RideShark
Unified Mobility

Data Privacy and Cybersecurity: What Transportation Professionals Need to Know

Katten

Presented By

Doron Goldstein & Max Jarvie

BLG
Borden Ladner Gervais

October 21, 2020

This presentation is a general discussion for informational purposes only, and may not be relied upon as legal advice.

Agenda

- The Global Scene: Financial Risks and the Evolving Privacy Landscape
- Privacy Principles
- Key Considerations
  - "Personal Information"
  - Consent
  - Privacy by design
  - Security
  - Service Provider Management
- Best Practices

Source: *United Nations Global Pulse*, "Data Privacy"

The Global Scene:

Financial Risks and the Evolving Privacy Landscape

Recent trends in financial risk: Fines and penalties

Global NEWS

CANADA November 1, 2018 12:28 pm

Failure to report Canadian privacy breaches could mean big fines after Nov. 1

By Staff The Canadian Press

REUTERS

BUSINESS NEWS OCTOBER 16, 2020 / 5:42 AM / UPDATED 3 DAYS AGO

British Airways hit with UK data watchdog's biggest-ever fine

By Muvija M 3 MIN READ

(Reuters) - Britain's data protection watchdog said on Friday it has fined British Airways 20 million pounds - its biggest such penalty to date - for failing to protect data that left more than 400,000 of its customers' details the subject of a 2018 cyber attack.

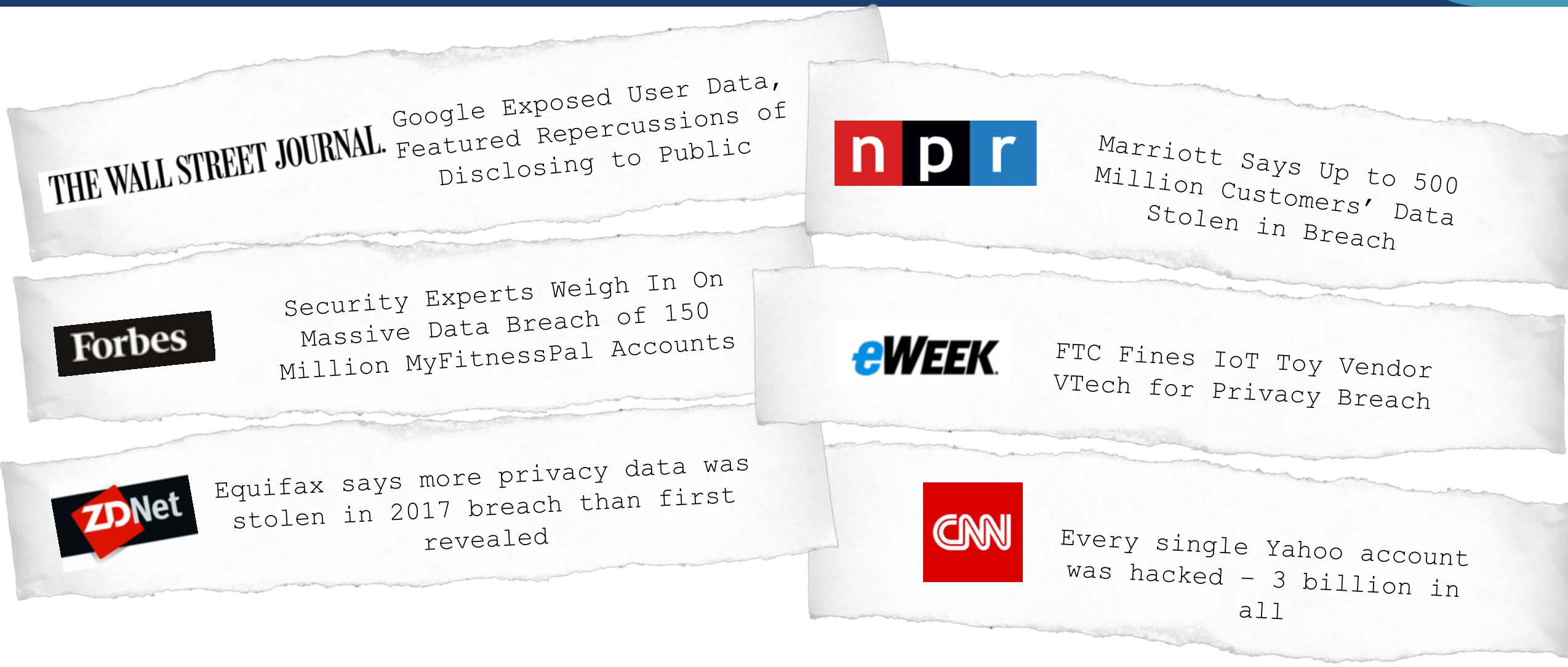
The Washington Post
Democracy Dies in Darkness

