



Architecting for Privacy in a Big Data Era

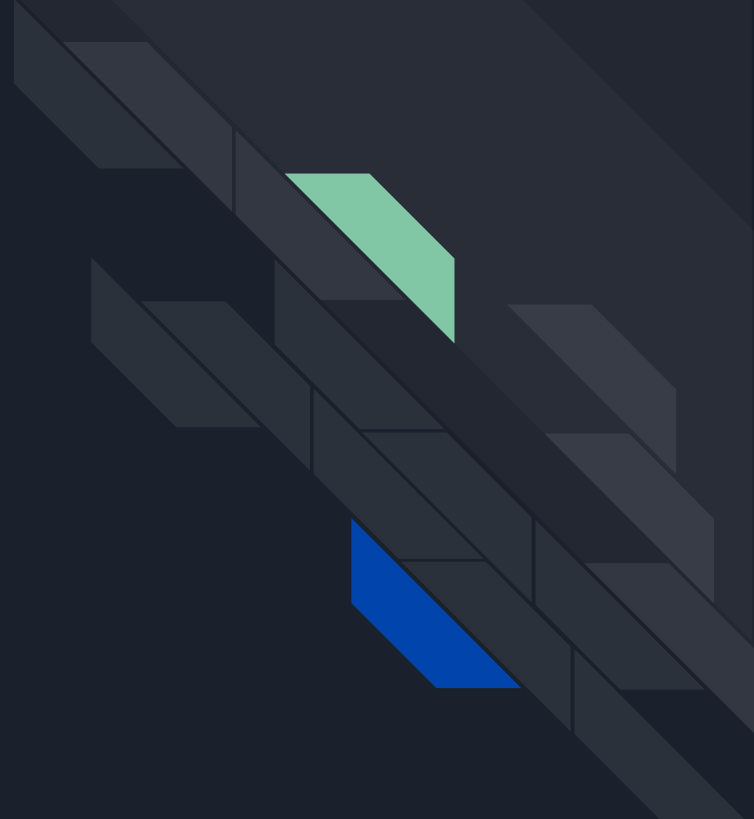
James H. (Jim) Morse, Jr., CISSP
Presented at Midwest Architecture
Community Collaboration 2018



Disclaimer

The content of this presentation is solely the opinion of the author and is not endorsed or to be construed as the position any employer, past, present or future.

The Death of Privacy





Massive amounts of data collected

Who's collecting and how?

- Social Media
- Search Engines, E-mail, & Maps
- Credit Monitoring Sites
- Cellphones
- Public Wi-Fi
- Digital Home Assistants
- Toll Road Passes
- Parking Passes
- Transit Passes
- Health care Systems

Who's using this data?

- Marketers
- Intelligence Agencies
- Criminal Enterprises
- Lawyers



Advent of Big Data Analytics

- Helps to provide insights into customer behavior
- Recommendations for new products
- De-anonymization
- Used to target for criminal activity



Scourge of Data Breaches

Yahoo - 3 billion records

eBay - 145 million records

Equifax - 143 million records

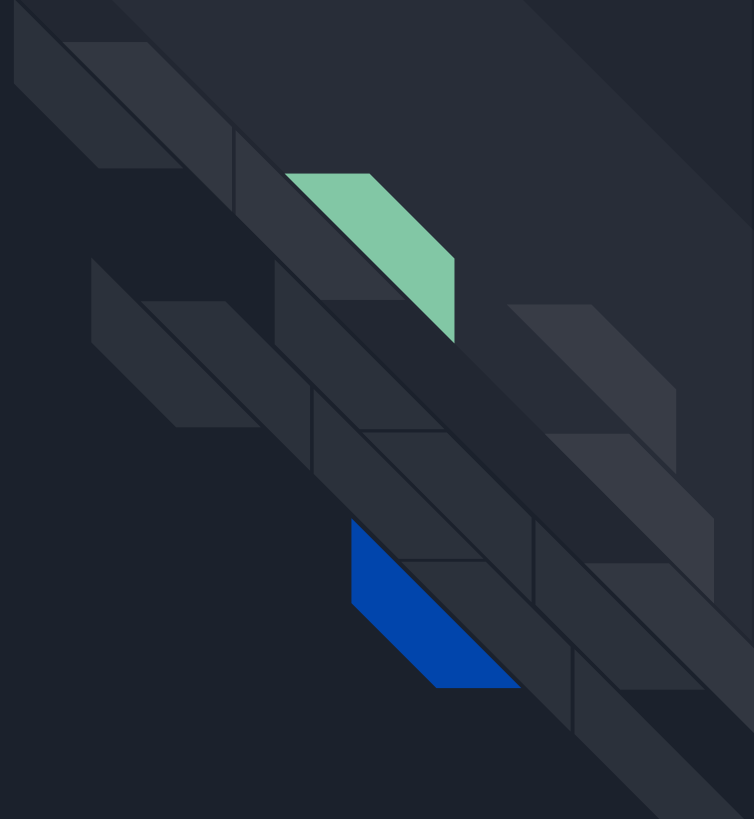
Heartland Payment Systems - 134 million records


