Around the Financial Services World in 90 Minutes

By
Lynn A. Goldstein
L. Richard Fischer
Russell W. Schrader
Melanie Shillito

March 8, 2013
U.S. Privacy and Data Security
In February 2012, the White House released a blueprint for a new U.S. consumer privacy protection framework—“Consumer Data Privacy in a Networked World”

- The framework would guide the collection and use of personal information about consumers
- The framework includes a consumer privacy “Bill of Rights” to provide baseline protections for consumers and greater certainty for companies
- The framework includes a process to produce “codes of conduct” that would implement the Bill of Rights
- The framework strengthens the Federal Trade Commission’s (“FTC”) enforcement authority on consumer privacy
- The framework also encourages international interoperability
The framework is intended to apply to all commercial uses of “personal data,” which is defined as “any data, including aggregations of data, which is linkable to a specific individual,” as well as data that is linked to a specific computer or other device.

The Bill of Rights is based on the Fair Information Practice Principles and includes seven principles that companies would be required to follow when collecting and using personal information about consumers:

- **Individual control.** Consumers have a right to exercise control over the personal data companies collect from them and how a company uses that information.
- **Transparency.** Consumers have a right to easily understandable and accessible information about a company’s privacy and security practices.
- **Respect for context.** Consumers have a right to expect that a company will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.
• **Security.** Consumers have a right to expect the secure and responsible handling of personal data

• **Access and accuracy.** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate

• **Focused collection.** Consumers have a right to reasonable limits on the personal data that a company collects and retains

• **Accountability.** Consumers have a right to have personal data handled by a company with appropriate measures in place to assure the company adheres to the Bill of Rights
Although the Administration has not recommended modifying existing federal statutes relating to the collection of information, it has suggested the following principles:

- **Individual control.** Choice about collection
- **Transparency.** Disclose if personal data is collected from third parties and the nature of that information
- **Focused collection.** Collect only data needed to accomplish specific purpose
• The White Paper includes:
  • A process to develop voluntary, but enforceable, codes of conduct that would implement the Bill of Rights
  • This multi-stakeholder process, which is being led by the Department of Commerce’s National Telecommunications and Information Administration ("NTIA"), would identify markets and industry sectors that involve significant consumer data privacy issues and could be ripe for an enforceable code of conduct
  • The NTIA announced that it has commenced a multi-stakeholder process to develop privacy codes of conduct
• The White Paper sets forth:
  • The legal framework under which the FTC is the federal government’s leading consumer privacy enforcement authority
  • The White Paper also would position the FTC as the primary enforcer of the Bill of Rights and of a company’s commitment to adopt the codes of conduct
  • The FTC would be authorized to grant “safe harbor” status to a company that complies with a code of conduct reviewed and approved by the FTC
  • The privacy framework recognizes the potential burden of compliance with divergent international privacy laws. Accordingly, the White House encourages interoperability in privacy laws worldwide
The White House paper also encourages:

- Mutual recognition of different commercial data privacy frameworks, including joint enforcement efforts that are conducted according to publicly announced policies
- International stakeholders to identify globally accepted accountability mechanisms that can be used to develop international codes of conduct designed to simplify the compliance burdens faced by multinational organizations
NTIA MULTI-STAKEHOLDER PROCESS

• Led by the NTIA, the multi-stakeholder process is intended to develop voluntary, but enforceable, codes of conduct that implement the proposed privacy Bill of Rights
• The goal is to identify markets and industry sectors that involve significant consumer data privacy issues and may be appropriate for an enforceable code of conduct
• In March 2012, the NTIA published a request for comment on consumer data privacy issues
  • Specifically, the NTIA requested comment on issues that may warrant legally enforceable codes of conduct and procedures for developing such codes of conduct
  • Among other things, the NTIA indicated that it is considering developing a code regarding transparency in privacy notices for “mobile apps”
The NTIA received more than 80 comment letters

- Many commenters agreed that mobile apps and the mobile space are a priority
- Some commenters stated that this process should balance the goal of openness with the goal of obtaining a workable solution
- Commenters indicated that codes of conduct would be most workable when the industry takes the lead in drafting them
- Other commenters expressed concern that existing institutional and public stakeholders may not be well prepared, vested or focused to understand important nuances in developing codes of conduct

The NTIA has hosted a series of meetings to create such codes of conduct
On May 17, 2012, Representatives Luetkemeyer (R-MO), Garrett (R-NJ) and Westmoreland (R-GA) introduced a bill to limit the customer privacy notifications required of financial services providers under the GLBA