Europe

French watchdog slaps Google with $57M fine under new EU law

By Associated Press
January 21, 2019 at 12:27 PM

Recent trends in financial risk: Losses from data breach



Recent trends in financial risk: Losses from data breach

- **Business losses to cybercrime data breaches will rise from US$3 trillion each year to over US$5 trillion in 2024, an average annual growth of 11% (**Juniper Research's *The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024* report)

- The increase in losses to cybercrime will primarily be driven by increasing fines for data breaches as regulation tightens, as well as a greater proportion of business lost as enterprises become more dependent on the digital realm

Recent trends in financial risk:
Loss of market value from reported breaches

Katten BLG

Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap

By Victor Reklaitis
Published: Sept 14, 2017 6:25 a.m. ET

THE VERGE

Facebook stock tanks after data breach report, shaving billions off company's market value

By Shannon Liao | @Shannon_Liao | Mar 19, 2018, 2:58pm EDT

comparitech

Analysis: How data breaches affect stock market share prices (2018 update)

PAUL BISCHOFF - TECH JOURNALIST, PRIVACY ADVOCATE AND VPN EXPERT
@pabischoff September 6, 2018

Recent trends in financial risk: Not just data breaches

MediaPost News Events Awards Members More

EmailMarketingDAILY

AROUND THE NET

German Authorities Mete Out A EUR14.5 Million GDPR Fine For Data Retention

Estate Agent Today, Monday, December 2, 2019 9:51 AM

German real estate firm Deutsche Wohnen has been hit with a €14.5 million fine for retaining old customer data longer than necessary. UK real estate agents are being warned to heed GDPR rules on data retention.

Tuesday, 03 December 2019 14:58

A troubling new twist on privacy class action lawsuits in Canada

Written by Teresa Scassa

"This case is interesting because raises the possibility of class action lawsuits being used for privacy complaints other than data security breaches. This should put fear into the heart of any company whose general practices or policies have led them to collect too much personal information, obtain insufficient consent, or retain data for longer than necessary…"

