

Privacy Compliance: A practical approach to demonstrating proper data governance



Agenda

- Privacy means different things to different people...
 - › Legal Staff, State AG, Legislators, Individual, Company
- The relationship that “Privacy” really has to security
- Impact of Privacy culture
- Do any frameworks address Privacy?
- Can we use existing security tasks to show Due Care?



Where it all began...

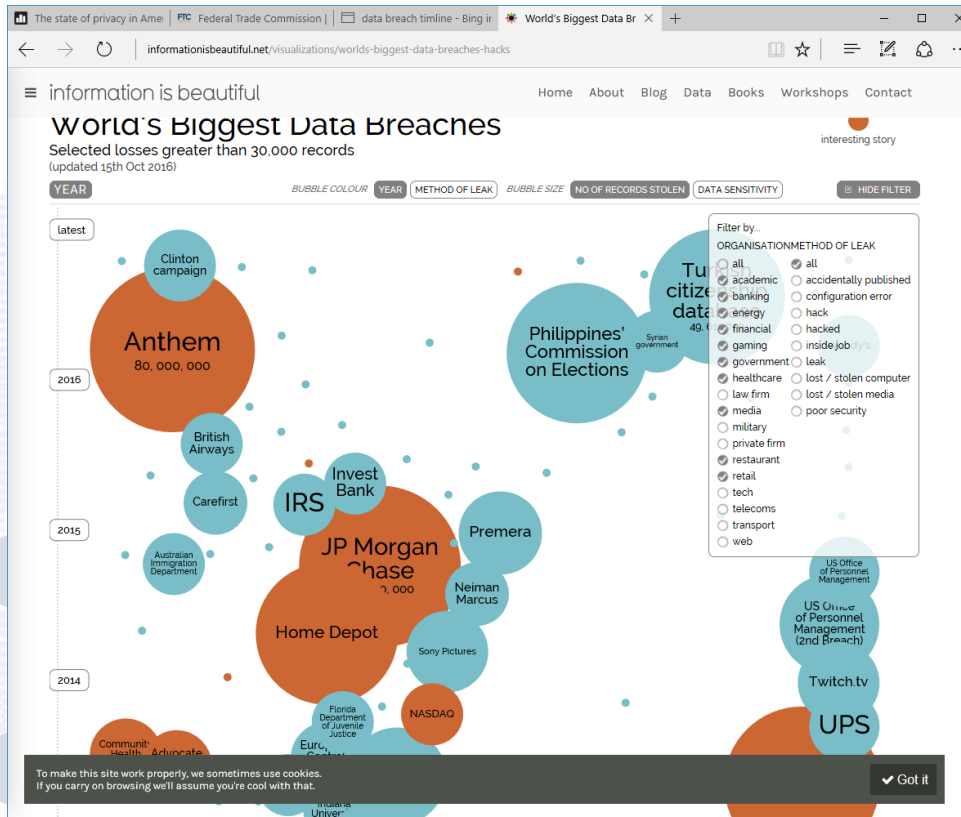
Information Graphics (Infographic)

The screenshot displays a web browser window with the URL <http://www.tiki-toki.com/timeline/entry/480661/A-Brief-History-of-US-Federal-Data-Privacy-Laws>. The page title is "Tiki-Toki A Brief History of US Federal Data Privacy Laws". The main content is a timeline for June 2002, featuring several key events:

- OMB MEMORANDUM**: OMB A-130 Management of Federal Information Resources
- EVENT**: Data Quality Act (Focuses on ensuring and maximizing the quality, objectivity, utility, and integrity of)
- MAJOR COMPREHENSIVE LAW**: Federal Information Security Management Enacted as Title III of the E-Government Act
- MAJOR COMPREHENSIVE LAW**: E-Government Act (Enhances the management and promotion of electronic Government services and)
- OMB MEMORANDUM**: OMB Memo April 7, 2010 (Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction)
- MAJOR COMPREHENSIVE LAW**: Confidential Information Protection and Enacted as Title V of the E-Government Act

The timeline interface includes a navigation bar with "ABOUT THIS TIMELINE", "CREATE A TIMELINE", "CONTACT", "LOGIN", and "FREE SIGN UP". At the bottom, there are advertisements for Ganttology and TikiToki Desktop.

<http://www.tiki-toki.com/timeline/entry/480661/A-Brief-History-of-US-Federal-Data-Privacy-Laws/>



<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



Privacy as a consequence

Events -> Financial Loss -> Consumer Outrage -> State Law -> A business
consequence: requiring notification (Wall of Shame) -> Decrease in consumer trust ->
Investment by business in security -> Consumer protection agencies seek penalties ->
Reasonable Man Test

Privacy Law ([Link](#))

