

# Legally Defensible, Proactively Protected

David Navetta, Esq., CIPP

Benjamin Tomhave, MS, CISSP



# David Navetta, Esq., CIPP



- ✳ Founding Partner, InfoLawGroup LLP
- ✳ Co-Chair, ABA Information Security Committee
- ✳ Certified Information Privacy Professional (through IAAP)





# Ben Tomhave, MS, CISSP



- \* Gemini Security Solutions
- \* MS Engineering Mgmt  
(InfoSec Mgmt)
- \* Co-Vice Chair, ABA ISC
- \* ~15 yrs (AOL, WF, E&Y,  
INS/BT, ICSA Labs)





# “Just the Facts”

- \* Not if, but when
- \* Mounting legal costs
- \* Increasing regulatory burden



**SECURITY PROS WILL HAVE TO DEFEND  
THEIR DECISIONS IN A FOREIGN REALM:  
THE LEGAL WORLD**



# The Gap is Acute

- ✱ Collision of the legal and information security worlds
- ✱ More regulations, more lawsuits, more contract obligations
- ✱ Making decisions that have legal implications and interpreting legal requirements
- ✱ Conversation is lacking or non-existent

# The Gap is Acute

- ✱ Collision of the legal and information security worlds
- ✱ More regulations, more lawsuits, more contract obligations
- ✱ Making decisions that have legal implications and interpreting legal requirements
- ✱ Conversation is lacking or non-existent

**RESULT:**  
**INCREASED LEGAL RISK FOR ORGANIZATIONS!**



# Multiple Legal Regimes

- \* State, Federal, International (e.g. E.U.)
  - \* Evolving & Overlapping laws, jurisdictions
  - \* Regulator / private enforcement
- \* Contract law
- \* Tort law
- \* Securities law





# Legal Defensibility

- ✱ Viewing requirements from an external legal perspective (plaintiff, judge, jury, regulator)
- ✱ Security choices become legal positions
- ✱ Security decision-making process with legal baked in
- ✱ The goal is to anticipate reasonably foreseeable (legal) consequences and reduce legal risks



# Using Legal Defensibility...

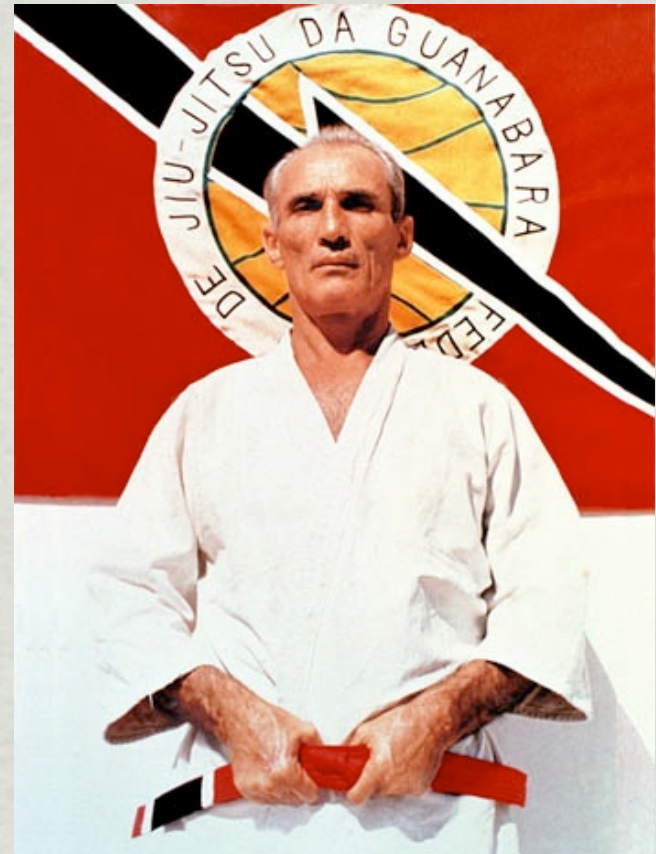
- ✱ Key Attributes
- ✱ Real-World Examples
- ✱ Recommended Steps
- ✱ Action Plan





# Sidebar: LegDef Origins

- ✱ Survivability
  - ★ Defensibility
  - ★ Recoverability
- ✱ Resilience
- ✱ How to codify?