Privacy laws are here…and increasing in number and scope

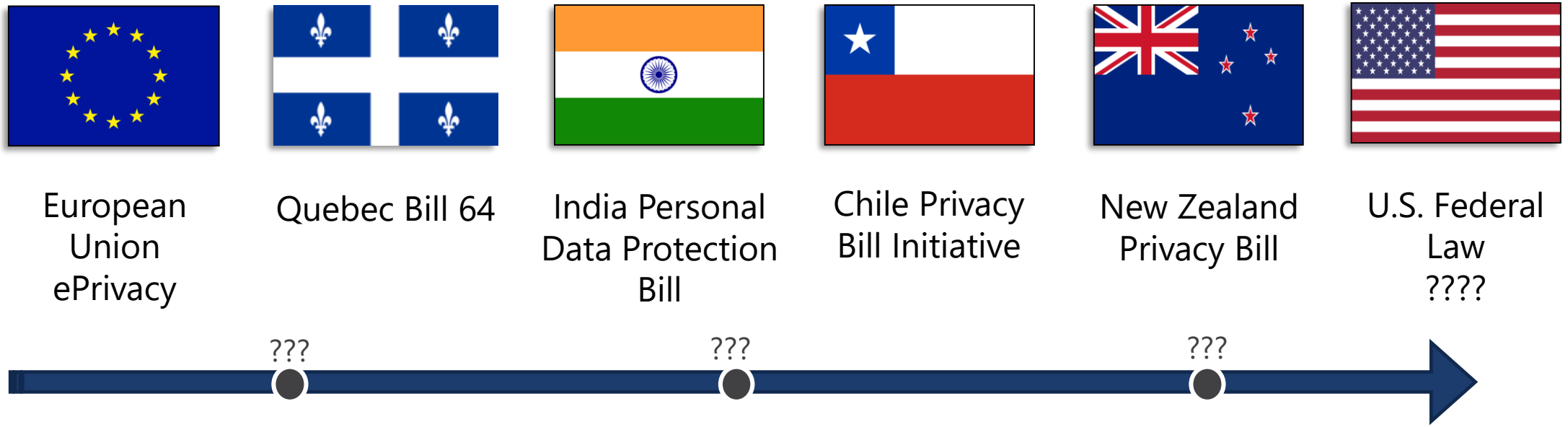
European Union GDPR:
May 2018

California Consumer Privacy Act
January 2020

Brazil LGPD
September 2020

2018 2019 2020

Other laws still being considered



Recent trends in data protection laws

Limited/Sectoral Protection → **Broad Protection**

What do these laws generally do?

- Give individuals specific rights
- Strengthen data protection standards/require legal basis for processing
- Increase and specify security requirements
- Implement and expand internal compliance requirements
- Limit transfers (to third parties/data localization)
- Have broader scope and often extraterritorial reach
- Create or expand reporting requirements on fast timelines
- Create significant penalties for non-compliance

Specific Individual Rights

- Transparency/Be Informed
- Access & Portability
- Rectification
- Erasure/Deletion/”Right to be Forgotten”
- Restriction of Processing
- Objection
- Opt-Out/Non-Discrimination – “Do Not Sell My Information”

** Generally must respond within 30 days (GDPR)/45 days (CCPA) of data subject request*

What are the general consequences for violation?

- Significant potential liability:
  - Regulatory enforcement:
    - *GDPR – Up to greater of €20million or 4% of global turnover*
    - *CCPA – Up to $7,500 per violation ("violation" could be per-person)*
    - *PIPEDA – Up to $100,000 for failure to report a security breach*
  - Private right of action (CCPA):
    - *Statutory damages (failure to have "reasonable" security) – $100-$750*
    - *"Small" data breach of 10,000, in addition to the other costs, now has an additional $1 million - $7.5 million; a data breach of 100,000 would be $10 million - $75 million.*

What's next, and why

If they haven't yet, laws are likely to change soon

- Driving the trend: European Union (GDPR)
- EU Adequacy decisions
  - Exports of personal data from EU to third countries permitted only where the recipient jurisdiction has received an adequacy decision from the EU or the exporter can ensure that personal data will be protected
  - Adequacy reviews now being taking into account a broader context that extends beyond the scope of criteria used to determine original EU adequacy under previous EU privacy law (the 95 Directive)
  - Schrems II (July 2020) - SCCs alone not adequate - may put pressure on smaller states to create legal frameworks that provide protections EU expects

The global landscape: Main takeaways

- Overall trend: broader protections and greater control for individuals
- More regulatory oversight of organizations – well-funded regulators with direct fining powers

- For organizations, it's not all doom and gloom
  - Following the general principles of privacy law will bring you almost to the finish line in every jurisdiction
  - Following the principles of privacy by design can put you ahead of the game

Privacy Principles

Privacy Principles

The OECD *Fair Information Principles*

- 1. Collection Limitation Principle.
- 2. Data Quality Principle.
- 3. Purpose Specification Principle.
- 4. Use Limitation Principle.
- 5. Security Safeguards Principle.
- 6. Openness Principle.
- 7. Individual Participation Principle.
- 8. Accountability Principle.

