ControlCase
Compliance as a Service

Privacy Compliance: A practical approach to demonstrating proper data governance

Agenda

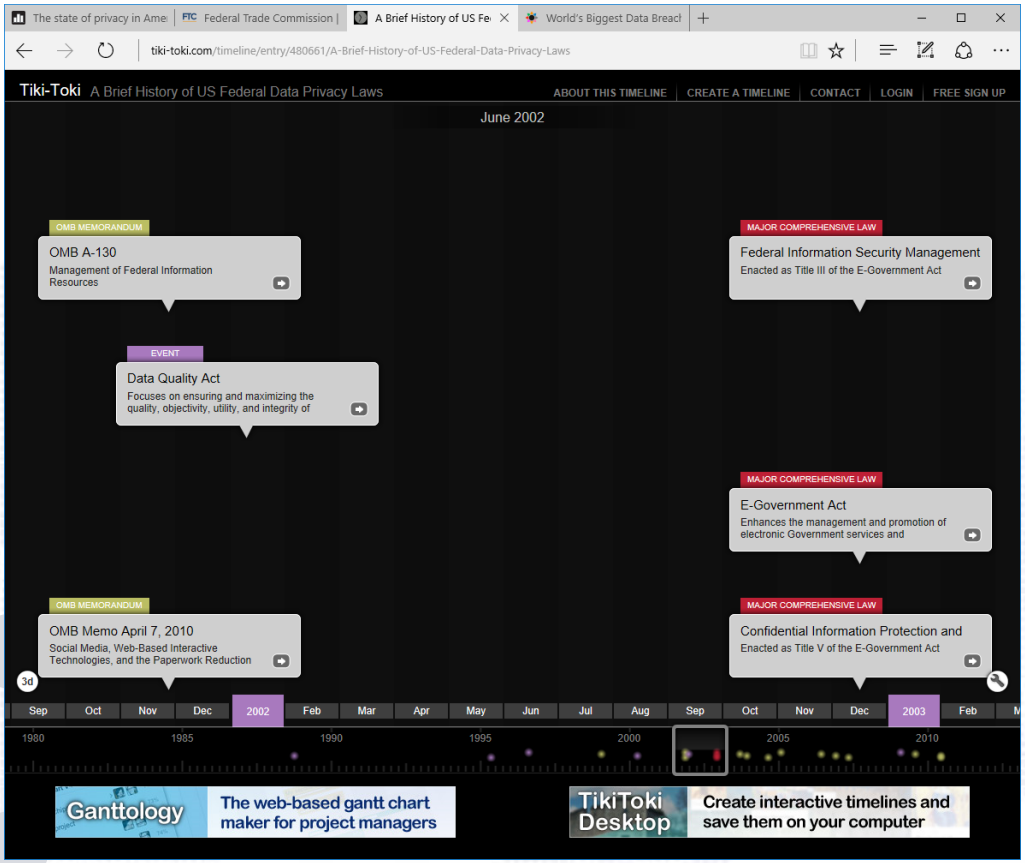
- Privacy means different things to different people…
  - Legal Staff, State AG, Legislators, Individual, Company
- The relationship that “Privacy” really has to security
- Impact of Privacy culture
- Do any frameworks address Privacy?
- Can we use existing security tasks to show Due Care?

ControlCase
Compliance as a Service

Where it all began…

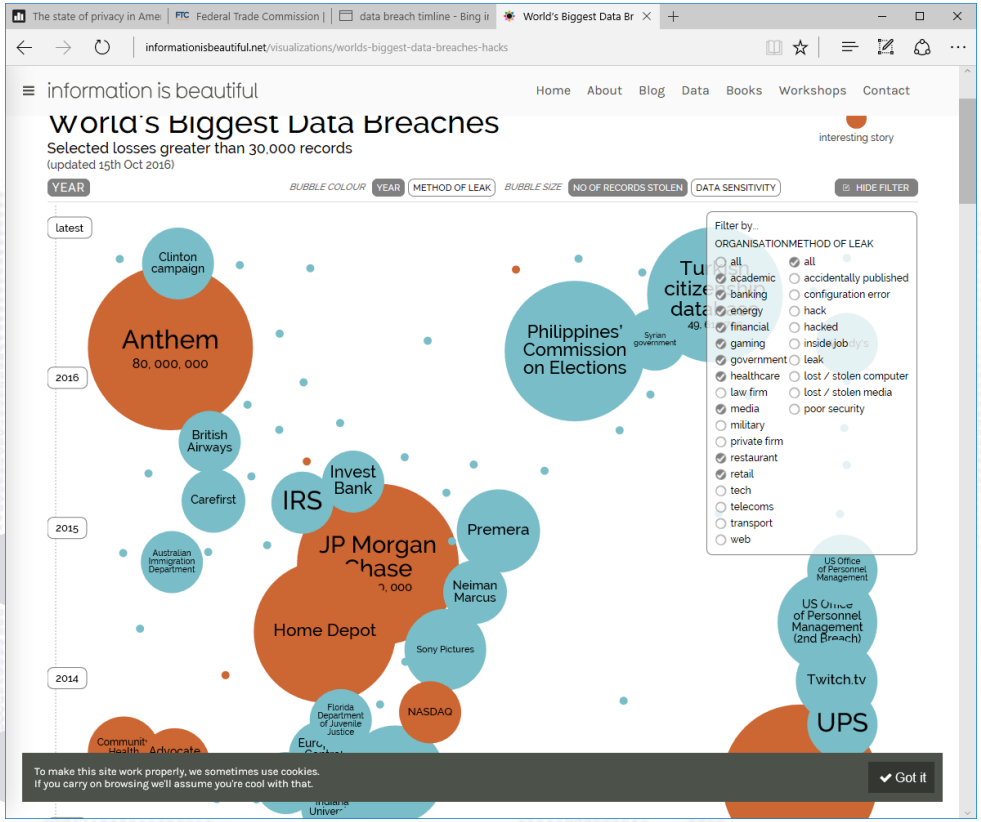
Information Graphics (Infographic)

