Data Stewardship and Data Breach: What to do and what’s at risk?

June 14, 2016

Association of Corporate Counsel
HOUSTON
Agenda

- Types of data
- Rights to data
- Data breach defined and how to address breach
  - Both U.S. and Canadian perspectives
- Recommendations and Best Practices
Types of Data

- Financial data
- Technical data
- Corporate data
- Personnel data
- Data from wearable devices
- Health care data
  - Individual patient data
  - Collective patient data
- Enterprise metadata
- Analyzed data
Who owns data?

- Fragmented nature of data collection and analysis causes lots of gray areas with respect to data ownership

- Data in General
  - If you generate data completely based on your activities, without restriction, then you own it
  - If your work is subject to any agreements, there may be shared ownership, restricted ownership, or no ownership

- Better Question - Who has what rights to access, modify, and share data?
Potential Intellectual Property for Data

• Copyright
  • Database structure
  • Database content rights in EU

• Trade Secrets
  • State Laws
  • Defend Trade Secrets Act of 2016

• Patents
  • Patent eligibility for what you do with your data
    • Recent case law and patent guidelines do not provide clear path
Ways to Monetize Data

• Monetization = data $ product/service

• Internal Use - connect the dots, decreasing waste, benchmark performance, identify risks, forecast trends

• Collaborative Use - make recommendations of products or services, improve delivery of products or services

• Transactional Use – direct sale or exchange for value

• Where is the value?
  - Aggregated or integrated data
  - Data analytics - descriptive or exploratory
  - Predictive models
  - Prescriptive models
Data Stewardship

• Obligations associated with agreements
  • Are you subjected to agreements that convey obligations (e.g. Obligations to maintain, secure, etc.)
• Obligations associated with trade secrets
• Obligations associated with financial data
• Obligations associated with personal data (e.g. SS# and health data)
U.S. - Predominantly Determined by State Laws

- 47 states, D.C., & U.S. territories
- Definitions differ for what constitutes “personal information”
- Some laws require notification of residents based upon “unauthorized access”
- Some require a risk of harm analysis to determine whether notification is required
- Many states require notice to the State Attorney General or specific agency
- Notice within a defined timeframe, but these timeframes can vary
- Limited precedent
What is a Data Breach in general in the U.S.? (That may trigger state notification laws)

• Unauthorized access to and acquisition of specific types of information associated with a named individual
  • SSN
  • Driver's license number
  • Credit card number
  • Bank account Information
• information that identifies an individual and relates to:
  (i) the physical or mental health or condition of the individual;
  (ii) the provision of health care to the individual; or
  (iii) payment for the provision of health care to the individual.
What is Breach in Texas?


“Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."
Epic Systems Corp. v. Tata Consultancy Services Ltd.

• Tata accessed Epic's web portal without authorization while servicing a mutual client, and then used information obtained to develop a competitive software product and other improper purposes

• Epic sued Tata on numerous grounds
  • Breach of contract
  • Wisconsin Computer Crimes Act
  • Computer Fraud and Abuse Act
  • Trade Secret violation

• Jury awarded $940M
• Court entered an injunction
PF Changs

- PF Changs' computer system was breached and credit card data was stolen
  - Notified consumers and encouraged them to monitor accounts
- Several consumers sued; district court found no Article III standing
- 7th Circuit reversed district court and found that that PF Changs diners had standing to sue
  - One diner had suffered no fraudulent activity on card, but had spent time monitoring account, replacing card, etc.
  - One diner had 4 fraudulent charges that were reimbursed by the bank
- 7th circuit noted both had spent time mitigating risks and resolving issues with potential breach
Spokeo, Inc. v. Robins

- Robins sued Spokeo alleging that his online profile was inaccurate and in violation of the Fair Credit Reporting Act
- District Court found that Robins failed to plead injury in fact and thus lacked Article III standing
  - Case dismissed
- Ninth Circuit reversed, finding that Robins had adequately alleged injury in fact based on his statutory rights and his personal interests in proper handling of his credit information
- Supreme Court found 9th Circuit's analysis was incomplete for failure to consider both aspects of the injury-in-fact requirement
  - injury-in-fact requirement requires a "protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"
  - 9th Circuit failed to address "concreteness"
Compliance is Complex

- PCI-DSS
- HIPAA HITECH
- INDUSTRY SELF REGULATION
- STATE PRIVACY LAWS
- INTERNATIONAL DATA PROTECTION
- FERPA
- STATE BREACH NOTIFICATION LAWS
- FTC
- GLBA
- FTC
- FDA
Canadian Privacy Law

