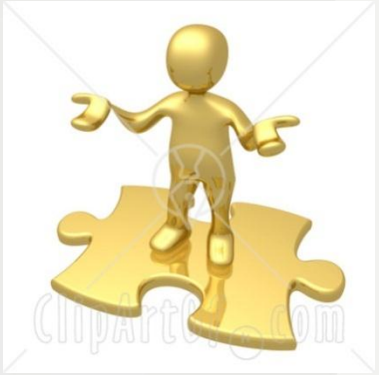


Implementation of Reasonable Security Practices and Procedures

- As per agreement; or
- International Standards IS / ISO / IEC 27001 relating to 'Information Technology - Security Techniques - Information Security Management System - Requirements' ("**Standards**"); or
- Any code of best practices for data protection prepared by an industry association and approved and notified by the Central Government ("**Code**")
- Bodies corporate who have implemented such Standards or Codes require certification from Central Government approved auditors:
  - at least once a year; or
  - in case of significant upgradation of process and computer resource

Celebrating a Century

Privacy Rules – What To Do



Collection of Information

- SPDI to be collected only if necessary and required for lawful purpose
- Information to be used only for the purpose for which it is collected
- Information provider should know that:
  - information is being collected
  - the purpose of collection
  - the intended recipients
  - name and address of agency collecting and retaining the information
- SPDI not to be retained for longer period than required
- Information provider should be allowed to review / amend the information provided and the option to withdraw consent at any time
- In case of withdrawal of consent, the body corporate may not provide the goods or services for which the concerned information was sought

Celebrating a Century

Privacy Rules – What To Do

Disclosure of SPDI to Third Party

- As per agreement; or
- Obtain prior permission from the provider

Consent for Purpose

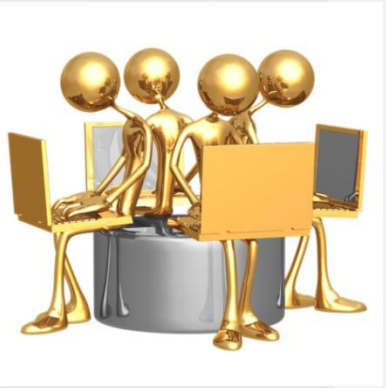
- Obtain prior consent from provider of SPDI regarding purpose of usage

Transfer

- Permitted to transfer information to any person or body corporate located anywhere, who ensure the same / equal level of data protection; and
- Only if the transfer is necessary for the performance of lawful contract between the body corporate and provider of information or where such provider of information has consented to the transfer

Celebrating a Century

Privacy Rules – What To Do



Privacy Policy

- Provide a Privacy Policy to information providers and publish the same on website
- Privacy Policy shall contain:
  - type of information collected
  - purpose for collection of information
  - security practices and procedures followed
  - disclosure policy

Grievance Officer

- Designate a Grievance Officer to address grievances of information providers
- Name and contact details of Grievance Officer to be published on website
- Grievance Officer to redress the grievances within one month

Celebrating a Century

Best Practices

Follow the 5 P's

Provider's agreement

Privacy policy

Procedures for information security

Pro-active monitoring

Purge the unnecessary

Celebrating a Century

Rise of Cybercrime

- Data theft is now a multi-billion dollar international industry
  - Increased use of technology to college, use, share and retain personal information (e.g., 8 out of 10 households use online banking)
  - Cloud computing means data aggregation and hackers have more to gain from one single attack
  - Stolen data readily traded on black market
- Identity theft and impact on victims
  - Someone uses personally identifying information (e.g., name, SSN, credit card number) without permission to commit fraud or other crimes
  - 9 million Americans have their identities stolen each year
  - Victims spend hundreds of dollars to repair damage to name and credit
  - Impact could be loss of job opportunities, denial of loans, and potential prosecution for crimes not committed
- Today:
  - Theft of information became leading type of fraudulent activity globally
  - Approximately 600 breaches in the U.S. alone put more than 12 million records in jeopardy

OVERVIEW

- What Data is Private?
- Importance of Data Privacy
- Evolution of Privacy Laws in the U.S.
- Role of The Federal Trade Commission (FTC)
- Key Privacy Legislation Impacting U.S. Companies
- 2012 FTC Report – Blue Print for Federal Privacy Bill
- Cautionary Tales
- Takeaways
- Questions?

What Data is Private?

