HOSPITALITYLAWYER.COM PRESENTS

THE 2010 HOSPITALITY LAW CONFERENCE

FOCUSING ON WORLDWIDE LEGAL, SAFETY & SECURITY SOLUTIONS

FEBRUARY 3-5, 2010 • HOUSTON, TEXAS

Information Protection & Privacy – The New High Stakes Game

Chris Zoladz

HospitalityLawyer.com

Presenter

- Chris Zoladz, Founder, Navigate LLC
- Founded Navigate in April 2009 to provide strategic and tactical information protection & privacy consulting services
- Former Vice President, Information Protection & Privacy at Marriott International, Inc.
- Founding Board Member and Past President of the International Association of Privacy Professionals (IAPP)

Agenda

- The Perfect Storm
  - Customer Expectations
  - Business Demands
  - Legal Requirements
- Risk Management Challenges
- Gauging Your Risk
- Recommendations
- The Future

Disclaimer

The information in this presentation is provided for informational purposes only, and is not intended and should not be considered to be legal advice.

Events Shaping Consumer Concerns

- Since 2005 there have been over 341 million records put at risk in the U.S.

  (Source: Privacy Rights Clearinghouse)

- 91% linked to organized crime

  (Source: Verizon Business Services)

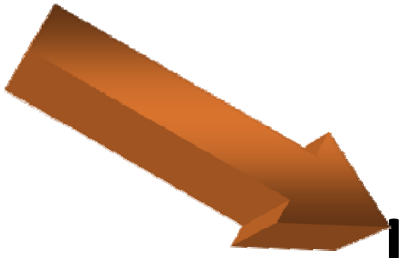
- Some recent headlines:
  - HeathNet
  - HSBC
  - Notre Dame

Customer Expectations

- ✓ Protect their personal information
- ✓ Do not overuse or misuse their information
- ✓ Inability to meet these expectations results in loss of loyalty and business

Business Demands

- Maximize revenues and return to shareholders
- Do more with less



Increased risk

  - Standard processes and controls are bypassed or not completely followed
  - Movement to outsourcing (e.g., cloud computing) without understanding if and how security requirements are met
- Personalized marketing and service delivery

PCI DSS

PCI DSS = Payment Card Industry Data Security Standard

Comprehensive mandatory information security standard required by credit card companies