- The legislation is entitled the “Eliminate Privacy Notice Confusion Act” (H.R. 5817)
- H.R. 5817 would have granted exemptions from the annual GLBA privacy notice requirement to a financial institution that maintains the same privacy policy from year to year
- The annual notice requirement would be eliminated where there is no change to the privacy policy, which would remove an expense for banks and help make privacy notices more meaningful to consumers

On December 12, 2012, H.R. 5817 passed the House; however, the Senate did not consider the bill prior to adjournment
TCPA LITIGATION

• On January 2, 2013, a class action was brought against a bank in California district court, alleging that the bank’s use of an automatic telephone dialing system to call the cell phones of consumers without their permission, and despite requests to cease doing so, violated the Telephone Consumer Protection Act (“TCPA”)
  • The named plaintiff was not a customer of the bank, and never provided his cell phone number to the bank
  • In the class action complaint, plaintiffs argued that the bank’s negligent and willful calls caused the class “irreparable harm” because they were charged for the incoming calls
  • The plaintiffs seek $5 million in damages—$500 in statutory damages for each negligent call in violation of the TCPA and $1,500 for each willful violation
  • On February 15, 2012, the Federal Communications Commission revised its TCPA rules to require prior express written consent to deliver an autodialed or prerecorded telemarketing call to a cell phone
The current Congressional cybersecurity debate demonstrates two distinct approaches:

- Democrats support the creation of a new regulatory structure to be led by the Department of Homeland Security (“DHS”)
- Republicans instead want to address cybersecurity through information sharing, strengthening existing cyber-related criminal provisions and other non-regulatory mechanisms
- To date, the Senate’s efforts to pass a comprehensive cybersecurity bill have not been successful
- The House, however, passed several narrow cybersecurity bills in the last Congress
FEDERAL CYBERSECURITY LEGISLATION

• Senate consideration and outcome
  • As Senate Majority Leader Reid (D-NV) promised in October 2012, the “lame-duck” Senate reconsidered its earlier vote on Senator Lieberman’s (I-CT) cybersecurity bill—the Cybersecurity Act of 2012 (S. 3414)
  • In August, the Senate failed to invoke cloture on S. 3414, with 52 votes in favor of cloture
  • On November 14, 2012, the Senate once again failed to invoke cloture on S. 3414
    • With 60 votes needed to invoke cloture, only 51 Senators voted in favor
Is cybersecurity dead?

Following the Senate’s vote, Majority Leader Reid stated on the Senate floor that cybersecurity was “dead” for 2012.

The White House, however, is still attempting to identify common ground.

What happens now? Is an executive order in our future?

Rumors continue to circulate about the possibility of a cybersecurity Executive Order that the Administration is reportedly drafting.

This draft Executive Order reportedly would direct various federal agencies to create a new cybersecurity council at DHS, including representatives from those agencies, including the Director of National Intelligence (similar to S. 3414).

The draft Executive Order also would direct certain federal agencies to develop voluntary cybersecurity guidelines for owners of critical infrastructure (similar to S. 3414).

But, an Executive Order cannot provide a federal agency with authority that it does not have under existing law.
FEDERAL DATA SECURITY AND BREACH NOTICE LEGISLATION

• It appears unlikely that a general data security bill will pass in the near future, despite substantial time spent on such legislation by both the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce

• Ultimately, the passage of general data security legislation may depend on:
  • The occurrence of one or more additional high-profile data breaches; and/or
  • The fate of a cybersecurity bill and the ability to add a general data security provision or breach notification provision to such a cybersecurity bill
In general, the data security bills introduced to date would imposing nationwide standards for the protection of personal information, as well as for security breach notification.

For example, S. 1207, introduced by Senators Pryor (D-AR) and Rockefeller (D-WV), would have directed the FTC to establish rules requiring companies that own or possess personal information to implement reasonable data security procedures, and establish nationwide security breach notification requirements.

For financial institutions, the critical issues relating to these data security bills are:

- The extent to which financial institutions subject to the GLBA would be exempted from the legislation; and
- If exempted, whether financial institutions would nevertheless share in any preemption provided by the bills.
On June 26, 2012, the FTC filed suit, in an Arizona federal court, against hospitality company Wyndham Worldwide Corporation (“Wyndham”) for alleged data security failings that led to three security breaches at Wyndham hotels.

This case is noteworthy because it is the first data security case that the FTC has actually been forced to litigate.

