It’s 2018... Is Your Information Trustworthy?

Records Knowledge Conference
Sacramento, California
March 13th, 2018

By Bassam Zarkout
It’s 2018… Is Your Information Trustworthy?

About this session

- DigitalTransformation in Government and Private Sectors has led to an explosion of corporate information, which must be governed. A core tenet of IG is Information Trustworthiness… a framework that incorporates elements like accuracy, security, legal usage, protection of individuals rights for privacy, controls over dissemination, etc.

- Organizations face challenges in striking the appropriate balance between these elements. Advances in technologies like Blockchain, IoT, AI, RPA are fundamentally changing the nature, form and format of information assets, adding further complexity and urgency to this issue.

- Session will explore above topics and highlight the pivotal role that the disciplines of Records Management and Information Governance will play in this emerging world.

About Bassam Zarkout

- Tech executive with 25+ years of experience in IG, RM, ECM and IoT domains (including design/implementation of IG platforms as CTO of RSD)

- Founder of IGnPower, a consulting practice focused on IoT Data Governance, Privacy and Trustworthiness (and impact of Blockchain and AI on them)

- One of top 10 social influencer in Financial, Risk, Compliance, Fintech and Regtech in Canada - Thompson Reuters

- Resides in Ottawa, Canada
Digital Transformation...

- Digitization of Content, Processes, Business models
- Significant business benefits:
  - New business models
  - Better outcomes

- Massive volumes of Information Assets:
  - Created, Stored, Consumed
  - Significant challenges associated with that volume
  - Complex corporate information landscape
    - Documents, records, email, email, social media, back-office report output, paper
    - On-premises, cloud, etc.

Digital Transformation

High Volume of Information Assets
Need to look after Corporate Information Assets

- Lifeblood of organizations
- Need insight about Corporate Information Assets

Information Governance

- What problem does it solve?
- Is it a...
  - Strategy?
  - Program?
  - Set of technologies?

Who should lead Information Governance

- Chief Data Officer
- Chief Digital Officer
- Chief Information Officer
- Chief IG Officer
- Chief Risk Officer
- Chief Data Officer
- Legal Counsel
- Records Manager
- Data Protection Officer
- Other?
Information Governance: Strategy ↔ Program ↔ Technology

<table>
<thead>
<tr>
<th>IG Strategy</th>
<th>IG Program</th>
<th>IG Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision</td>
<td>Framework for Executing Strategy</td>
<td>Alignment with IT Strategy</td>
</tr>
<tr>
<td>Mission</td>
<td>Budgets</td>
<td>Alignment with Security Strategy</td>
</tr>
<tr>
<td>Mandate</td>
<td>Committed Stakeholders</td>
<td>Alignment with Data Privacy Strategy</td>
</tr>
<tr>
<td>Culture</td>
<td>Definition of Value for Stakeholders</td>
<td>Technologies to Power specific Use Cases</td>
</tr>
<tr>
<td>Executive Sponsorship</td>
<td>Published Corporate Policies</td>
<td>Other</td>
</tr>
<tr>
<td>Other</td>
<td>Specific Use Cases (with priorities)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication Strategy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

Information Governance Program

- **Cost**: Reduce cost of ownership of corporate information
- **Risk**: Reduce legal and regulatory compliance risks associated with owning information
- **Value**: Increase business value of information
Lifecycle of Corporate Information Assets

**Lifecycle Policy based on...**
- Business requirements
- Operational requirements
- Regulatory requirement
- Legal requirements
- Data Privacy requirements

**Retention during lifecycle...**
- Maintain integrity, accessibility and compliance with privacy
- Duration may be decades long
- Lifecycle of Information Asset may be longer than lifecycle of systems used to create it and store it

**What to do at end of life of asset...**
- Decision needed re what actions to take
- Regulations and laws may require disposition of assets
- Auditable execution of actions during lifecycle (and EoL):
  - Retention
  - Holds
  - Disposition, Transfer, Expungement
Challenges facing Information Governance

Despite its short history, Information Governance has had its share of challenges...

- Lack of maturity in discipline and organizations
- Technical complexity
- Organizational complexity
- Moving target... Privacy, IoT, Blockchain, etc.