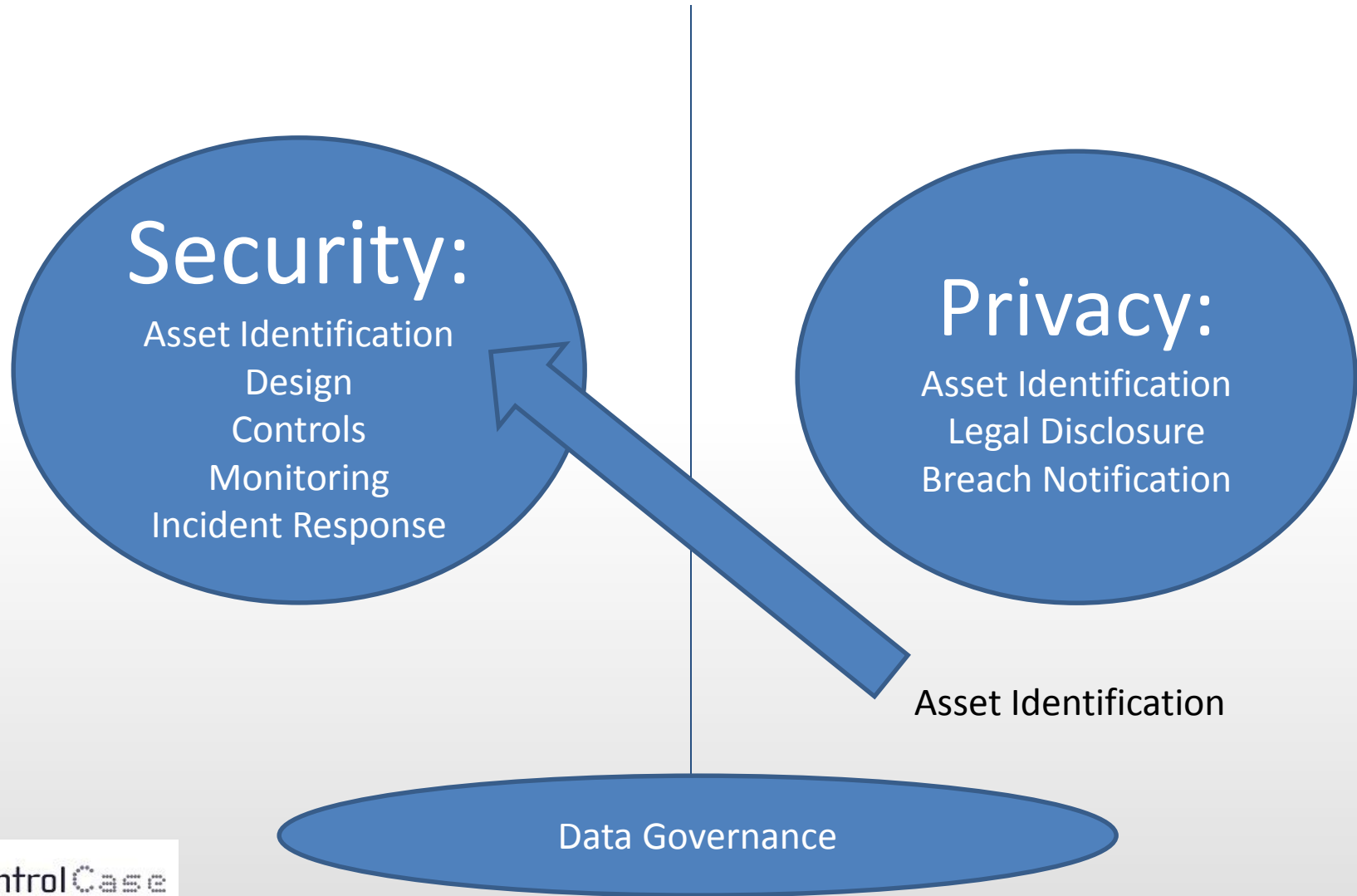
• State Reaction

- Lack of Federal law created a legal vacuum filled by independent states
- Trend in constituents who wanted action in response to breach
- Unrealistic language for business to manage effectively nationally- Harm or No Harm, Encryption exclusion or not, Specific data element included or not...
- Untenable situation for security pros to react appropriately * (**Dreaded word- Sensitive**)

• Federal Reaction

- 8+ bills drafted
- Both parties sponsored similar language
- Pre-emption in question
- Mass., Ca., NH. used as reference language but bills in waiting are not keeping up with changes
- Harm trigger is one sticking point for breach notification provision

Privacy as an input to Security



Privacy Culture Transformation

- Those that value privacy
 - Group Discussion: Who???
- Those that trade privacy
 - Group Discussion: Who???

Assessing Privacy Program Maturity

• Less Mature

- Legal discussion only
- Security team does not manage to privacy culture change
- Security program unable to navigate even vernacular differences... *not a linguistics problem*
- Employees handling consumer data and product development staff cannot demonstrate internal changes to privacy concerns

• More Mature

- All internal corporate teams at the table i.e. every staff member in every department can state the value of being a good custodian of consumer/employee data
- Responsible party (e.g. data protection officer) identified and effective
- Evidence of discovery of consumer and employee data produced and findings addressed
- Employee education/sensitivity training provided and updated with real internal incidents
- Data governance program in place

Suggested Engine for Data Governance

Data Governance Program





Thank You !