womblebonddickinson.com

WOMBLE BOND DICKINSON

Data: Legal Landmines

Ted Claypoole

Womble Bond Dickinson

Date

Three eras for utility data: Technology Drivers

Pre-Digital:

- Paper records and rudimentary digital
- Analytical tools lacking
- Poor granularity
- Communication by postal service
- Little commercial value

Early-Digital:

- Digitized data
- Analytical tools emerging
- Limited real time granularity
- Real-time communication based phone service
- Emerging commercial value

AMI:

- Granular data
- Powerful analytical tools
- Full granularity
- Internet and wireless communication
- High commercial value

US Regulatory Restrictions on Data

Categories of Data:

- Personal Financial (ID, Trans.)
- Personal Healthcare (ID, Trans.)
- Children's Data (Primarily ID)
- Social Security Numbers (ID)
- Video Rentals (Trans.)

US Regulatory Restrictions on Data

Data Treatment:

- Retention
- Notice Requirements
- Destruction
- Protection

Data Privacy Requirements

“Do not give it away on purpose” (willful)

Data Security Requirements

“Do not give it away accidentally” (negligent, reckless)

Data Security Standards

- Reasonableness for current technology and sophistication of organization
- Include policy, procedure, training, technology
- Non apply to us all
  - (Does your company have employees, customers or benefits?)

In-House Counsel Role

“Keep the things that need kept”

“Destroy the things that need destroyed”

In-House Counsel Role

Legitimate Business Reason to Keep Data (regulation and litigation included)

Otherwise, be liberal in destroying data that has no justification for retention (Colorado law)

Data Breach Law

PREPARE	• Regulatory compliance • Breach response planning • Cybersecurity insurance	• Corporate due diligence • Vendor relationships • International compliance
RESPOND	• Investigate incident • Preserve privileges • Assess scope and harm	• Minimize legal risk • Breach notification laws • Law enforcement outreach
DEFEND	• Consumer class actions • Regulatory enforcement • State attorney actions	• Law enforcement requests • Internal investigations • Litigation with third parties

Keys to Preparing

- Conduct periodic risk and threat assessments, and stay current with best practices.
- Develop and test your incident response plan.
- Store sensitive data in encrypted form and maintain offline backup copies of critical files.
- Enforce basic cybersecurity hygiene, deploy technological measures, and “design for security.”
- Requirements under HIPAA, GLBA, PCI, GDPR, etc.

Keys to Responding

- Conduct incident response at the direction of counsel to preserve privileges and navigate legal risk.
- Contain and remediate the breach, usually with outside help from a data security firm.
- Fully investigate the attack, prevent reinfection, and engage law enforcement as appropriate.
- Ensure that key stakeholders stay informed, including corporate executives and boards of directors.
- Determine extent of harm to data subjects, consumers, and third parties, and take steps to minimize legal risk.
- Comply with applicable breach notification laws.

Forensic use

Relevancy:

- Evidence of alibi and occupancy
- Evidence of residency
- Evidence of misdeeds (divorce, child or elder neglect)

Fourth Amend. Standard:

- Reasonable expectation of privacy

Third Party Doctrine:

- United States v. Miller, 385 U.S. 293 (1966) (no expectation of privacy to third party business records)
- But Kyllo v. United States, 522 U.S. 27 (2001) (serious concerns where intimate details concerning personal activities in the home are involved)

IoT – How Serious Is This?

GAO Report, July 2017

Estimated 25 – 50 Billion Devices by 2025

Family of Four had 10 Connected Devices Last Year

Estimated to grow to 50 Devices by 2022

Business – Industrial Control Systems

What Data Concerns Us?

- Provided data – consciously given
- Observed data – e.g. CCTV, cookies, facial recognition
- Derived data – e.g. calculating customer profitability from the ratio of visits/purchases
- Inferred data – e.g. predicting future health outcomes

Who Regulates IoT in U.S.?

FTC
FCC
FAA
HHS
FDA
NTA

Tidal Wave Coming

EU – GDPR demonstrated how data can be regulated

Canada, Brazil, Mexico, Israel, Japan also providing more rights in data to consumers

CCPA – California sets likely precedent for US

State Privacy Codes

The California Consumer Privacy Act:

- https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

General State by State Listing:

- https://statedatauselaw.com/

Privacy Considerations

- **Consent to collect data**
  - Opt in (NH); opt out (CO); opt out with fee (CA)
  - Consent to specific uses for data
  - Timeliness of consent
  - Withdrawal of consent
- **Consent to share with third parties**
  - Enforcement of restrictions
  - Third party systems (VT, WI)
- **Who pays for data collection costs when data is used by third parties?**

Consumer Rights Under CCPA

- **Right to know**, at or prior to collection, the purpose of collection and the categories of personal information collected
- **Right to request** certain additional information, **including access** to specific pieces of personal information collected
- **Right to request deletion** of their personal information in certain instances and subject to several exceptions
- **Right to know** whether their personal information is sold or disclosed and to whom
- **Right to say no** to the sale of personal information
- **Right to equal service and price**, even if they exercise their privacy rights

You Must Disclose Upon Consumer Access Request

1. The categories of personal information you collected about that consumer.
2. The categories of sources from which the personal information is collected.
3. The business or commercial purpose for collecting or selling personal information.
4. The categories of third parties with whom you share personal information.
5. The specific pieces of personal information you collected about that consumer.