Key Considerations

Key considerations: Personal information

What is “Personal Information”?

- Direct identifiers (Name, address, birthdate, SIN…)
- Indirect identifiers (location, IP address, Google advertising ID, credit card number)
- Information “about” an individual (profiles, reports, opinions, evaluations, comments, disciplinary actions)
- New personal information your product generates during processing (profiles, predicted preferences)

Sensitive personal information:

- Any information can be considered be sensitive, depending on the context.
  - Financial information and health information are often considered sensitive.
  - Granular geolocation information can be potentially sensitive (particularly longitudinal collections of such information)
  - The more information you collect, the more likely it is to be sensitive in the aggregate.

Key considerations: Personal information

Bottom line:

- Know what you are collecting!
- Interpret “personal information” generously
- Think about what might be sensitive, particularly in the aggregate

Key considerations: Consent

- **Legal grounds for collection, use and disclosure vary from place to place…**
- **…but always include informed consent as a (or in some cases the) core requirement**

- **Example: the Office of the Privacy Commissioner of Canada's (OPC) new "Guidelines for obtaining meaningful consent":**
  - *"PIPEDA requires individuals to understand the nature, purpose and consequences of what they are consenting to. In order for consent to be considered valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner."*

Key considerations: Consent

Bottom line:

- Obtain *informed* or *meaningful* consent
- Emphasize key elements: what you are collecting, all the uses, parties to whom it may be disclosed, residual risks of harm that might occur even after mitigation measures taken
- Give “yes” or “no” choices with respect to purposes that are not “core” to the service.
- Provide information in manageable and easily accessible ways

Key considerations: Privacy by Design (PbD)

The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.

(Source: Designing Privacy-by-Design, Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen, APF 2012, LNCS 8319, pp. 55–72, 2014)

Key considerations: Privacy by Design

The Seven Principles

- **Proactive not reactive; preventive not remedial**
  - The privacy by design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, privacy by design comes before-the-fact, not after.
- **Privacy as the default**
  - Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.
- **Privacy embedded into design**
  - Privacy by design is embedded into the design and architecture of IT systems as well as business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system without diminishing functionality.
- **Full functionality – positive-sum, not zero-sum**
  - Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by design avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both.
- **End-to-end security – full lifecycle protection**
  - Privacy by design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures cradle-to-grave, secure lifecycle management of information, end-to-end.
- **Visibility and transparency – keep it open**
  - Privacy by design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
- **Respect for user privacy – keep it user-centric**
  - Above all, privacy by design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Key Considerations: Privacy by Design

Criticisms

- The principles are vague; leave open questions in relation to application to systems (see "Engineering Privacy by Design“ by Seda Gurses, Carmela Troncoso, and Claudia Diaz)

- the principles as written do not make it clear “what ‘privacy by design’ actually is and how it should be translated into engineering practice.