# Key Attributes

- \* Risk Management
  - \* Awareness, Understanding, Translation
  - \* Collaboration
    - \* Documentation of... decision-making processes... key infosec decisions with potential for legal impact.
      - \* Attorney-client privilege



# Real-World Examples

- ✱ HHS: investigations v. actions  
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html#seventh>
- ✱ Online banking
  - ✱ Shames-Yeakel v. Citizens Financial Bank
  - ✱ EMI v. Comerica
- ✱ Guin v. Brazos Higher Education Service Corp. Inc.



# PCI Interpretative Variances

**12.8** If cardholder data is **shared** with **service providers**, maintain and implement policies and procedures to manage service providers, to include the following:

**12.8.1** Maintain a list of service providers.

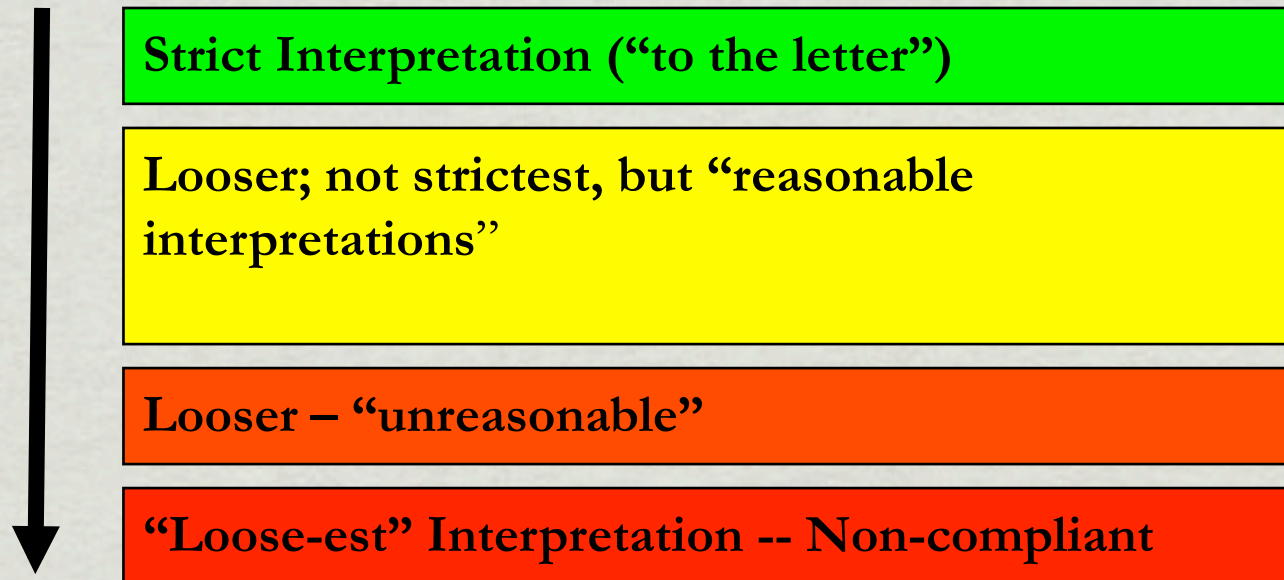
**12.8.2** Maintain a **written agreement** that includes an acknowledgement that the service providers are **responsible for the security of cardholder data** the service providers possess.