The FTC alleged that Wyndham violated Section 5 of FTC Act because:

- Wyndham’s privacy policy misrepresented the security measures that Wyndham took to protect consumer information.
- Wyndham’s failure to protect consumer information caused substantial consumer injury.

The FTC also alleged that Wyndham’s security failings included:

- The failure to implement security measures, such as complex user IDs and passwords, firewalls and network segmentation between the company’s corporate network and its hotels.
- Allowing improper software configurations that resulted in storage of payment card information in clear readable text.
FTC V. WYNDHAM WORLDWIDE CORPORATION

• The FTC alleged that these security failings resulted in a breach that involved payment card information relating to more than 500,000 accounts and the export of hundreds of thousands of payment card numbers to a domain registered in Russia

• After suffering the first incident, the FTC alleged that Wyndham failed to:
  • Remedy known security vulnerabilities
  • Employ reasonable measures to detect unauthorized access
  • Follow proper incident response procedures

• The FTC alleged that, as a result, Wyndham experienced two additional breaches, each involving information relating to more than 50,000 payment card accounts
On August 27, 2012, Wyndham filed a motion to dismiss

- Wyndham argued that the FTC lacks the authority under Section 5 of the FTC Act to establish and enforce information security requirements for a private company
- Wyndham also argued that the FTC has not published any rules to provide businesses with notice of the types of information security protections a company must employ
- Instead, Wyndham argued that “the FTC is enforcing its vision of data-security policy through this selective, *ex post* enforcement action, which seeks to hold [Wyndham] liable without any fair notice as to what the law required”

If the court agrees with Wyndham’s arguments, it would be a significant blow to the FTC

- The FTC historically has used Section 5 as a mechanism to bring data security enforcement actions against companies that are not otherwise subject to the FTC’s Safeguards Rule issued under the GLBA
On July 3, 2012, the U.S. Court of Appeals for the First Circuit issued an opinion addressing when a bank may be liable to a commercial customer for fraudulent withdrawals.

The First Circuit found that the bank’s information security requirements were not “commercially reasonable” security controls under Article 4A of the Uniform Commercial Code (“UCC”).

In the case at issue, a community bank authorized six apparently fraudulent withdrawals totaling more than $500,000 from an account held by a construction company.
PATCO CONSTRUCTION CO. V. PEOPLE’S UNITED BANK

- The fraudsters had supplied the correct answers to the construction company’s customized answers to the bank’s security questions for access to Internet banking
- The bank’s security systems flagged each of the withdrawals as unusually “high-risk” because they were inconsistent with the timing, value and geographic location of the construction company’s regular payment orders
- However, the bank did not notify the construction company of the attempted withdrawals
- The bank was able to block or recover more than $200,000
- Nevertheless, the construction company was left with a loss of more than $345,000
The construction company sued, alleging that the bank should bear the loss associated with the fraudulent withdrawals because the bank’s security system was not commercially reasonable under Article 4A of the UCC, as codified under Maine law.

The district court granted summary judgment to the bank, holding that the bank’s security system was in fact commercially reasonable.

The First Circuit reversed, concluding that the bank’s “collective failures taken as a whole, rather than any single failure,” rendered the bank’s security system commercially unreasonable.
Among other things, the First Circuit found that the following “failures” contributed to the commercial unreasonableness of the bank’s security system:

• The bank lowered its transaction amount threshold for asking its customers challenge questions to a “one-size-fits-all” $1 transaction amount rule, even for commercial customers that had frequent high-dollar transfers
  • This low threshold guaranteed that challenge questions would be triggered on most transactions
  • As a result, customer answers were more likely to be exposed to keyloggers that were maliciously stored on the customers’ computers
• In addition, when the bank had warning that fraud was likely occurring in a given transaction, the bank did not monitor the transaction or give notice to its customer before completing the transaction
• Nonetheless, the First Circuit left open and remanded the question of whether Article 4A imposes any obligations or responsibilities on a commercial customer where a bank’s security system is commercially unreasonable

• On November 28, 2012, People’s United Bank reportedly agreed to settle Patco’s claims. Under the settlement, the bank would pay $390,000, which included the customer’s loss from the fraudulent withdrawals, plus interest

• Of note, the settlement agreement reportedly does not address the bank’s security procedures
Financial Services and
The Proposed EU General Data Protection Regulation

IAPP Global Privacy Summit
Washington
8 March 2013

Melanie Shillito, Director, Promontory
mshillito@promontory.com
Agenda

I. The proposed General Data Protection Regulation (GDPR)
   A. Territorial Scope
   B. New Definitions
   C. Principles and Processing Conditions
   D. Individuals Rights
   E. Data Controller/Processor Obligations
   F. Data Protection Officer
   G. Personal Data Transfers to Third Countries
   H. Sanctions

II. Rapporteur Report

III. What next
Territorial Scope

- The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU.