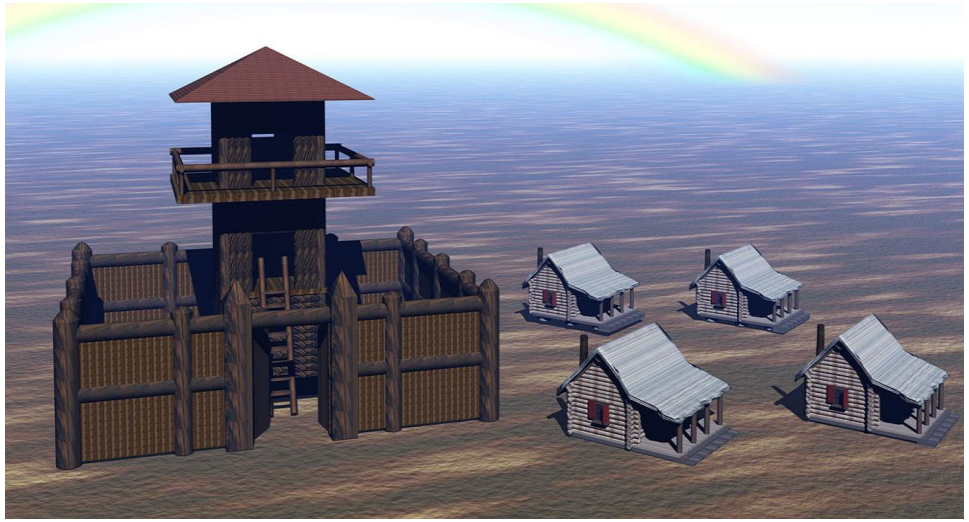
Key Considerations: Privacy by Design

Bottom line:

- Make a Privacy Impact Assessment an integral part of the design stage of any initiative.
- When designing the system, minimize the collection of data at the outset to only what is necessary.
- Where personal information that may potentially be collected is not ‘core’ (i.e., a condition of service), make not collecting it the default.
- Pay particular attention to function creep
- Create technological, policy and procedural barriers to data linkages with personally identifiable information

Key Considerations: Security

Key Considerations: Security



Key Considerations: Security

- This new generation of laws require compliance programs – documented policies and procedures that are enforced and updated regularly to reflect practices and developments:
  - "Reasonable" or "Appropriate" Information Security
  - Data Collection and Retention Policies
  - Data Protection and Security Policies
  - Incident Response Plan
  - Recordkeeping Requirements
  - Controls on transfers – specific contractual terms for vendors/ responsibility for vendors' actions

Key Considerations: Security

Bottom line:

- Be rigorous about your physical, technical and organizational safeguards for personal information
- Make sure your vendor agreements “flow down” your own privacy law obligations to your vendors

Key Considerations: Service Provider Management

- Accountability Principle
- Due Diligence/Security Reviews
- Ensuring adequate safeguards and protections in place with respect to service providers (2019 EY-IAPP Annual Privacy Governance Report)
  - Relying on assurances in the contract (94%)
  - Select third party based on data protection and information security warranties (88%)
  - Questionnaires re: data handling practices (57%)
  - Third party attestations or certifications (i.e. ISO27001, EU-U.S. Privacy Shield, SOC 2 Privacy, ISO 27002, TrustArc, etc.) (48%)
  - On-site audits (26%)
- Possible trend: more audits?

Best Practices

Best Practices: Know Your Data

- Understand what data you have and where it is.
- Think strategically about how you will be using data to maximize business opportunities both short, medium, and long-term.
- Consider whether you need all that data, and if there is other data that you need
- Determine how long you will keep data, before it becomes “stale”
- Be prepared to disclose what data you have, and why

Best Practices: Protect Your Data

- Conduct a full risk assessment, and periodic updates
- Implement security at all levels
- Encrypt data where possible
- Use multifactor authentication
- Maintain and update software and hardware
- Conduct Regular penetration and security tests, and at least annual reviews
- Do security reviews/due diligence on all vendors, and do annual audits

Best Practices: Protect Your Company

- Create a compliance program
- Train your personnel regularly
- Properly prioritize and fund information security
- Obtain appropriate cyber liability insurance coverage
- Have communications plans in place
- Conduct data breach exercises/tabletops
- Have appropriate contracts with vendors

Questions?

Thank You

For more information, contact:

Doron S. Goldstein
Partner
Katten Muchin Rosenman LLP
doron.goldstein@kattenlaw.com

Max Jarvie
Senior Associate
Borden Ladner Gervais LLP
mjarvie@blg.com

Katten

BLG
Borden Ladner Gervais