**IG practices still emerging**

- Long on vision
- Short on execution
- Short on effective executive sponsorship

**Most IG programs not well established**

- Tighter IT budgets
- Most CIOs focused on infrastructure
- Records Managed stuck in the past
- Business Leaders focused on business

**Unclear who is in charge**

**Information Governance Program**

- **Cost**: Reduce cost of ownership of corporate information
- **Risk**: Reduce legal and regulatory compliance risks associated with owning information
- **Value**: Increase business value of information
### The Evolution of the Internet of X

<table>
<thead>
<tr>
<th>Documents</th>
<th>Commerce Data</th>
<th>Social Media Data</th>
<th>Device Data</th>
<th>Transactional Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Documents</td>
<td>Internet of Commerce</td>
<td>Internet of People</td>
<td>Internet of Things</td>
<td>Internet of Value</td>
</tr>
</tbody>
</table>

#### Examples:

- **Documents**: Box, Office 365, Dropbox for Business, OneDrive for Business
- **Commerce Data**: Amazon, eBay, Uber
- **Social Media Data**: Facebook, Twitter, LinkedIn
- **Device Data**: Google, Intel, Microsoft, IBM, SAP
- **Transactional Data**: Microsoft, IBM, Bank of America, Ripple, R3
More to Information Assets than just Documents

Documents
- E-Documents
- Email
- Audio
- Video
- Paper
- Other

Other Media
- Social Media
  - Corporate Systems
  - Public Systems
- BOTs
- RPA
- Other

Blockchain
- Smart Contracts
- Smart Assets
- Other

IoT
- Smart Cities
- Connected Cars
- Smart Factories
- Other

Future
- Tbd

Retention & Disposition, Holds, Cybersecurity, Privacy, Safety & Reliability (apply to some above), other...
Internet of Things

- IoT is the ability to generate operational data from sensor-equipped objects ("things") for the purposes of exploiting this data, gaining operational insight and ultimately producing "better outcomes"
  - Enhance productivity
  - Create new business models
  - Eliminate unplanned maintenance
  - Increase revenue
  - Other...

- IoT Data...
  - It’s coming
  - Actually, it’s already here!
  - Massive volume
Internet of Things

- Significant Economic Impact
  - By 2025 $3.9t to $11t (trillions)

- Many Application Areas
  - Smart Factories
  - Smart Cities
  - Connected Cars
  - Energy Management
  - Healthcare
  - Etc.
Blockchain & Smart Contracts

- **Blockchain**
  - Cloud-based database shared by every participant in a transaction
  - Essentially a peer-to-peer ledger

- **Smart Contracts**
  - Computer protocols that facilitate, verify, or enforce negotiation / performance of contract
  - UI that emulates logic of contractual clauses

---

**Figure 1. Three levels of blockchain**

1. **Storing digital records**
   - Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

2. **Exchanging digital assets**
   - Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

3. **Executing smart contracts**
   - Self-governing contracts simplify and automate lengthy and inefficient business processes.
     - **Ground rules**: Terms and conditions are recorded in the contract's code.
     - **Implementation**: The shared network automatically executes the contract and monitors compliance.
     - **Verification**: Outcomes are validated instantaneously without a third party.

*Source: Deloitte*
Smart Cities: IoT and Blockchain

- Why Smart Cities?
  - Improve operational efficiency, drive citizen engagement, identify new revenue sources, etc.
  - By 2019, 40% of Local/Regional Governments will use IoT to turn infrastructure into Assets instead of Liabilities (IDC)

- Integrated approach
  - IoT, Ubiquitous Connectivity (5G), AI, etc.
  - Cloud is so 2010’s... welcome to the Edge

- Blockchain protects data integrity
  - Vendors still trying to figure out how it can help with data integrity
    - Help securing data integrity from point of capture to point of analysis and storage
    - Strengthen chain of custody of data

Source: Twitter
Smart Cities: IoT and Blockchain
Smart Cities: IoT and Blockchain

Impact of blockchain technology on smart cities

Categories of government activity

- **Identities**
  - Self-sovereign identity for citizens

- **Movement of assets of value**
  - Transferring money from one person/entity to another
  - Enabling direct payments, once a condition has been met

- **Ownership and registries**
  - Land registries, property title
  - Corporate registry
  - Registry of assets of value - e.g., vehicles

- **Verification**
  - Licenses, proofs of records, transactions, processes, or events
  - Were services provisioned by meeting all conditions?
  - Was this service performed on this piece of equipment?
  - Does this person have the right permit?
Smart Contracts: California Bill AB-2658