- The GDPR applies to processing of personal data relating to individuals residing in the EU by controllers established outside of the EU where activities relate to:
  - The offering of goods and services; or
  - The monitoring of their behaviour

- If the controller is established outside of the EU, and the above provision applies, a representative in the EU must be appointed unless:
  - The controller is established in an EU ‘approved country’
  - Goods and services are offered only occasionally
  - The enterprise employs less than 25 people
  - The controller is a public authority or body
## New Definitions

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Breach</td>
</tr>
<tr>
<td>Genetic Data</td>
</tr>
<tr>
<td>Biometric Data</td>
</tr>
<tr>
<td>Data Concerning Health</td>
</tr>
<tr>
<td>Main Establishment</td>
</tr>
<tr>
<td>Representative</td>
</tr>
<tr>
<td>Enterprise</td>
</tr>
<tr>
<td>Group of Undertakings</td>
</tr>
<tr>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>Child</td>
</tr>
</tbody>
</table>
Principles & Processing Conditions

• The Principles now include specific reference to:
  – Being transparent
  – Limiting personal data to the minimum necessary
  – The responsibility and liability of the data controller

• Processing conditions
  – Legitimate Interests condition is narrowed
    • Does not include legitimate interests of a third party
  – Legitimate interests cannot be relied upon for secondary purposes
  – There are specific conditions to be met if relying on consent
    • Explicit
    • Burden of proof on the Data Controller
    • Cannot be used if there is a significant imbalance between the individual and data controller
  – The exemptions to the prohibition on processing special categories of personal data now include
    • The establishment, exercise or defence of legal claims
    • Specific provisions relating to criminal convictions or related security measures
Individuals’ Rights

- Privacy Notices
  - Detail the contract terms and legitimate interests if applicable
  - Retention period
  - Right to lodge a complaint and the contact details of the supervisory authority
  - Recipients
  - Intended transfers

- Right of Access
  - One month
  - Free of charge
  - Electronic requests

- Right to be Forgotten
  - Not an absolute right

- Data Portability
  - Structured and commonly used format

- Profiling
  - Restrictions
Data Controller/Processor Obligations

- Data Protection by Design
- Joint Controllers/Processors
  - Specific recognition
- Personal Data Security Breach Notification
  - Without undue delay and where feasible the Data Protection Authority must be notified of all breaches within 24 hours
  - A data processor must inform the data controller immediately a personal data security breach is discovered
  - Document
  - Where the breach is likely to adversely affect an individual the individual must be notified without undue delay.
- Impact Assessment
  - If there is a specific risk, conduct a data protection impact assessment
  - Examples of areas of risk are detailed in the GDPR
- Prior Authorisation and Consultation
  - Needed in limited circumstances
Data Protection Officer

- A Data Protection Officer (DPO) must be appointed (Data Controller or Processor)
  - By a public authority or body
  - By an enterprise employing 250 or more
  - Where core activities require regular and systematic monitoring of individuals.
- The DPO must be appointed on the basis of professional qualities and expert knowledge of data protection law and practices and ability
- There must be no conflict of interest in the DPO duties
- The appointment must be for a minimum of two years
- The DPO can only be dismissed if he/she no longer fulfils the conditions required for performance of duties
- The DPO may be an external appointment
- The name of the DPO must be provided to the DPA and the public
- Individuals have the right to contact the DPO
- The DPO must have independence and be supported through the provision of staff, premises, equipment, etc.
Personal Data Transfers to Third Countries

• Personal data transfers to third countries or international organisations are allowed:
  – Where there has been an adequacy decision for the country/territory, processing sector or international organisation
  – Where appropriate safeguards are in place:
    • Binding Corporate Rules
    • EU Commission approved clauses (i.e. model clauses)
    • Standard DPA approved clauses in accordance with the consistency mechanism
    • Bespoke clauses authorised by a DPA (prior to processing)

• Derogations now include:
  – Legitimate interests of controller of processor as long as the transfers are not frequent or massive, and appropriate safeguards are in place
Sanctions