ControlCase
Compliance as a Service



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

ControlCase
Compliance as a Service



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

ControlCase
Compliance as a Service

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

ControlCase
Compliance as a Service

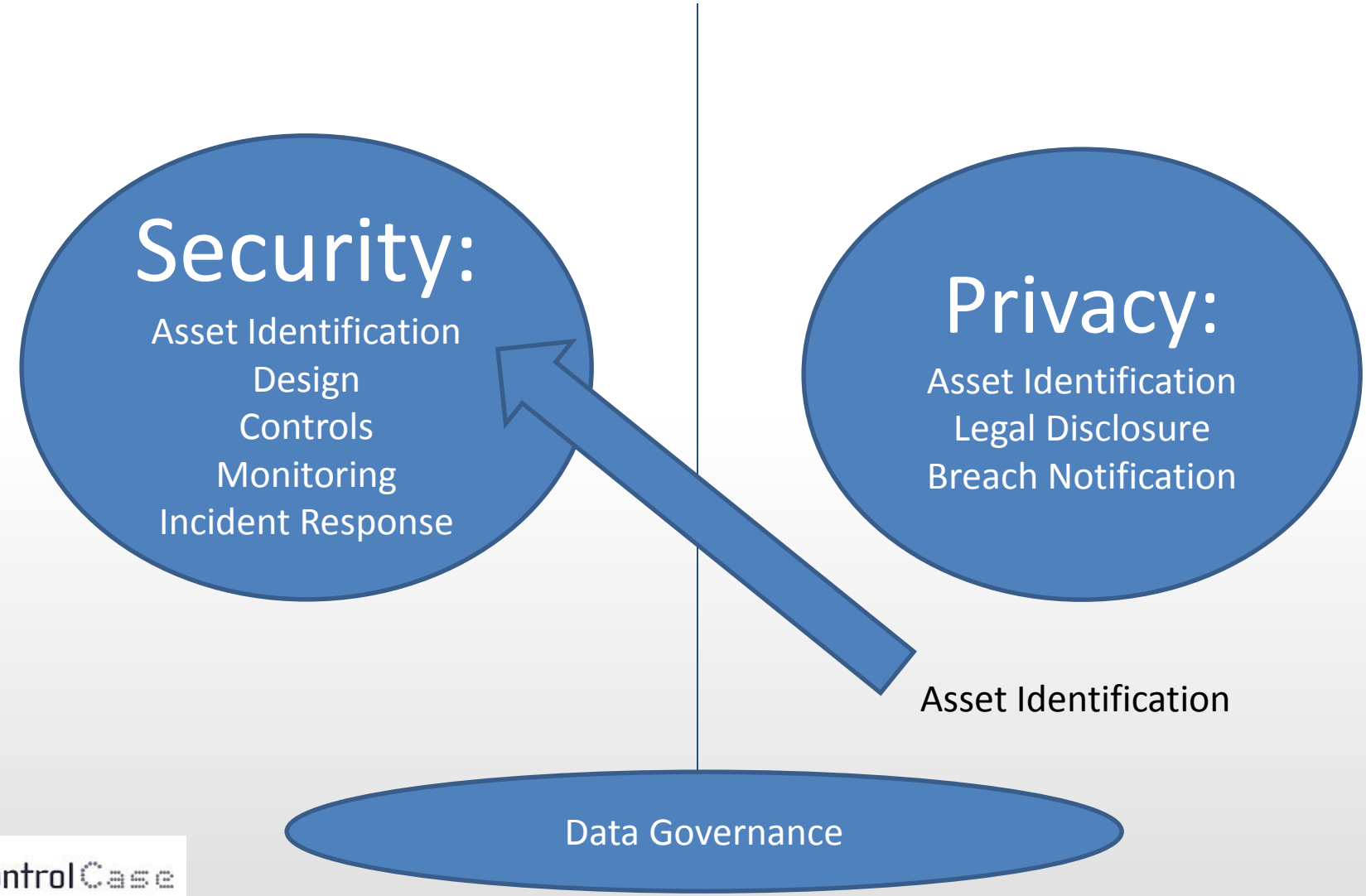
Privacy Law (Link)

