Organizational Accountability and Privacy Compliance

Marty Abrams
July 2013

What Are Our Compliance Objectives for Privacy?

- It isn't as simple as saying just comply with the law
  - The laws paint broad objectives such as protect fundamental rights and/or protecting against harms and risks
  - Often create procedural requirements that aren't consistent with how data appears, is used, how it travels, and where it rests
- An informational society morphs more quickly then we can change laws or regulations, or bring enforcement actions

Legacy data protection law and compliance is challenged by

- Self-publishing
- Fully observational world
- Expectations for advanced analytics
- Sensor rich environment that pinpoints location
- Distributed responsibility such as mobile computing
- Cloud computing
- Global business collaboration
- Anti-terrorism processes

Limits of Notice and Consent

- Purpose specification and consent have been the significant element in governance and
- still very important
- however:
  - With complex data application consent is too often a mechanism to transfer risk from the organization to the individual
    - Purpose specification notices as long as "Hamlet"
    - Does the notice really limit purpose or increase transparency?
  - To quote Malcolm Crompton, "the party that gets the benefit should bare the risk."

Transition Has Been Jolting

- Europe
  - 1995 – the Directive is heavily consent based
  - 2013 – "European law requires a legal basis to process, one of which is consent" (Viviane Reding, Vice-President of the European Commission)
- Canada
  - 2007, in response to questions – "Canada's law is consent based," Jennifer Stoddart, Privacy Commissioner of Canada
  - 2012 Accountability requires a comprehensive program

Telling Document

- WP 29 paper 3/2013 “Purpose Limitation”
  - Formula for determining what is a compatible purpose
  - When push comes to shove it is about a legitimate or fair purpose
  - How does one create a methodology around legitimate or fair purpose?
    - This is a forward looking topic at the International Conference in Warsaw

An Organization's Data Protection Objectives

- Manage external risks
  - Legal compliance
  - Reputational management
  - Protect investments
  - Assure business continuity
- Build public trust
  - Assure flow of data from and about individuals
- Alignment with organizational values
- Manage data as a financial value generating asset

Enforcement Agency Objectives

- My suggestion
  - Create an environment that via carrots and sticks encourages compliance with both the letter and spirit of the law
    - Clear stated objectives for compliance
    - High certainty of enforcement if an organization abuses it's data stewardship responsibilities
    - Added flexibility if an organization can demonstrate its willingness and capacity to be compliant
  - That means organizations must understand the risks they create for others
  - Mitigate those risks to the best of their abilities

Three Core Concepts Evolving

- The use of data rather than collection becoming the nexus for enforcement/compliance.
  - What does collection even mean?
  - How does one determine the future application of data?
- Uses of data evolve
  - What does respect for context and legitimate purpose actually mean?
- Without the discipline of collection based purpose specification, protection will be based on responsible and answerable organizations
  - That is accountability

