

HYLANT



Data Privacy Liability



May 06, 2015

Discussion

Categories of Data Privacy Violations

Data Privacy Regulation: State, Federal and International

Data Privacy Costs

Data Privacy Best Practices

Data Privacy Risk Transfer/Insurance

Categories of Data Privacy

Improper Contact:

CAN-SPAM: Push Notifications: Opt-In medium

Improper Collection:

COPPA: Yelp: \$450,000; TinyCo: \$300,000

State Consumer Protection Statutes; California Song Beverly

Improper Disclosure:

State Privacy Notification Laws

HIPAA and FTC

Data Privacy Regulation: State

State Privacy Breach Notification Laws:

- Subject to the state the affected party resides, not where you are headquartered or where the breach occurred.
- 47 states with legislation, plus D.C. and Puerto Rico
- Requirement to Notify State AGs

What to watch for:

- Increased Training & Maintenance Requirements
MA-Inventory PII and educate employees about safeguards
- Expanded Definition PII:
CA and FL-Username and Password
- Other State Laws similar to California Medical Info Act: \$1,000 per record
- Increased Regulatory Actions by State Attorney General's Offices
- Creativity of Plaintiff Attorneys

Data Privacy Regulation: Federal

Health Insurance Portability and Accountability Act (HIPAA)

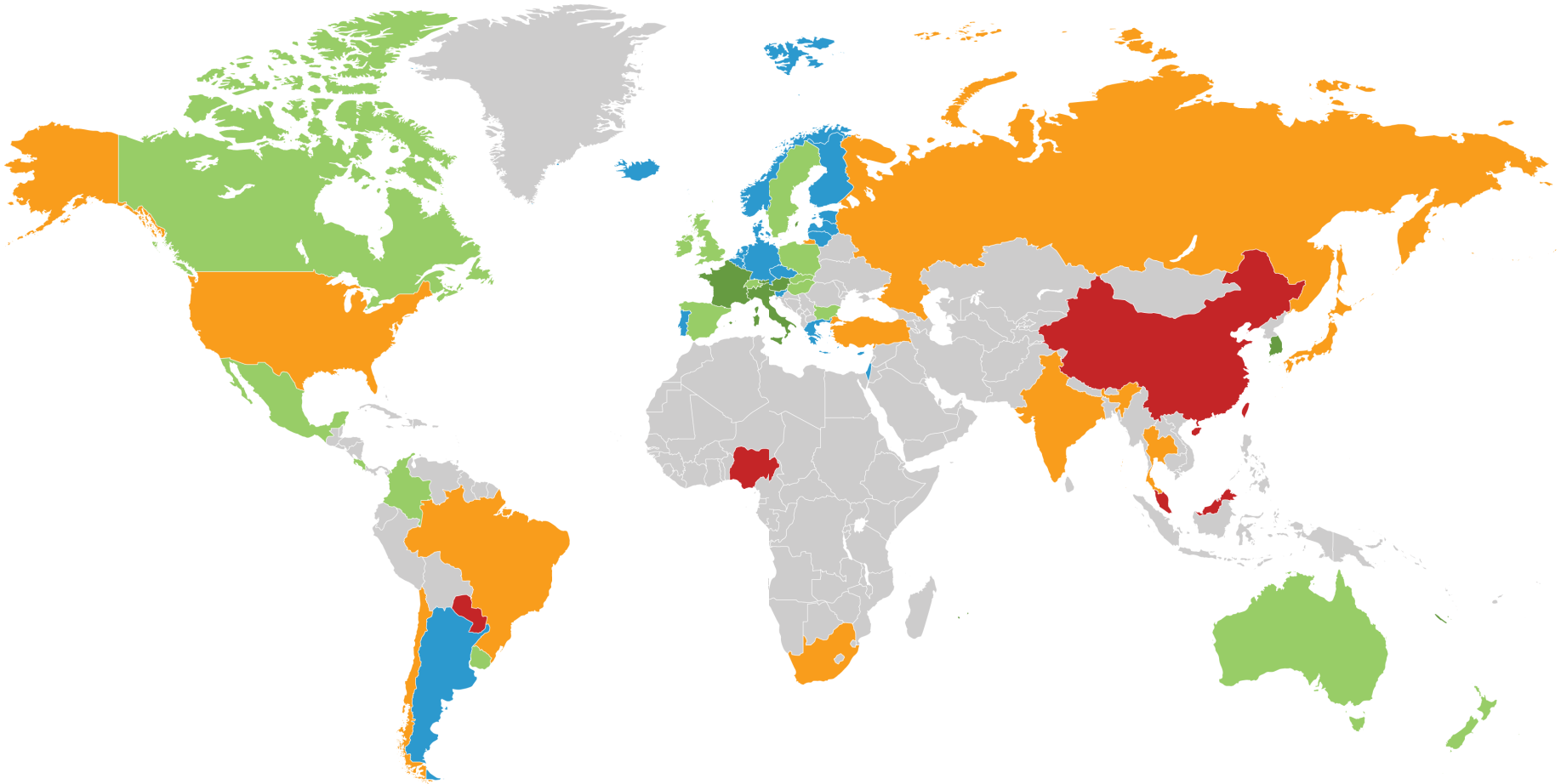
Universal Federal Cyber Security Laws: not yet but...
Cyber Threat Sharing Bills Passed in the House