Privacy Considerations

- **Customer/third party access to data**
  - Green Button --DENC
  - Web and app based --Duke
- **Aggregation/anonymization**
- **Release to**
  - Researchers,
  - Municipal authorities
  - Landlords (15/15).
- **Customer's right to correct/eliminate data**

WOMBLE
BOND
DICKINSON

"Womble Bond Dickinson," the "law firm" or the "firm" refers to the network of member firms of Womble Bond Dickinson (International) Limited, consisting of Womble Bond Dickinson (UK) LLP and Womble Bond Dickinson (US) LLP. Each of Womble Bond Dickinson (UK) LLP and Womble Bond Dickinson (US) LLP is a separate legal entity operating as an independent law firm. Womble Bond Dickinson (International) Limited does not practice law. Please see www.wombleborddickinson.com/us/legal-notices for further details.

Information contained in this document is intended to provide general information about significant legal developments and should not be construed as legal advice on any specific facts and circumstances, nor should they be construed as advertisements for legal services.

©2019 Womble Bond Dickinson (US) LLP

UNICO
Where Connections Make a Difference.

NETWORK SECURITY AND PRIVACY LIABILITY

CHRIS DANIELSON- RISK ADVISOR

RT RYAN TURNER SPECIALTY

NETWORK SECURITY AND PRIVACY LIABILITY – BASICS AND ITS IMPORTANCE

- Designed to Cover Data Breaches, Hacks, Interruption of Business Operations
- Third Party and First Party Exposure
- You Have a Computer System with Any Customer Data – You Have an Exposure

UNICO
Where Connections Make a Difference

HOW IS CYBER UNDERWRITTEN?

- Industry Class / Nature of Operations
- Revenues and/or Personal identifiable records
- Encryption and Controls
- Officers in Place to Handle Risk Management Services
- Incident Response Plan / Disaster Recovery Plan
- Compliance with Regulations/Laws

RT RYAN TURNER SPECIALTY

UNICO
Where Connections Make a Difference

THIRD PARTY CYBER COVERAGES

- Data Breaches – Unauthorized Access/Use of Computer Systems
- Privacy Regulation Violations
- Denial of Service Attack/Malicious Code
- PCI-DSS Fines
- Media Liability

RT RYAN TURNER SPECIALTY

UNICO
Where Connections Make a Difference

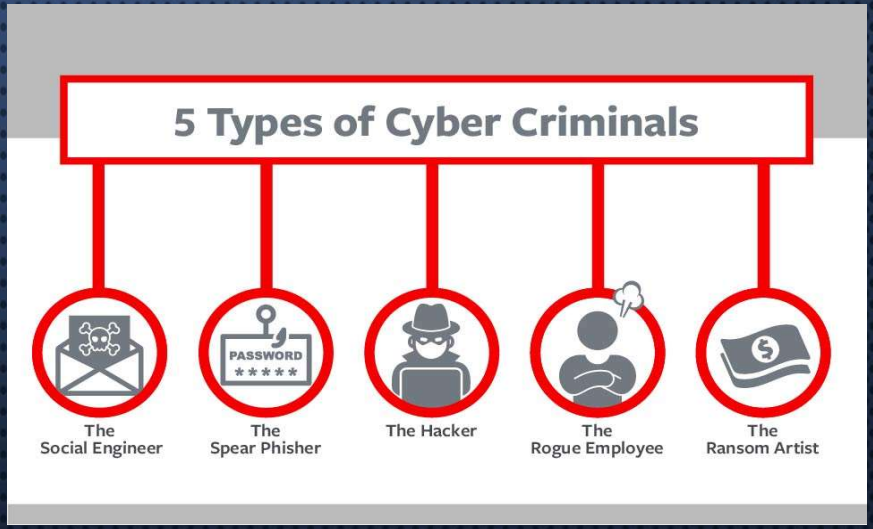
FIRST PARTY CYBER COVERAGES

- Business Interruption – Your Computer Systems and Cloud Computer Systems
- System Failure
- Data Recovery/Loss of Digital Assets
- Cyber Extortion – Ransomware
- Reputational Harm
- Theft of Minutes- Toll Fraud
- Social Engineering- Fraudulent Identity

RT RYAN TURNER SPECIALTY

SOCIAL ENGINEERING / CYBER CRIME

- PHISHING SCAMS
- EMPLOYEES BEING "DUPED"
- TELECOMMUNICATIONS FRAUD
- PROPER CONTROLS NEEDED



UNICO
Where Connections Make a Difference

10 EXCLUSIONS TO ASK YOUR AGENT ABOUT

1. Acts committed by Former Employees
2. Disputes Between 2 Insureds Under the Policy (Insured vs Insured)
3. Intentional Loss caused by employees, officers, directors or contractors
4. Fraudulent Acts
5. Some Fines & Penalties
6. Intentional Failures To Report A Breach Or Cyber Incident
7. Contractual Liability as required by Law (per contract provisions)
8. Infringement Of Trade Secret or Patent
9. Failure to maintain appropriate network security standard
10. Bodily injury & property damage

RT RYAN TURNER SPECIALTY

CONCLUSION AND QUESTIONS

CHRIS DANIELSON
UNITEL INSURANCE
651-216-5757 CDANIELSON@UNITELINSURANCE.COM