**12.8.3** Ensure there is an **established process** for engaging service providers including **proper due diligence** prior to engagement

**12.8.4** Maintain a **program** to **monitor** service providers' PCI DSS compliance status.

# Security v. Legal Viewpoint

## PCI SECURITY VIEWPOINT V. LEGAL VIEWPOINT





# Key Legal Issues

- \* “Reasonable” “Appropriate” “Comprehensive” “Adequate”
- \* Risk-based factors
  - \* Size, scope, type, complexity of organization
  - \* Nature and scope of activities
  - \* Resources of company
  - \* Sensitivity of data
  - \* Volume of data
- \* Third-party security assessments – matching risk tolerance



# Key Legal Issues

- ✱ What legal obligations?
- ✱ Interpretation by courts/regulators
- ✱ **Foreseeability!**
- ✱ Plaintiff attorney strategies
- ✱ Litigation strategy and procedure





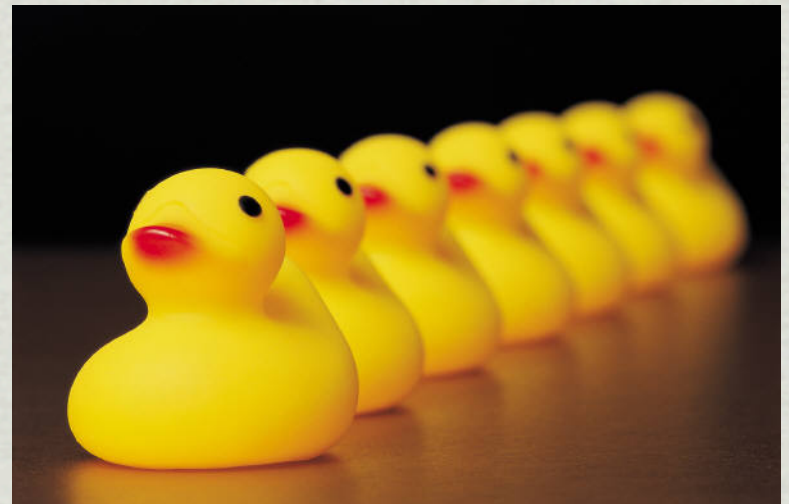
# Examples of Legal Obligations

- \* Security “standards” under the law
- \* Contract obligations
- \* Service providers and outsourcing
- \* Document retention and preservation



# Indicia of Legal Compliance

- \* Risk analysis and remediation
- \* Comply with own policies
- \* Misrepresentations
- \* Specific controls
- \* Vendor management
- \* Compliance with standards





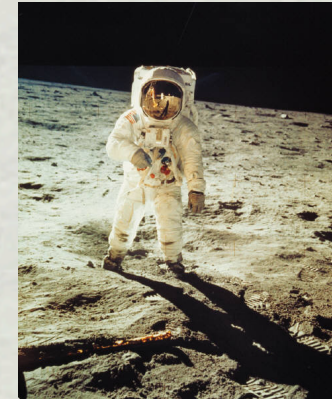
# Recommended Steps

- \* A champion arises!
- \* Find your allies
- \* Perform analysis
- \* Create your strategy
- \* Execute (w/ documentation!)





# Action Plan



1. Hold key stakeholder meeting(s) and collaboration
2. Conduct information security legal audit
  - ★ What legal requirements apply?
  - ★ Do current security measures address those legal requirements?



# Action Plan

## 3. Conduct legal defensibility analysis:

- ★ Develop security decision process formally incorporating legal analysis
- ★ Address areas of non-compliance
- ★ Develop legal positions on high risk legal requirements
- ★ Develop legal positions for “gray area” legal requirements

# Action Plan

## 4. Memorialize positions and proof:

- ★ Document indicia of legal compliance (e.g. identify standards compliant with, documentation of due diligence, etc.)
- ★ Document applicable legal positions under attorney-client privilege





**Q & A**

**THANK YOU!**

# Contact Information

- \* David Navetta, Esq., CIPP

- \* [www.infolawgroup.com](http://www.infolawgroup.com)

- \* [dnavetta@infolawgroup.com](mailto:dnavetta@infolawgroup.com)



- \* Benjamin Tomhave, MS, CISSP

- \* [geminisecurity.com](http://geminisecurity.com)

- \* [btomhave@geminisecurity.com](mailto:btomhave@geminisecurity.com)