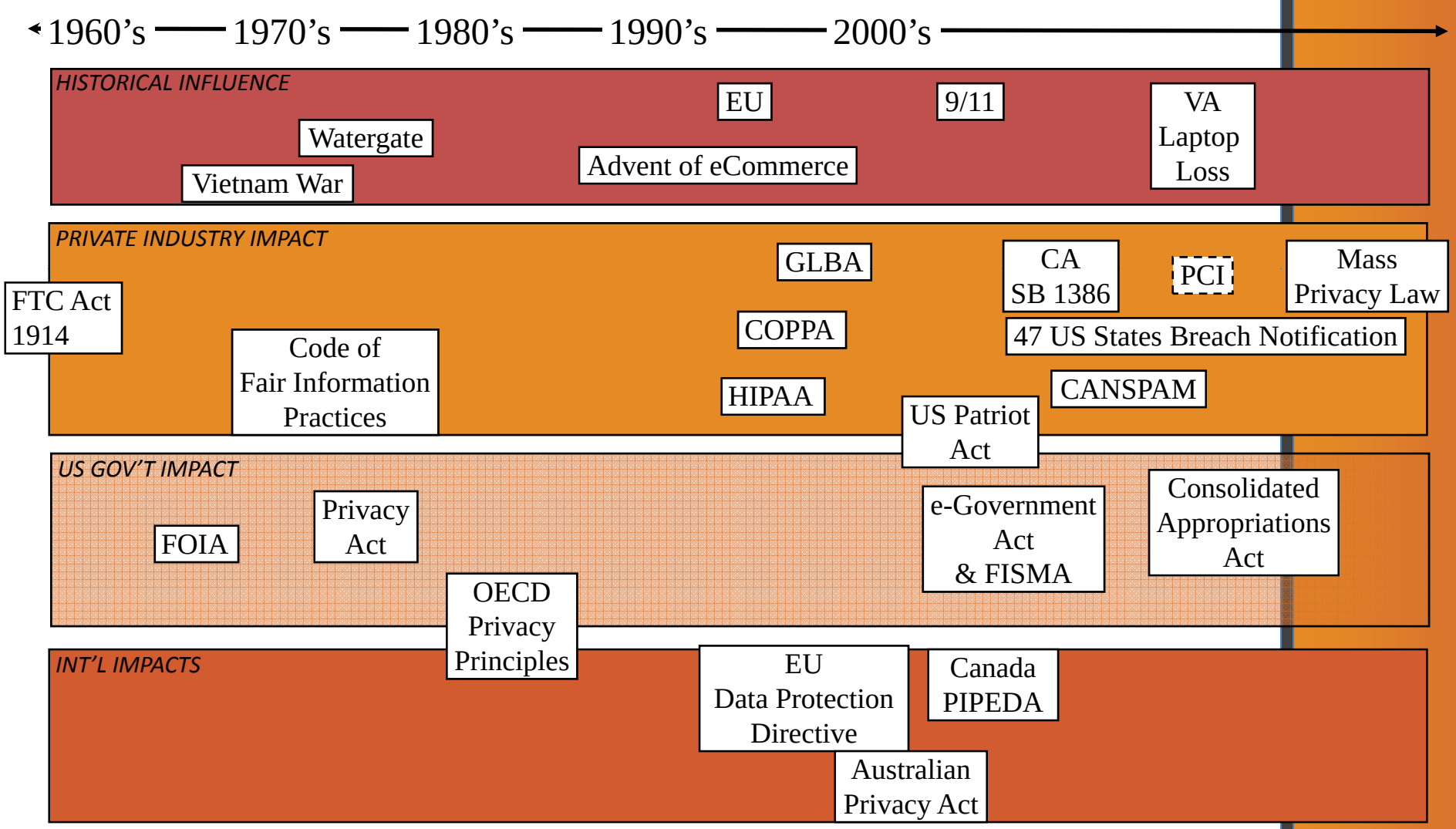
12 Security Categories

Approximately 250 Specific Requirements

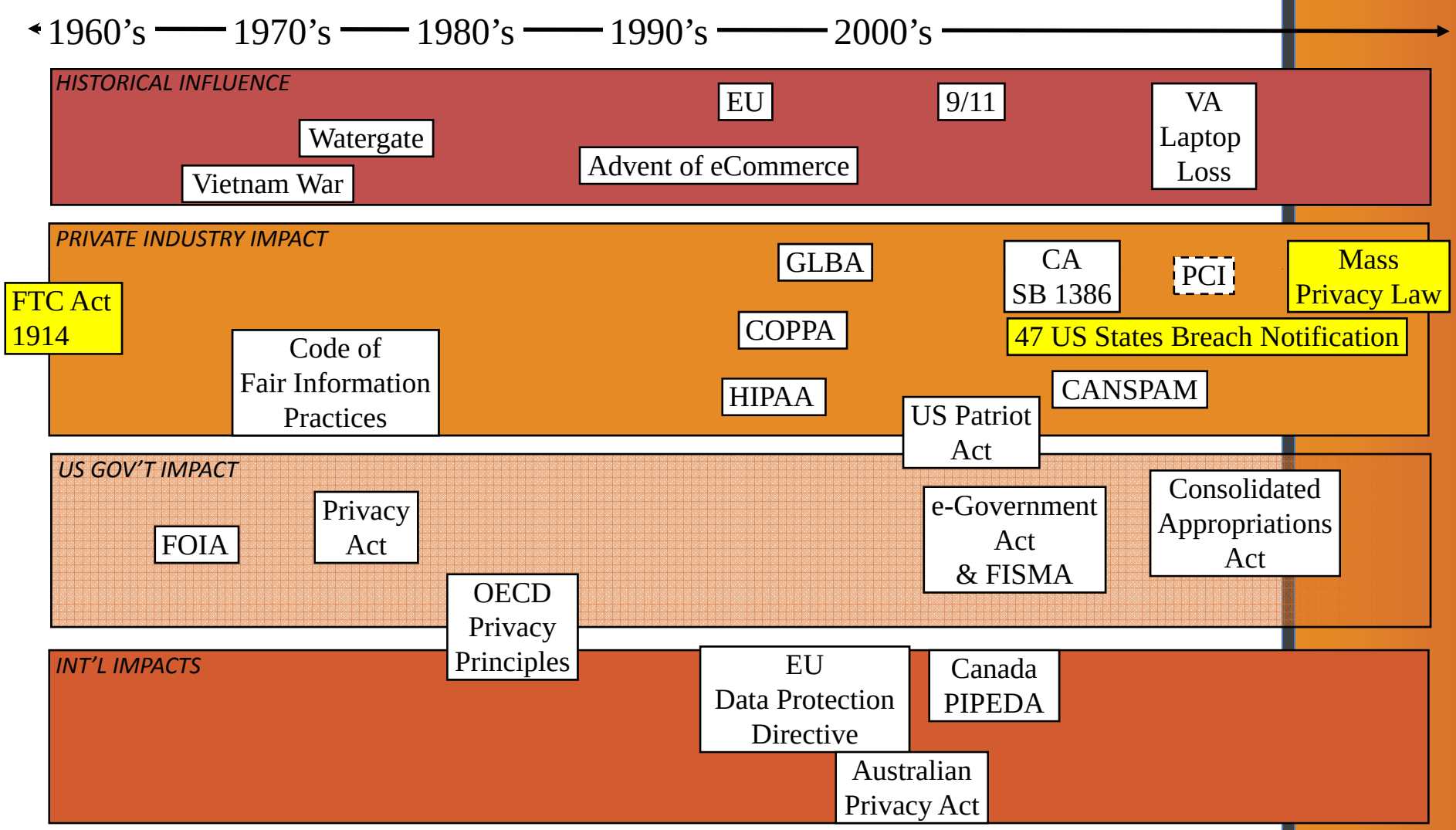
Pertains to every business process, computer system, website & service provider that involves the:

- **Collection**
- **Processing**
- **Storage**
- **Transmission of card data**

Timeline of Key Privacy Legislation



Timeline of Key Privacy Legislation



FTC's Position

"Privacy is a central element of the FTC's consumer protection mission." *(Source: www.ftc.gov)*

"Internet privacy has been and will remain a foremost area of focus. On behavioral marketing, there are obviously benefits that targeting can bring to consumers in the form of more relevant advertising and the additional revenue that targeting can provide. This revenue may be vital to the survival of some industries. But we have to face the fact that the current model is not working."
(Source: Speech by Jon Liebowitz – FTC Chairman in March 2009)

FTC Act

- Focuses on “unfair” or “deceptive” trade practices

- Settlements:
  - range from tens of thousands to millions of dollars
  - include agreement by the company to independent oversight of their information security program for 20 years.

- Learn More

  http://www.ftc.gov/privacy/privacyinitiates/promises_educ.html

U.S. State Security Breach Laws

- 47 States including the District of Columbia have a breach law
- The laws are similar but not the same, differences include:
  - Definition of a breach
  - Inclusions and exceptions
  - Definition of PII
  - Notification Requirements
- Learn More *http://www.mofoprivacy.com/disclaimer.aspx*

Massachusetts – Are You Ready?

- Standards for The Protection of Personal Information of Residents of the Commonwealth (effective March 1, 2010)

Affects all companies that own, license, store or maintain personal information concerning any Massachusetts resident.

- It is the most recent and most restrictive of any State

Massachusetts in Detail

- ✓ Written Information Security Program ("WISP)
- ✓ Designated Program Owners
- ✓ Employee Training
- ✓ Policies
  - ✓ possession of PII outside the facility
  - ✓ remote access to PII
  - ✓ disciplinary actions for violations
- ✓ Prevent terminated workers from accessing PII
- ✓ Service Provider program
- ✓ Limit the collection, storage and access to PII
- ✓ Risk Assessments
- ✓ Incident Response
- ✓ Inventory paper and electronic records as well as systems and media
- ✓ Regularly monitor and annually review security measures
- ✓ Encrypt PII on laptops, portable devices
- ✓ Specific computer security requirements

Learn More http://www.mass.gov/?pageID=ocahomepage&L=1&L0=Home&sid=Eoca

Risk Management Challenges

- "It won't happen to us" syndrome
- PII can be in many locations – paper and electronic
  - Laptops, Flash drives, CDs
  - Blackberrys, iPhones
  - Homes' of Teleworkers
  - Third party service providers
  - Contractors of third party service providers
- Limited staff and resources to assess and mitigate risk
- Potential resistance to business process and/or technology changes
- Focus on revenue generating/cost cutting initiatives - period