- Provincial Privacy Legislation:
  - **Private:** *Personal Information Protection Act* ("PIPA") (Alberta, British Columbia & Quebec)
  - **Health:** *Health Information Act*
  - **Public:** *Freedom of Information & Protection of Privacy Act*

- Federal Privacy Legislation:
  - **Private:** *Personal Information Protection & Electronic Documents Act*
  - **Public:** *Privacy Act*
Canadian Privacy Law – Key Principles

- Privacy law prohibits collection, use & disclosure of personal information absent consent (subject to exceptions)
- Subject to reasonableness standard (what reasonable person would consider appropriate in circumstances)
- Consent
  - Concept of consent is central to privacy law
  - Consent required for collection, use or disclosure of personal information (unless legislated exception)
Across Borders – Jurisdictional Conflict

- Flow of information more frequently occurring across provincial & international borders
- Conflicts may arise between privacy legislation & regulatory requirements in different jurisdictions
- Where company operates in multiple jurisdictions, best practice is to adhere to highest standard
Alberta PIPA – Highest Standard

- AB PIPA most restrictive legislation in Canada
- Some features to note in AB PIPA include:
  - Requirement that organizations provide notification to individuals regarding use of foreign service providers (s. 13.1)
  - Mandatory breach notification (s. 34.1)
AB PIPA – Notice of Foreign Service Provider

• Use of service provider outside Canada to collect, use, disclose or store personal information for organization requires notification (orally or in writing)
• “Service Provider” defined broadly & includes subsidiary or affiliate
• Trigger is transfer of personal information to service provider across borders, where organization requires consent from individual to collect personal information
Section 6 – Organizations must develop policies & practices with regards to foreign service providers

Organizations required to provide information regarding:
- Countries outside Canada where collection, use & disclosure or storage of personal information is occurring or may occur
- Purpose for which service provider authorized to collect, use or disclose personal information on behalf of company

New provisions due to concerns with personal information crossing borders
An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.
Alberta PIPA – Mandatory Breach Notification

• Significant Harm:
  • Bodily harm
  • Humiliation/damage to reputation/relationships
  • Loss of employment, business or professional opportunities
  • Financial loss or identity theft
  • Damage to or loss of property
  • Breach of contractual obligations
  • Failure to meet professional standards
Alberta PIPA – Mandatory Breach Notification

• Types of Breaches:
  • Stolen or lost laptops & memory sticks
  • Break & enters (stolen computer equipment, files etc.)
  • Email/fax/letter mail transmission errors
  • Errors in record disposal
  • IT system issues
  • Network attacks/viruses etc.
  • Human error
Avid Life Media – Decision #P2015-ND-49

• Avid Life Media responsible for adult websites “Ashley Madison” & “Established Men”

• Employees noticed unusual activity on company’s information systems – following day, messages appeared on employee computer screens

• Anonymous messages threatened to release customer records, employee documents & email communications unless company shut down websites

• A week later Avid Life confirmed personal information obtained by hackers

• Incident affected approximately 37 million individuals, including 2.4 million Canadians

• Information exposed included full name, address, height, weight, sex, email address, username & password for paying users
Avid Life (con’t)

• Avid Life took steps to contain breach, including notifying law enforcement
• Commissioner determined because nature of website, disclosure of personal information could result in hurt, humiliation & damage to reputation - harm significant
• Commissioner also determined “real” risk of harm because hacker’s technical expertise & malicious intent
• Commissioner required that affected Albertans be immediately notified of breach
• Vehicle of HR employee burglarized in U.S. & company laptop stolen
• Laptop contained personal information of over 5000 employees including: names, dates of birth, addresses, SINs, bank account information, phone numbers & email addresses
• Laptop password protected but no encryption
• Law enforcement notified
• Commissioner found significant harm: could be used for identify theft, fraud & phishing
• Commissioner also found real risk: malicious intent because computer stolen
Heart & Stroke Foundation – Decision #P2016-ND-13

- Organization discovered names & email addresses inadvertently stored on unsecure server by service provider
- No evidence information accessed by unauthorized individuals
- 918 individuals affected
- Commissioner found real risk of significant harm as could be used for social engineering attacks such as targeted phishing or spam emails
Hackers gained access to decommissioned version of website which contained email addresses, passwords & dates of registration

33,000 individuals affected but unable to tell how many Albertans

Organization was of view not sensitive information & no evidence of unauthorized use

Commissioner found harm because could gain access to accounts & could result in phishing or fraud

Commissioner also found real risk because stolen by hackers indicating malicious intent
• Employee discussed wages & severance amounts paid to certain employees with other employees
• Commissioner found involved significant harm as information could be used to hurt, humiliate, embarrass & damage relationships
• Commissioner also found likelihood of harm increased due to close relationships between co-workers & possible malicious motive behind disclosure
Plan for Breach