- **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

ControlCase
Compliance as a Service

Privacy as an input to Security



ControlCase
Compliance as a Service

Privacy Culture Transformation

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

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

ControlCase
Compliance as a Service

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

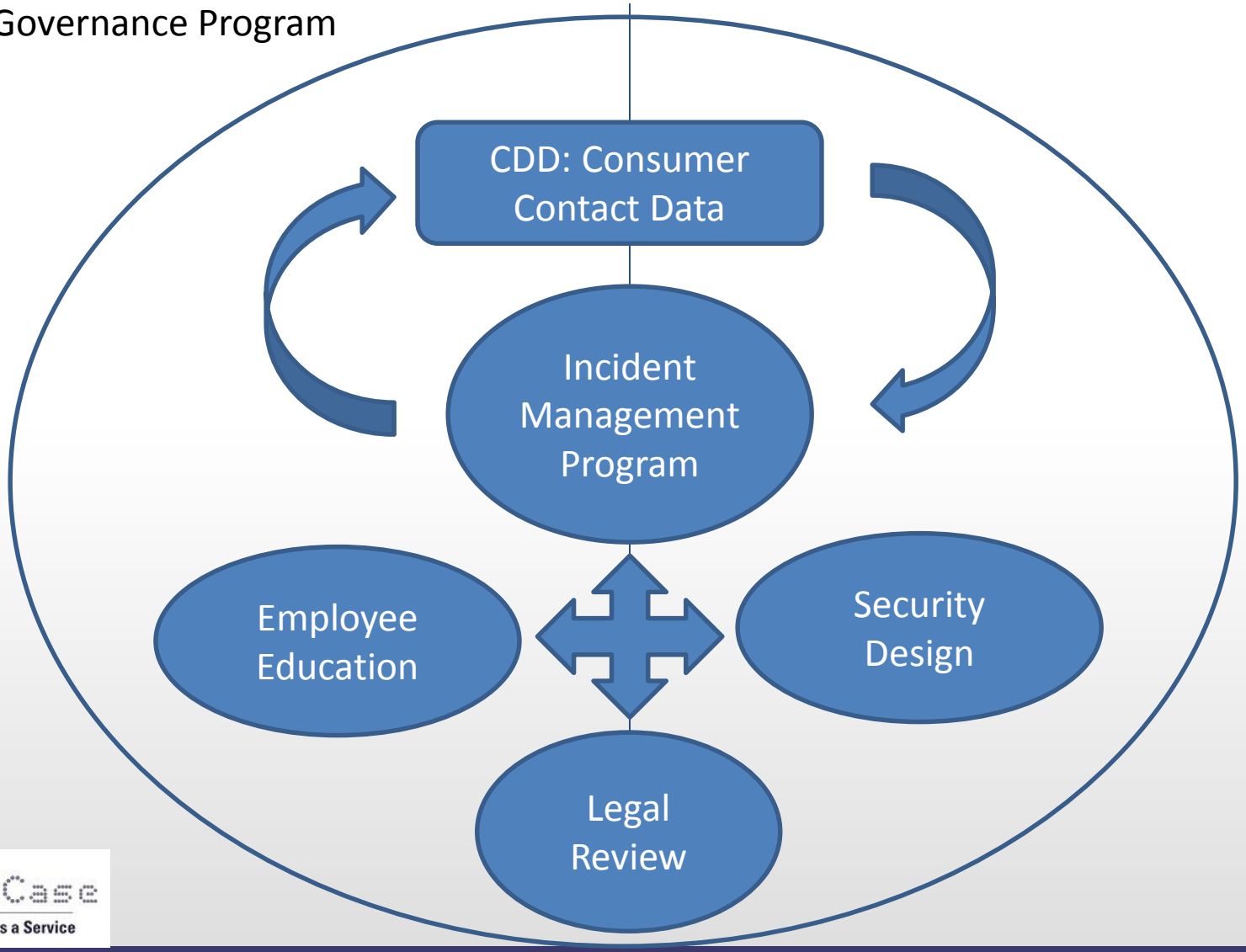
- More Mature

- 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

ControlCase
Compliance as a Service

Suggested Engine for Data Governance

Data Governance Program



ControlCase
Compliance as a Service

Thank You !

ControlCase
Compliance as a Service