FTC Act, Section 5: Unfair or Deceptive Trade Practices:
Violation of Your Privacy Policy

What to watch for:

- Increased Enforcement from OCR; FTC; SEC
- Continued HIPAA Audits, including Business Associates
- Creativity of Plaintiff Attorneys

Data Privacy Regulation: International



Source: US Department of Commerce and country specific legislation: Forester Research

- Most restricted
- Restricted
- Some restrictions
- Minimal restrictions
- Effectively no restrictions

Data Privacy Regulation: International

European Union:

- Everyone has the fundamental right to the protection of personal data
- Notification Requirement to the Data Protection Authority
- Fines of up to 5% annual revenues including direct lawsuits
- Consent for the use of personal data should be explicit and must be obtained through affirmative action
- Data Transfer Outside of EU: Binding Corporate Rules

What to watch for:

How will other countries address Privacy Regulation?

Canada, Mexico & some Asian countries have enacted laws

Required Notification vs “Best Practices” Notification:

Affected parties and/or Privacy Regulators

How can/will it be enforced for business that do not have physical locations in those countries?

Data Privacy Costs?

Breach Expenses



Notification

Credit
Monitoring

Forensics

Legal

Liability



Damages to
Affected Parties

Legal Costs

Regulatory



Regulatory
Defense

Fines and
Penalties

Best Practices

1. Inventory your Data:
What kind? How Much? Where is it? Who has access? How is it protected? Health Data? Log-In Credentials? Credit Cards Data? Financial Data? SS#?
2. Evaluation of contracts with outside service providers, specifically 3rd party IT, data storage or data processing vendors
3. Require and obtain certificates of insurance for both Professional E&O and Privacy/Cyber Liability coverage
4. Continuous 3rd party assessments
5. Build an Incident Response Team with Experienced Outside Vendors
6. Test Your Incident Response Plan with Table Top Exercises
7. Evaluate the need for insurance as a “safety net” to other internal and external safeguards

Risk Transfer: Why has the insurance become so attractive?

- Inability to completely eliminate all risks through...
 - IT security Investments
 - Indemnification Provisions with 3rd party vendors
 - The Human Factor
- Board Level Pressures: Protect Corporate Assets
- Increased legislation, regulatory enforcement and ever creative plaintiffs bar
- Alignment with Breach Response Teams
- Loss Prevention Services
- Proven Balance Sheet Protection...PAID CLAIMS

What does the Data Privacy Risk Marketplace look like?

- Traditional Insurance Excluding Data Privacy Claims
- 50+ insurance companies Standalone Cyber
- 2014: \$2 Billion Premium...\$10 Billion
- Race for market share means lower premiums and broader coverage
- Knowledge Gap: Underwriting and Agents
- Department of Treasury's Push for Information Sharing and Cyber Insurance