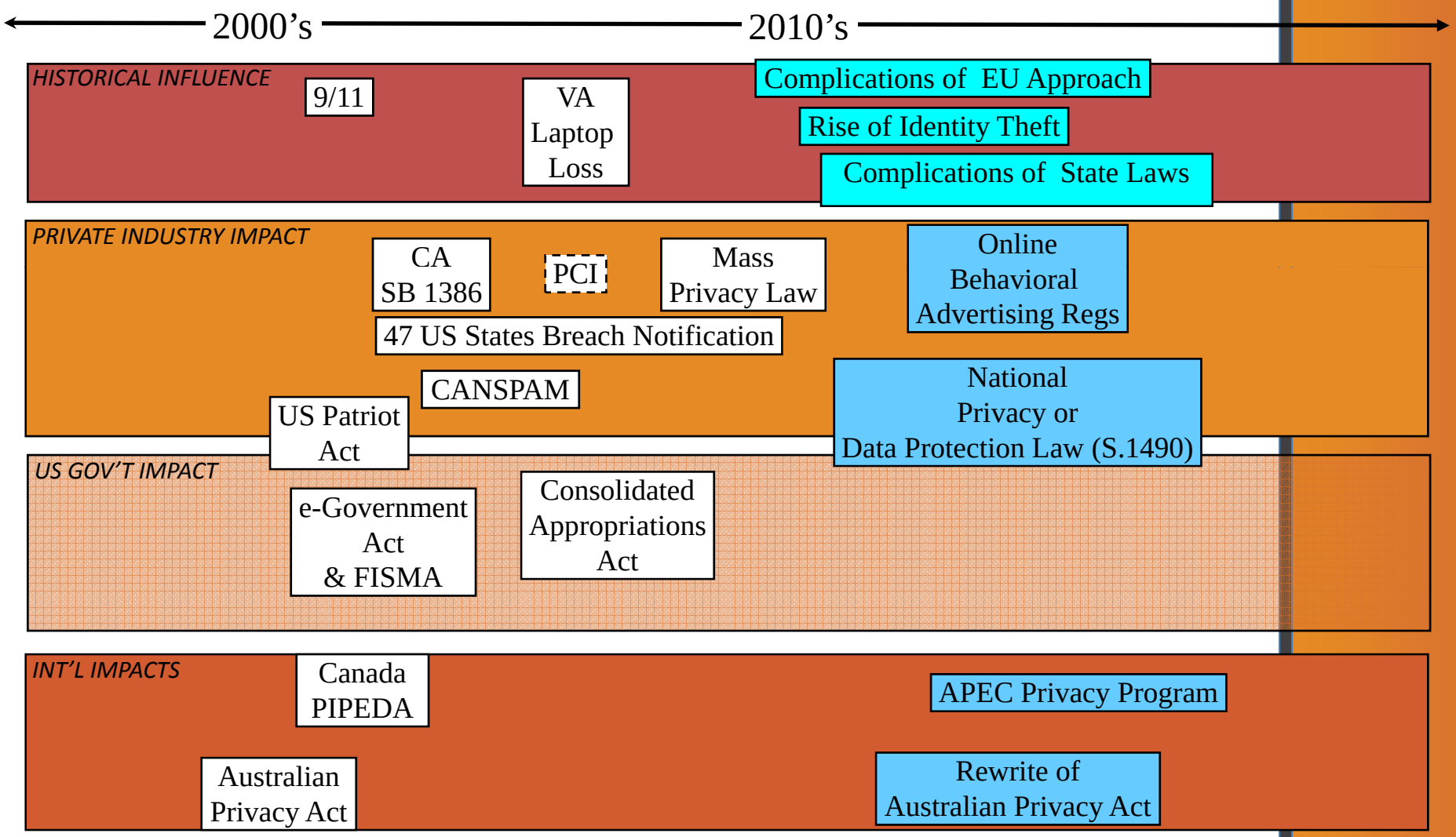
Gauging Your Risk

- Are there adequate resources dedicated to this area?
- Are the necessary activities being focused on?
  - Policies and procedures
  - Training
  - Communications
  - Risk Assessment
  - Monitoring new threats and legal requirements, etc.
- Is there a current risk assessment?
- Does it include all the places PII is contained?

Gauging Your Risk (cont'd)

- Is senior management aware of the risks?
- Are remediation plans prepared and implemented?
- Have insurance options been considered?
- Is the residual risk documented and approved by senior management?
- Is there an effective process to manage information protection & privacy risks and legal requirements on an on-going basis?

Future of Privacy Legislation



S.1490 - *Personal Data Privacy and Security Act of 2009*

- A bill to:
  - Prevent and mitigate identity theft
  - Ensure privacy
  - Provide notice of security breaches
  - Enhance criminal penalties
  - Enhance law enforcement assistance
  - Enhance other protections against security breaches, fraudulent access, and misuse of personally identifiable information
- $5,000 per day per violation, up to a maximum of $500,000 per violation, double if there is an intentional or willful violation

Recommendations

- Data minimization
- Eliminate data duplication
- Secure destruction
- It is not all or nothing - do as much as you can as quickly as you can
- Be prepared to defend your company

Questions and Contact Details

Chris Zoladz, Founder, Navigate LLC

Chris@navigatellc.net, or 240-475-3640

Learn More http://www.navigatellc.net