• Identify the types of data your company collects/ processes/ develops
• Identify persons who are/will be responsible for data management
• Create a risk assessment plan and mitigation plan
• Develop policies and educate all staff
• Have a reporting mechanism that is well publicized and encouraged
• Procure insurance to cover data breaches (cyber policy)
• Review vendor contracts
• Identify compliance requirements according to applicable laws, taking into consideration all regions of concern
Plan for Breach – Cross-Border Considerations

• Special legislation applies when contracting with certain provincial governments or municipalities
• If Canadian corporate affiliate transfers data to U.S., Canadian company will remain responsible for integrity of data
• Personal data of U.S. data subjects stored in Canada will be subject to Canadian data protection legislation
Plan for Breach – Cross-Border Considerations

• When transferring personal information cross-border between Canada & U.S.:
  • Want to be satisfied that U.S. party has policies & processes in place, including training & effective security measures, to ensure data in its care is properly safeguarded in accordance with Canadian law
  • Set out requirements for safeguards in written contract
  • Retain right to audit & inspect company & practices
  • Make it clear to individuals that information may be processed in foreign country & may be accessible to law enforcement & national security authorities
  • Ideally, will provide notice at time information is collected
  • Set out breach notification procedures in case of data breach
  • Include indemnification provisions in written contract
Agreements with Employees

- Background checks
- Security credentials – assign, monitor, revoke
- Intellectual property – beyond patents
- Simple assignment language is insufficient
When Breach Occurs

Involve in-house/outside counsel immediately
- Can assert privilege to maximum extent possible
- Use counsel to conduct employee interviews
- Assess claims vs. affected entities
- Initiate Notification Protocol
- Notify vendors, insurance, regulators, law enforcement officials

Investigate
- What data? Whose data?
- Who are the affected parties?
- Is the issue more than just data (e.g., trade secret theft)?
- Preserve forensic records

Mitigate/Remediate
- Recover device / data
- Establish that breach was limited or data not accessed
- Take steps to protect reputation
• STEP 1: Contain Breach
  • Take immediate, common sense actions to limit breach
    • Stopping breach, recovering records, shutting down system, revoking access or correcting weaknesses in physical security
    • Contact person responsible for security organization
    • Notify police if breach involves theft or other criminal activity
Alberta PIPA – Mandatory Breach Notification - Response

• STEP 2: Evaluate Risks Associated with Breach
  • Personal or health information
    • Health information, social insurance numbers, financial information
  • Cause & extent of breach
    • Risks of continued exposure, accessibility of information
  • Individuals affected by breach
    • Number of people or organizations affected
  • Foreseeable harm from breach
    • Relationship between unauthorized recipients & data subject, severity & type of harm that could result to subject or public
• **STEP 3: Notification**
  - Notification can mitigate situation
    - Legislation & Contract obligations
    - Risk of identity theft & fraud
    - Risk of physical harm, hurt, humiliation or damage to reputation
    - Risk of loss of business or employment opportunities
  - Notify subject of breach
    - As soon as possible by phone, letter or in person
    - Should include date, time, circumstances & information of breach, contact information & description of steps taken to reduce harm
  - Police, insurers, regulators, credit card companies & Privacy Commissioner
STEP 4: Prevention

- Mitigate risks associated with cause of breach
- Potentially security audit of physical & technical security
- Training for staff regarding security procedures
Before Breach Happens

• Make sure your Terms of Use & Privacy Policy is up-to-date
  • Explain how data will be used

• Obtain lawful prior consent for use and monitoring
  • through warnings or banners
  • terms of use

• Notify users
  • use of the system constitutes consent to interception of communications and
  • results of monitoring may be disclosed to others, including law enforcement.

• If an organization is a federal, state, or local agency or a state university, its actions may implicate the Fourth Amendment
  • inform users of diminished expectation of privacy
Challenges

- No clear legal and regulatory framework within the U.S. or globally
- Lack of uniform data protection, privacy, and security standards
- Lack of interoperability and interoperability standards
- Inadequate funding or reimbursement models
- Cultural resistance
- Trust concerns on a global scale
Dentons global platform

Legend
Locations in grey reflect combinations that have been approved but are not yet effective.
Questions?

Heather Khassian
Houston
1 713 658 4626
Heather.khassian@dentons.com

April Kosten
Calgary
1 403 268 3108
April.kosten@dentons.com
Thank you

Dentons US LLP
LyondellBasell Tower
1221 McKinney Street, Suite 1900
Houston, TX 77010
United States

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways. Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries. www.dentons.com.