Administrative sanctions:

• Three levels of fine
  – Up to 250,000 EUR or if an enterprise, or up to 0.5% of the annual worldwide turnover
    • For not properly responding to individuals’ requests
    • For charging a fee for a subject access request
  – Up to 500,000 EUR or if an enterprise, up to 1% of the annual worldwide turnover
    • For not providing the requisite information to individuals
    • For not complying with the rights of individuals
  – Up to 1,000,000 EUR or if an enterprise, up to 2% of the annual worldwide turnover.
    • For processing without legal basis
    • For not adopting internal policies or implementing appropriate measures for demonstrating compliance
    • For not appointing a DPO
    • For not notifying a personal data breach

(Please note the examples given are not exhaustive.)
Rapporteur Report

- 218 page report
- 350 proposed amendments
- New definition of ‘producer’
  - Will need to comply with the ‘privacy by design and default’ obligations
- More limited ‘one stop shop’ Data Protection Authority
- Almost all companies will need to appoint a Data Protection Officer
- More focus on consent as the key criteria for processing
- Legitimate interest processing condition narrowed even further
- Information Notice (privacy statement) obligations increased and more difficult
- Territorial scope widened
- Fines – 72 hour notification obligation
- Much strengthened European Data Protection Board
What next

Adoption of First Position – European Parliament (Pending)

• 20/21 March: Consideration of Amendments (LIBE)
• 24/25 March: Orientation Vote (LIBE)

Adoption of First Position – Council of Ministers (Pending)

• When the Council has considered the regulation in full, a ‘General Approach’ is reached at the Committee of Permanent Representatives I (COREPER 1) following the adoption of the European Parliament’s position

Trialogues

• Trialogues between the European Parliament, Council of Ministers and European Commission are due to commence in the Summer/Autumn of 2013
• Can last from 3 months to 1 year
What next continued

Final Approval at the European Parliament and Council of Ministers

• When the European Parliament and Council have reached a common position, both amend their initial positions accordingly and put the texts to a final vote:
  ─ Plenary at the European Parliament
  ─ Justice and Home Affairs Council at the Council of Ministers
• It is difficult for individual institutions to further amend their respective texts at this stage.

Adoption

• The final text is approved by the Heads of the European Parliament and Council of Ministers and is published in the Official Journal of the EU.
Melanie Shillito
Director
Promontory Financial Group (UK) Limited
2nd Floor
30 Old Broad Street
London EC2N 1HT

Direct: 020 7997 3411
mshillito@promontory.com
Latin America and Asia Pacific
LATIN AMERICA
COLOMBIA

• Scope: applies to processing of personal data in Colombian territory and when processor/controller not in Colombia is subject to Colombia law

• Notice and Consent: need prior and informed authorization for processing
  – When requesting authorization, need to inform data subject of
    ➢ Processing to which personal data will be subjected and to purpose
    ➢ Rights of data subject
  – Explicit consent is required for sensitive information

• Cross-Border Data Transfer: cannot transfer personal data to countries that do not provide adequate level of protection unless
  – Express and unequivocal consent to transfer
  – One of specified legal bases applies
• Breach Notification: must inform DPA about any violations of security codes and any risks in administration of individual information

• Penalties:
  — Under Criminal code, penalties include imprisonment and fines
  — With respect to civil and/or administrative penalties, fines may be imposed, suspension of actives related to processing of personal information may be ordered, and temporary closure of operations may be ordered if noncompliance with orders continues
  — Individuals have private rights of action
PERU

• Scope: applies to personal information held in both publicly and privately administered databases

• Notice and Consent: must provide notice of specified information prior to collection of personal information
  – Prior, informed, express and unequivocal consent must be obtained to process personal information unless otherwise provided by law
  – To process sensitive information, consent must also be in writing

• Cross-Border Data Transfer: allowed if recipient has adequate data protection as determined by DPA
  – Certain specified expectations

• Penalties:
  – Fines may be imposed
  – No private right of action, but individual may be indemnified if affected by violation of law
COSTA RICA

- **Scope:** applies to automatic and manual processing by both public and private entities
- **Notice and Consent:** must inform individuals of specified information at the time of collection
  - Express consent required in written or electronic form to collect, use and disclose personal information unless one of limited exceptions applies
  - Processing of sensitive personal information is prohibited unless individuals consent or one of limited exceptions applies
- **Cross-Border Data Transfer:** may only disclose personal information with explicit consent and if transfer does not violate principles and rights under Costa Rican law
  - Rule applies broadly to all transfers whether within or outside Costa Rica
- **Penalties:** three levels of offenses with corresponding levels of sanctions
  - Most serious offenses may result in fines and suspension from using database
NICARAGUA

