The Year of Privacy

Stas Bodrov | sbodrov@sbalawyers.ca | @bodroffff1
PURPOSE OF CYBERSECURITY

- Propriety information
- Business operation
- Explicit crime
- Assets
- Data – privacy
AGENDA

- Privacy laws and regulations in Europe, Canada, and the US
- Canadian courts and privacy torts
- Class actions in Canada
- Where to next?
European Convention on Human Rights – 1953
  - Article 8
  - Zakharov v Russia (2015)


General Data Protection Regulation (GDPR) – 2018
  - One unified law
  - Replaced the Data Protection Directive
Extraterritorial application
- Data controller
- Data processor
- Data subject

Does not apply to purely personal or household activities – only professional / commercial activities

Personal data
GDPR – RIGHTS OF A DATA SUBJECT

- Transparency and Communication
- Right of Access
- Accuracy
- Erasure
- Restricting Processing
- Right to Object
GDPR – CONTROLLERS AND PROCESSORS

- GDPR Implementation
- Demonstrated Compliance
- Controller and Processor Contract
- “Appropriate” Security Measures
- Breach Notification
  - Supervisory Authority – without undue delay and, where feasible, not later than 72 hours
  - Data Subject – high risk to the rights and freedoms of a natural person
GDPR – FAILURE TO COMPLY

- Regulatory Sanctions
  - Access and Audit Rights
  - Administrative Orders
  - Fines – 4% or 20 Million Euro

- Data Subjects Action
  - Material or Immaterial
GOOGLE V CNIL

- 2014 – Google v Spain – Google order to delist personal information
- 2016 – CNIL fines Google 100,000 Euros for failing to delist
- Google appeals to the ECJ
- September 2019 – ECJ finds that the scope of de-listing is limited to the EU states
- Google does not have to de-list globally
CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

- June 28, 2018
- Doing business in California
  - > $25 Million annual revenue
  - Information of > 50,000 consumers/devices
  - > 50% of revenue from selling personal information
- Data controllers – contracts!
CCPA – PERSONAL INFORMATION

- Personal information
  - Identifies
  - Relates to
  - Describes
  - Is capable of being associated with
  - Could reasonably be linked, directly or indirectly
  - Particular consumer or household
  - Inferences drawn from any of the information identified
CCPA – USE OF PERSONAL DATA

- Control over personal data
- Consumer rights
  - Access and deletion of personal data
  - Know what has been collected
  - Know what information has been shared
  - Opt out of sale of personal data
  - Cannot discriminate
CCPA – BREACHES

- There is no explicit breach notification rules in the CCPA
- Any consumer’s
  - Nonencrypted or nonredacted
  - Unauthorized access AND exfiltration, theft, or disclosure
  - Implement and maintain reasonable security procedures and practices
  - Appropriate to the nature of the information
- CIS Critical Security Controls
$100 to $750 per incident
Don’t need actual damages
10,000 users = at least $1,000,000 exposure
January 1 and July 1, 2020
PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

- Canadian data privacy law
- Private sector
- Three key words
  - Collect
  - Use
  - Disclose
- Extraterritorial application
PERSONAL INFORMATION

- Information about an identifiable individual
- Personal health information
  - Physical or mental health
  - Health services provided
  - Donation of body parts
  - Information collected in the course of providing health services
  - Information collected incidentally to the provision of health services
- Security safeguards that are appropriate to the sensitivity of the data
MANDATORY BREACH REQUIREMENT

- Digital Privacy Act
- Three pronged amendment in November 2018
  - Record keeping
  - Reporting
  - Notification
- Breach of a security safeguard
  - Loss of, unauthorized access to, unauthorized disclosure
- Real risk of significant harm
- As soon as feasible
OTHER PRIVACY REGULATIONS

- Sectoral – MUSH
- Privacy Act
- Freedom of Information and Protection of Privacy Act
- Municipal Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act, 2004
  - Has its own notification and reporting requirements
  - Collected, used, or disclosed without authorization
PIPEDA COMPLIANCE

- Private organization have to comply
- Fines
  - $100,000 fine per violation
  - Directors personally liable
- Risk management strategies
  - Understand the obligations and which act applies to you
  - Shift risk
  - Training, policies, and procedures
  - Insurance
  - Privilege – DO NOT HANDLE BREACHES IN-HOUSE
Tort – civil wrong doing

2012 – *Jones v Tsige*
- Intrusion upon seclusion
- No need to prove damages
- Up to $20,000 in damages
**SOCIAL ENGINEERING**

- *The Brick v Chubb*
  - 2010 – Brick’s accounts payable department
  - Over $338,000 was transferred
  - Claimed $224,475.14 under a fraud policy
  - Chubb denied coverage
  - The Courts agreed
  - The policy would cover direct loss resulting from funds transfer fraud by a third party
  - The Brick instructed the bank to transfer funds
SOCIAL ENGINEERING

- **Dentons Canada LLP v Trisura**
  - Dentons lawyer transferred $2.5 million
  - Recovered $785k, claimed $1.75 million
  - Trisure denied the claim
  - Separate social engineering policy

- **Take away**
  - Policies and procedures are important
  - Two-factor authentication
CLASS ACTION

- Collective group
- Suffered similar harm
- Fault is of the same party
- Certification
Unlawful access to patient record
Selling patient records
Not a reasonable cause of action
  - Intrusion – YES
  - Seclusion – NO
  - Not sensitive enough
Narrow parameters
KAPLAN V CASINO RAMA

- Anonymous hacker
- Refused ransom = posted online
- Not certified
  - IPC – not reasonable security measures
  - Casino liability
  - Sensitivity = level of protection
  - No commonality
- Good breach management
CLASS ACTION TAKE AWAY

- Scary
- Sensitivity of data
- Reasonable level of security
- Class actions are narrowed
- Breach management
FUTURE
VERY NEAR FUTURE

- PIPEDA Review
- More funding
- Cyber certification
- Political platforms
- More power over privacy
- Biometrics