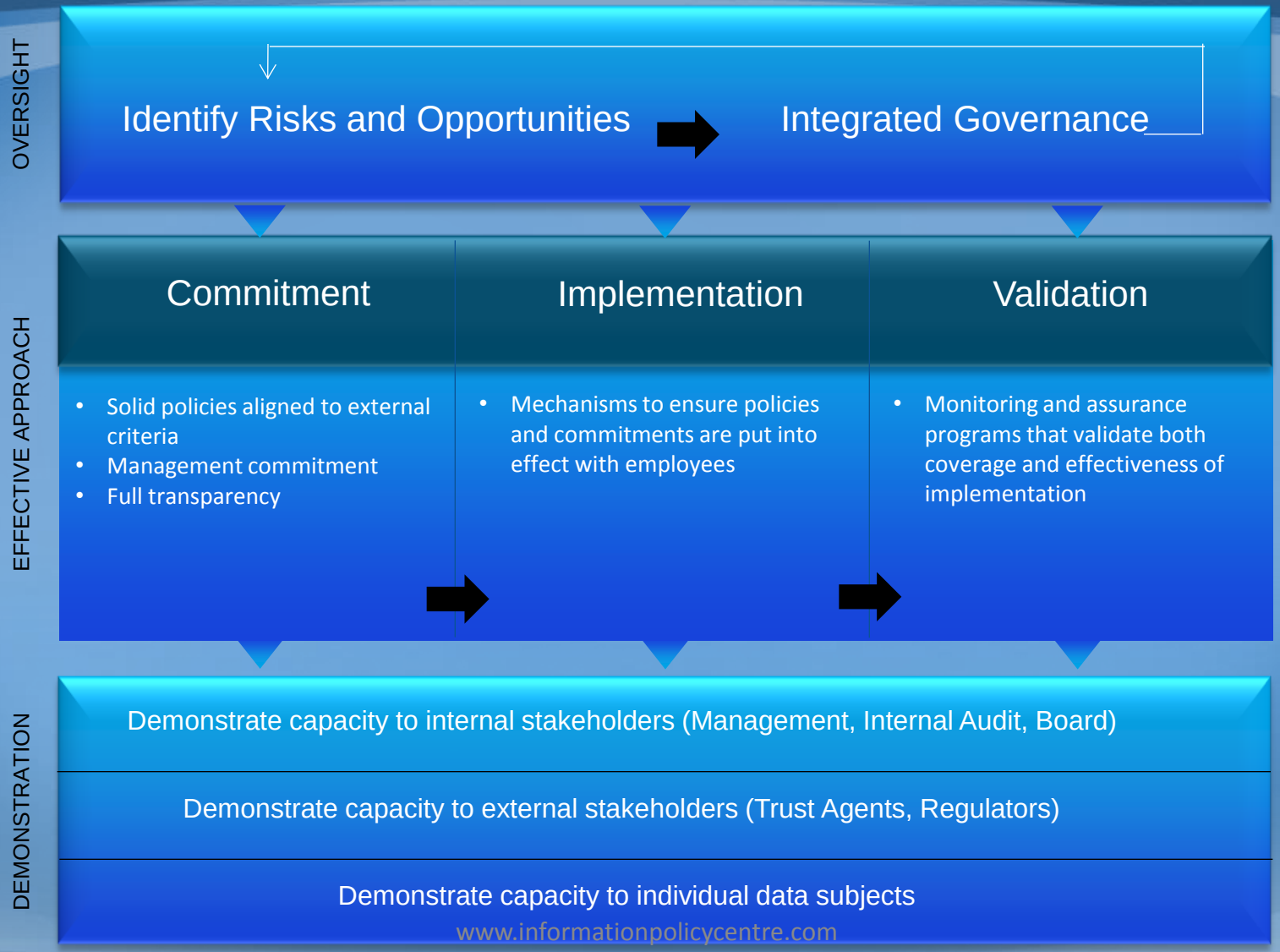
The Essential Elements of Accountability Are the Outline for a Full Program

- Was defined by Global Accountability project
- Began in 2009 in Dublin
- Continued in Paris, Madrid, Brussels, Warsaw and Toronto
- Has included participation from governments, DPAs, civil society, academics and business.
- Has heavily influenced policy development.

Essential Elements

1. High level commitment to being a responsible and answerable organization with policies linked to data protection law.
2. Mechanisms to put policies into effect including processes to identify and mitigate risks to individuals.
3. Systems providing internal oversight and assurance reviews and optionally third party validation.
4. Individual participation including the ability to see and dispute.
5. Means for remediation and external enforcement.

Accountability Ecosystem



Use and Obligations

- Uses of data, such as fulfillment and research, are characterized.
- Obligations are linked to types of uses.
- As uses of data change they pick-up the added obligations that go with new uses.
- Requires a comprehensive program with organizations standing ready to demonstrate the program.

Accountability and Big Data

- Centre Big Data Project suggests a two phase approach:
  - Research or discovery
    - Support for research as an always compatible purpose
  - Application
    - One is better able to apply traditional data protection approaches
- Both phases require assessment and mitigation of the risks for individuals
  - De-identification is an example of a mitigation strategy
- An organization will have to stand ready to demonstrate its risk abatement process – this suggests an accountability approach.

Policy Vacuum

- A consensus needs to be created on the parameters of information processing related risks for individuals.
  - Beyond financial harm
  - But not so inclusive that includes the ocean

Richard Thomas Suggestion

- Three types of risks
  - Tangible
    - Lose of life, pay more for a loan
  - Intangible
    - Reputation
  - Societal
    - Stifle free expression and liberty
- Evaluated based on likelihood
- More work to be done

Thanks

Martin Abrams
E-Mail: mabrams@hunton.com
www.informationpolicycentre.com