Target - 110 million records

TJX Companies, Inc. - 94 million records

Uber - 57 million records

Where do we go from here?





It all begins with the architecture

All levels of the architecture must be considered and integrated

Business Architecture	<ul style="list-style-type: none">• Where privacy truly begins• Processes and risk management drive all other layers
Information Architecture	<ul style="list-style-type: none">• Drives security requirements• Where privacy is executed
Application Architecture	<ul style="list-style-type: none">• Secondary focus for security• Supports but doesn't guarantee privacy
Technology Architecture	<ul style="list-style-type: none">• Historically, the primary focus for security• Supports but doesn't guarantee privacy



Business Architecture

What decisions does the business need to make?

How do we communicate with our customers?

What are the risks to compromised privacy?

- HIPPA
- PCI
- Reputation
- Lost Sales

What processes and resources are needed to protect the business?



Information Architecture

What data is truly needed to support the business? How do we collect it?

How do we store it? What are the encryption standards?

How do we regulate access? What does improper access look like?

How do we keep it up to date? Do customers get to see it? Request to be forgotten?

Destruction! How and when do we destroy data that is no longer needed?



Application Architecture

Authentication, Authorization, & Accounting

- Traditionally relied on IT Dept
- IT Dept can't make the call on authorization

Enforcing good behavior

- Developers must know what proper access looks like
- Logging can't just be at the system level - must be at the application level as well



Technology Architecture

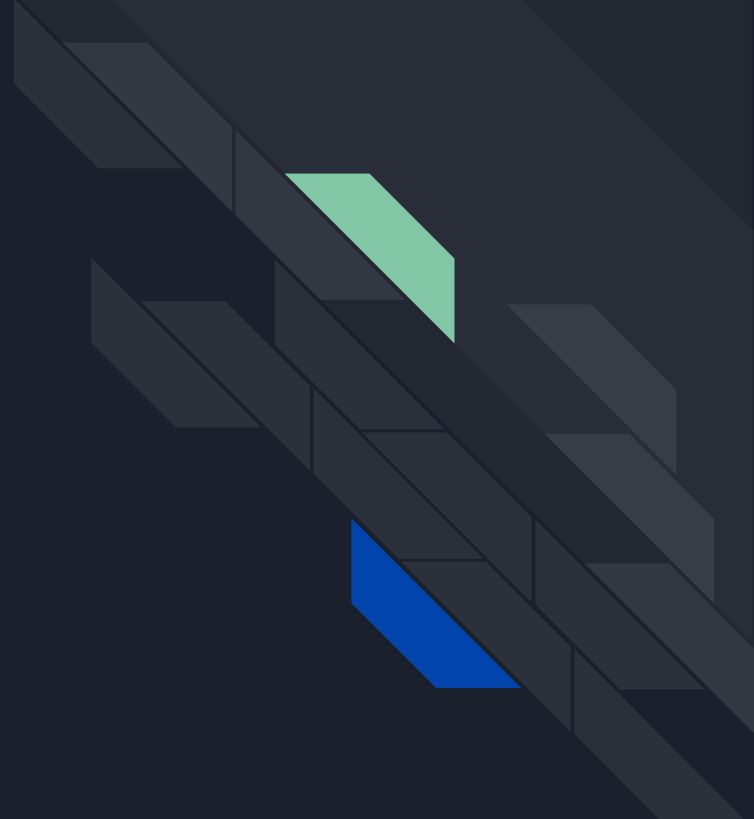
The one constant is new vulnerabilities

Must assume that compromises will occur

- Detection is key
- Mitigation should be as automatic as possible
- Post-incident activities should be planned and rehearsed

Summary

- We can't stop at just technology
- We can't just chase vulnerabilities
- We must consider the whole data lifecycle
- Each of the architecture layers must interlock to close the seams & gaps



Questions?