- Personally Identifiable Information (PII) is any information relating to an identified or identifiable natural person.
- PII includes any piece of information which can be used to uniquely identify or trace an individual's identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual.
- Data elements vary
- Combination/factor analysis

What is PII? – Data Elements

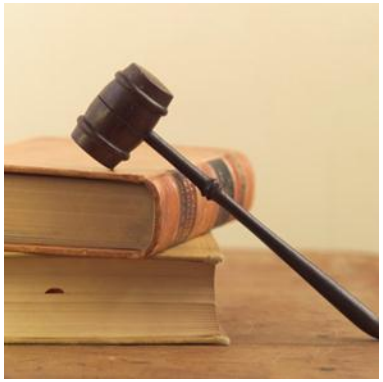
- **Typical data elements include:**
- ***Full name***
- ***National identification number (Social Security Number (SSN) in U.S.)***
- ***Date of birth***
- Driver's license number
- Passport number
- Biometric records (e.g., face, finger prints, handwriting samples, voice prints, other biometric identifiers)
- Credit card and financial account numbers
- Telephone number
- Street address
- Zip code
- Email address
- Digital identifiers
- "Sensitive" information (e.g., demographic information, gender, citizenship, racial or ethnic origin, medical or health information (including accommodations), religious beliefs or affiliation, political opinions

Importance of Data Privacy

- A breach of data privacy can cause:
- Harm to individual: financial, social, other
- Financial cost to organizations
  - The average cost per breached record is $222
  - The average organizational cost of compliance is $3.5M
  - Reputational injury/brand damage

Importance of Data Privacy (cont'd)

- Companies must respect all applicable laws regarding data
- Risks of Non-Compliance:
  - Costs of notice and remediation
  - Regulatory action
  - Fines and penalties
  - Potential lawsuits
  - Loss of business, company resources & employee time
  - Damage to brand and reputation
  - Reduction in ability to do business



Evolution of Privacy Laws

- Right to Privacy Not Specifically Enumerated in Constitution
- Dates back to Colonial America/Revolutionary War
  - Focus on freedom from government intrusion
    - Bill of Rights – Third Amendment (no quartering of soldiers in private homes without owner's consent), Fourth Amendment (no search & seizure without warrant) and Fifth Amendment (no deprivation of life, liberty or property without due process of law)
- 1890: *The Right to Privacy* (Harvard Law Review article by Attorney Samuel Warren and future Supreme Court Justice Louis Brandeis)
  - **"Right to be let alone"**
  - Rapid growth of newspapers that frequently reported on scandals and gossip
- Fast forward to 1990s
  - Rise of the Internet and email
  - Easier to collect and aggregate personal information
- Key legislation
  - Medical: Protection of medical records
    - *Heath Insurance Portability and Accountability Act of 1996 (*HIPAA)
  - Financial: Protection of personal information accessed by financial institutions
    - *The Gramm-Leach-Bliley Act of 1999 (GLB)*

Evolution of Privacy Laws (cont'd)

- September 11, 2001
  - Terrorist attacks awaken the nation
  - Political push to expand powers of law enforcement
- Key Legislation
  - Terrorism:
    - *The USA Patriot Act of 2001*
    - Amendments to Patriot Act to allow law enforcement agencies greater access to personal information to track financing of international terrorism
  - Cyber and Physical Security:
    - *Homeland Security Act of 2002*
    - Created Department of Homeland Security and a Privacy Office
  - Corporate Controls:
    - *Sarbanes-Oxley Act of 2002*
    - Required public companies to implement processes and controls to ensure accuracy of financial reporting
    - Criminal liability imposed on individual corporate executives
  - Email:
    - *The Can-SPAM Act Of 2003:*
    - Restricts sending commercial messages to deceive or mislead recipients
    - Spammers must allow Internet users to opt out

Evolution of Privacy Laws (cont'd)

- Currently there are 46 different state data breach notification laws (requiring written notification to impacted individuals when PII has been obtained by unauthorized party)
- State legislation on protection of personal information broader than federal (California, Massachusetts); zip code and email addresses may be considered personal information in addition to social security numbers
- No controlling federal privacy legislation
- Follow the guidelines of the Federal Trade Commission (FTC) and the most restrictive state data breach laws

Role of the Federal Trade Commission (FTC)

- Broad authority under Section 5 of the FTC Act
  - Prohibits business from engaging in “unfair or deceptive acts or practices in or affecting commerce.”
  - FTC has brought over 22 actions under Section 5 in past 10 years.
- Investigates “unfair” trade practices such as:
  - Failure of a business to comply with its own privacy policies
  - Failure of a business to implement industry-standard data security measures

FTC Report Protecting Consumer Privacy in Era of Rapid Change (March 2012)

- Congress has been unable to pass a Federal Privacy Bill (what a surprise).
- FTC Report is a blue print for potential post-election Federal Legislation, currently self-regulatory best practices with the following three main themes:

(1) "Privacy by Design":
- Promote privacy throughout the organization and at every stage of development of products and services
- Delete consumer data no longer needed and allow consumers to do the same
- Provide reasonable security for data
- Limit collection of data (consistent with context of particular transaction)
- Implement reasonable data retention and disposal policies
- Maintain reasonable accuracy of data