- Builds on existing Uniform Electronic Transactions Act
- Paves way for electronic records secured by Blockchain to be deemed legal and enforceable
- Expands definition of “electronic” record and “electronic signature” to encompass those secured via Blockchain
- Expands legal definition of “contract” to encompass smart contracts
Multiple Governance & Control concerns about Information Assets

- **Retention, Disposition, and Holds**
  - Applies to Information Assets
  - Records Management, Information Governance, eDiscovery

- **Cybersecurity**
  - Applies to Assets and Information Assets

- **Privacy**
  - Applies to Information Assets that reference Data Subjects

- **Safety & Reliability**
  - Applies to Assets

- **Other**

**Notes**
- Multidisciplinary effort
- IG and RM are part of it
- Security is part of it
- Privacy is part of it
- In some cases, Safety and Reliability are part of it

Sometimes these requirements conflict with each other
Cybersecurity... a major concern

NIST Cyber Security Framework

1. Identify
   - AAA: Asset Management
   - BE: Business Environment
   - CV: Governance
   - RA: Risk Assessment
   - RM: Risk Management Strategy

2. Protect
   - AC: Access Control
   - AT: Awareness Training
   - DS: Data Security
   - IP: Information Protection
   - PR: Protective Technology

3. Detect
   - AE: Anomalies and Events
   - CM: Security Continuous Monitoring
   - DP: Detection Processes

4. Respond
   - RP: Response Planning
   - CO: Communications
   - AN: Analysis
   - M: Mitigation
   - IM: Improvements

5. Recover
   - RP: Recovery Planning
   - IM: Improvements
   - CO: Communications

Source: Twitter
Information & Data Privacy

- An aspect of Information Technology that deals with the ability of an Organization to determine what Personal Data (data about individuals) can be shared with 3rd parties
- Privacy Laws in the US
  - US Federal Privacy Act
  - State-level Privacy Acts
  - HIPAA
  - PCI
  - Other
Many businesses are still beginners at data-use governance

Only about half of respondents have put key measures in place

- 56% Have an overall information security strategy
- 53% Require employee training on privacy policy and practices
- 51% Have an accurate inventory of personal data
- 49% Limit personal data collection, retention, and access to the minimum necessary
- 46% Conduct compliance audits of third parties that handle personal data
- 46% Require third parties to comply with their privacy policies

Base: 9,500 respondents
EU General Data Protection Directive

- **What is it?**
  - Directive from the European Union that unifies data protection laws in EU
  - Identifies and grants rights for Data Subjects
  - Enforces protection of their Personal Data
  - Expands territorial scope
    - Not limited to EU companies

- **Who does it apply to?**
  - Obligations on Data Controllers and Data Processors
  - Significant penalties for non-compliance
    - Up to 20 M€ ($25 million) or 4% of global revenue

- **When does it apply?**
  - May 25th, 2018
Personal Data

- **What is it?**
  - Information provided by Data Subjects to Data Controllers and Data Processors that can be traced back to the Data Subjects

- **Personal**
  - Name, gender, national ID, location, DOB, physical, genetic, psychological, mental, cultural, social characteristics, online computer identifiers, medical, financial, etc.

- **Organizational**
  - Recruitment, salary, performance, benefits, etc.

- **Other**
  - Race, ethnic, religious, political opinions, biometric, etc.
Information Trustworthiness

- Degree of confidence one has about an Information Asset that it meets the key corporate, legal, compliance and standards requirements

Information Governance Program

- Cost
  - Reduce cost of ownership of corporate information

- Risk
  - Reduce legal and regulatory compliance risks associated with owning information

- Value
  - Increase business value of information

Information Trustworthiness empowers the Information Governance Program

Multiple adjacent (and overlapping) domains of Information Trustworthiness, each may have a different stakeholder
Information Trustworthiness

- **Each Domain can have multiple states**
  - **A. Current State**
    - Actual state as it exists now
  - **B. Minimum State**
    - Non-negotiable minimum level
    - Mandated by requirements
    - Laws, regulations, industry standards, best practices, etc.
  - **C. Market State**
    - State that is common with competitors (on-par) in same market industry
  - **D. Leader State**
    - Target level of Trustworthiness to be a leader
    - Alignment with corporate vision, ROI, risk, etc.
  - **E. Maximum State**
    - Highest level theoretically achievable
    - Justification to reach this state?
IG Journey: Information Trustworthiness centric approach