• Scope: applies to personal information of natural and legal persons in private and public databases
• Notice and Consent: must inform individual of specified information prior to processing personal information
  — When personal information collected directly from individual notice must enable individual to opt out of processing for purposes separate from those necessary to legal relationship
  — When remote means or electronic, optical or other technology (e.g., cookies) used to collect personal information, individual should be informed at that time about use of these technologies and how to disable it
  — Express consent required to process financial or economic data and sensitive information
• Cross-Border Data Transfer: may transfer when purposes are directly related to legitimate interests of organization and recipient, and individual informed about purposes of transfer and identify of recipient and consents
  – Transfer to countries that do not provide adequate security and protection is prohibited except in very limited circumstances
  – Requesting organization is accountable for transferred personal information
• Penalties:
  – Violations of law may result in criminal and/or civil penalties
ASIA-PACIFIC
MALAYSIA

• Scope: protects all personal information of natural persons processed in context of ‘commercial transactions’ that are processed in Malaysia and processed outside Malaysia where information is intended to be further processed in Malaysia

• Notice and Consent: must inform individuals whose personal information is collected and processed as soon as practicable, but specifically prior to, at time of, or before use of information for a purpose other than that for which it was originally collected or disclosure to a third-party
  – Consent is required to process personal information unless an exception applies
  – Explicit consent is required to process sensitive personal information
• Cross-Border Data Transfer: only may transfer to countries that have been approved unless exception applies

• Penalties:
  – Criminal sanctions include fines and/or imprisonment. Organizations are liable; directors and officers may be charged severally or jointly; where organization is found guilty, individuals will be deemed to have committed the offense unless they can prove otherwise
  – Commissioner can order processing to cease pending remedy of contraventions
  – There is no private right of action
PHILIPPINES

• Scope: applies to processing of all personal information
  — Applies to organizations and service providers that are not established in the Philippines but that use equipment located in the Philippines or those who maintain an office, branch or agency in the Philippines and applies to processing outside the Philippines if processing relates to personal information about a Philippine citizen or a resident and the entity has links to the Philippines.
  — Does not apply to personal information collected from residents of foreign jurisdictions in accordance with the laws of those jurisdictions and that is being processed in the Philippines
• Notice and Consent: must provide individuals with specified information about processing activities
  — Consent is required to process personal information or disclose personal information to third-parties for all purposes unless another justification or an exception exists
  — Consent must be evidenced in writing, electronic form or by recorded means
  — Processing of sensitive information is prohibited unless the individual has consented or an exception applies
• Cross-Border Data Transfer: organization is responsible for personal information transferred to a third-party, whether domestically or internationally

• Breach Notification: must notify promptly when sensitive personal information or other information that might to lead to identify fraud has been, or is reasonably believed to have been, acquired by an unauthorized person and such unauthorized acquisition is likely to give rise to a real risk of serious harm.

• Penalties: failure to comply can result in criminal and administrative penalties
  — If offender is a corporation, partnership or any legal person, penalty will be imposed upon responsible officers who participated in, or by their gross negligence allowed, commission of the crime
  — If offender is a legal person, court may suspend or revoke any of its rights under the Philippine Act
SINGAPORE

• Scope: governs collection, use and disclosure of personal information of natural persons, by private sector organizations incorporated or having a physical presence in Singapore

• Notice and Consent: at or before time of collection, must provide notice of specified information
  — Consent is necessary to collect, use and disclose personal information unless exception applies
  — No specific form of consent is required

• Cross-Border Data Transfer: can only transfer personal data outside Singapore if requirements in Act to ensure receiving organization provides protection for transferred data are met

• Penalties: criminal sanctions include fines and/or imprisonment
  — Private right of action exists
AMENDMENTS TO EXISTING LAWS

Australia

- Privacy principles for public and private sectors replaced with single set of privacy principles, the Australian Privacy Principles

Hong Kong

- Regulates more closely the use of personal information in direct marketing activities

Taiwan

- Because of concerns about the use of sensitive personal information and personal information collected prior to enactment of the amendment, implementation of following provisions has been delayed
  - Article which governs the collection, processing and use of sensitive personal information
  - Article which required data collectors to notify individual personal information collected was not obtained directly from the individual