(2) Simplify Consumer Choice:
- Provide consumer choice for any communications not related to original transaction
- "Do Not Track" mechanisms allow consumer to control collection and use of their online data
- Certain choices require consumer to "opt in"

(3) Improve Transparency to Consumers:
- Clearer and shorter privacy notices
- Provide access to consumer data
- Educate consumers about company's data privacy practices

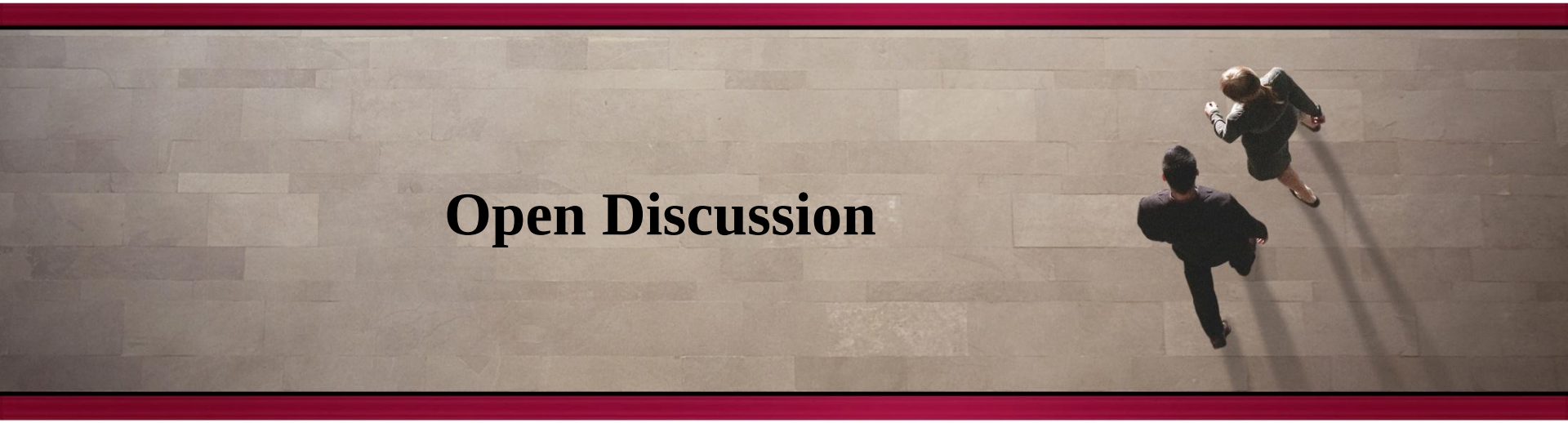
Cautionary Tales

- FTC Enforcement
  - FTC can launch an investigation on its own initiative or in response to a complaint
  - 22 actions and counting over the last 10 years
  - FTC settlements from $4 - $20M civil penalty and audits for next 20 years
- Government Lawsuits
  - Civil and criminal actions
  - Civil fines $50,000 per violation up to $1.5M annually
  - 10 Years in prison
- Private Class Actions
  - Data breach classes certified
  - Damages exceed $1B

Takeaways

- Companies should train employees and require its suppliers to:
  1. Always treat Personally Identifiable Information (PII) and sensitive data as if it were your own.
  2. Always think of data privacy issues from the customer's or consumer's perspective.
  3. Protect PII in use, storage and transit.
  4. Delete unnecessary PII and properly dispose of devices.
  5. De-identify PII.

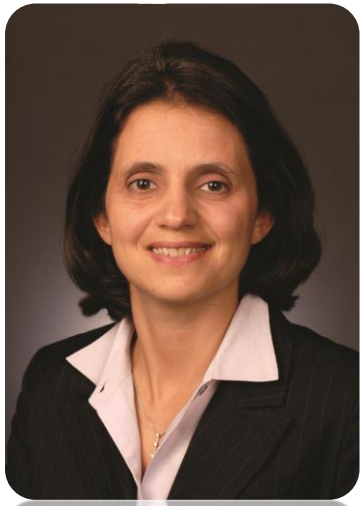
Open Discussion



Questions and Answers

Pepper Hamilton LLP
Attorneys at Law

Thank You!



+1.212.808.2745
demontv@pepperlaw.com

+1.949.567.3506
kleins@pepperlaw.com

+91 22 6636 5000
anand.mehta@
khaitanco.com

+91 22 6636 5000
supratim.chakraborty@
khaitanco.com

Pepper Hamilton LLP
Attorneys at Law

For more information, visit www.pepperlaw.com and www.khaitanco.com

Pepper Hamilton LLP
Attorneys at Law