- Define states for each Trustworthiness Domain
  - Current, Minimum, Market, Leader, Maximum
  - Define better outcome at end of each segment

- Determine interdependency of states across Domains
  - Does Privacy impact Legal Holds & eDiscovery Readiness?
  - Does Security impact Retention & Disposition processes?
  - Other

- Define Information Governance Journey
  - Define cost justification and ROI models
    - Is there really an ROI for segment?
  - Define Trustworthiness by Design Requirements
  - Determine priorities

- Develop Trustworthiness Maturity Model
  - Progress of Current state towards other states
  - Track, measure, manage, adapt
## IG Journey: Information Trustworthiness centric approach

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>RM</th>
<th>Legal</th>
<th>Privacy</th>
<th>Security</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Align RM Program and Retention Schedule with Legal requirements</td>
<td>RA</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>?</td>
</tr>
<tr>
<td>2</td>
<td>Align Legal requirements with Privacy requirements</td>
<td>C</td>
<td>RA</td>
<td>R</td>
<td>C</td>
<td>?</td>
</tr>
<tr>
<td>3</td>
<td>Align Security requirements with Privacy requirements</td>
<td>I</td>
<td>I</td>
<td>RA</td>
<td>R</td>
<td>?</td>
</tr>
<tr>
<td>4</td>
<td>Align RM Program and Retention Schedule with Privacy requirements</td>
<td>R</td>
<td>C</td>
<td>RA</td>
<td>R</td>
<td>?</td>
</tr>
<tr>
<td>5</td>
<td>Align Legal and Security requirements</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>RA</td>
<td>?</td>
</tr>
<tr>
<td>6</td>
<td>Align RM Program and Retention Schedule with Security requirements</td>
<td>RA</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>?</td>
</tr>
</tbody>
</table>

**RACI Model:** Responsible, Accountable, Consulted, Informed

**Diagram:**

- Information Trustworthiness
- Retention & Disposition
- Legal Holds & Legal Usage of Data
- Information & Data Privacy
- Information & Data Security
- Future? (eg. Safety)
Summary

- Digital Transformation continuing unabated
  - Information Assets → lifeblood of organizations
  - Information Governance programs needed to govern these assets

- Internet of X evolution ... new challenges
  - New technologies: IoT, Blockchain, AI
  - New solutions: Smart Cities, Smart Factories, etc.
  - Growing overlapping concerns
    - Retention, legal, privacy, security, etc.

- Information Trustworthiness Framework
  - Empowers the Information Governance Program
  - Supports investment decision making
  - Maturity Model → track, measure, manage, adapt
  - RM has significant role to play
Thank You...
### Useful Twitter Hashtags

<table>
<thead>
<tr>
<th>Category</th>
<th>Helpful Twitter Hashtags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Transformation</td>
<td>#DigitalTransformation #RPA</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>#IoT #IoT #InternetofThings #SmartCities #Industry40 #4IR #DigitalTwins</td>
</tr>
<tr>
<td>Blockchain</td>
<td>#Blockchain #SmartContracts #FinTech #RegTech</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>#AI #ArtificialIntelligence #AutonomousCars #MachineLearning #ML</td>
</tr>
<tr>
<td>Privacy</td>
<td>#GDPR #PrivacybyDesign #PrivacybyDefault #DataPrivacy #HIPAA #PCI</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>#CyberSecurity</td>
</tr>
</tbody>
</table>
Blockchain

**How Blockchain Works**

1. **Alice wants to send money to Ben**
2. **The first Block is created online and represents the transaction**
3. **This Block is broadcast to every party in the network**
4. **Those in the network approve the transaction and validate it**
5. **The Block is then added to the Chain which provides a permanent, non-repudiable and transparent record of the transaction**
6. **Ben receives the money from Alice**

**Notes:**
- Transactions are not valid until added to the Chain. Tampering is immediately evident.
- The Blockchain is regarded as safe as everyone in the network has a copy. The source of any discrepancies are usually evident immediately.
Data Protection Impact Assessment (DPIA)

- Effort led by Data Protection Officer

- Assess risks to Personal Data in relation to affected types of data processes
  - Origin
  - Nature
  - Particularity
  - Severity

- Identify methods for compliance requirements for protecting Personal Data
  - Identify minimum requirements
  - Consult with Supervisory Authority if necessary

---

1 Data Controllers and Data Processors
2 New data processes, changes in data processes, and changes in scope of data