DIGITAL ECONOMY, DATA PROTECTION, AND INFORMATION ACCOUNTABILITY

MARTIN ABRAMS
Why information accountability 2.0?

We live in a fully observational world that powers innovation through advanced analytics. This isn’t just about businesses making money. Absent effective data governance individuals run the risks of losing free will and the benefits of better healthcare, education and opportunity. With effective data governance in a market economy we may assure both.
UPDATING THE DEFINITION OF DATA PROTECTION

• Peter Hustinx – Former European Data Protection Supervisor
  • Data protection is broader than privacy in that it facilitates other fundamental rights
  • Those fundamental rights include education, health, and opportunity
  • Data protection is therefore the appropriate processing of information that may be linked to a unique individual
  • Individuals fundamental rights are impacted by not using data that facilitates those rights

• Next generation data protection requires a more holistic approach to data governance
  • Simple checkbox compliance doesn’t match the spirit of why we have DP law
  • Consent alone is less effective as a governing tool

• Our challenge is to move governance beyond privacy
• That is why we are discussing accountability
EVOLUTION OF AN INFORMATION ECONOMY THAT HAS IMPACTED OVERSIGHT

• Mainframe era – Data and systems were the same

• Database technologies – Data could serve many systems, secondary use became an issue

• Emergence of predictive sciences – Broad data sets used to predict future behavior

• Internet – Explosion of observation, often by many parties

• Internet of Things – Observation accelerates

• Big Data – All data available for predictions
NATURE OF DATA RELATED TO INDIVIDUALS

• Origins of data have changed as technology has evolved
  • Mainframe-era data was collected directly from us
  • Today, fastest growing data sets come from observation and product of predictive sciences
  • To understand effective data protection one needs to understand the origins of data
DATA TAXONOMY BASED ON ORIGIN

• Was developed for OECD March 2014 workshop

• Data may be segmented into four classifications based on origin
  • **Provided** – Comes directly from individual with their direct knowledge
  • **Observed** – Individuals’ behavior is monitored on the Internet, public places and sensors built into things like cars
  • **Derived** – The product of grouping data and simple math
  • **Inferred** – Categories that come from predicative sciences
POLICY IMPLICATIONS FROM TAXONOMY

• Observed and inferred data are fastest growing data sets
• Often without the attention of busy individuals
• Therefore consent, while very important, becomes less effective in protecting fundamental rights
• How does one fill the gap?
INFORMATION ACCOUNTABILITY

• Part of Colombia’s data protection law

• Accountability first appears in OECD Guidelines in 1980, but not well defined

• First principle in Canadian private sector law (2000)

• Last principles in APEC data privacy framework (2004)

• Fully defined by “Accountability Global Dialogue” (2008 to present)

• Part of EU Draft Regulation

• Guidance from Hong Kong and Canadian regulators
ACCOUNTABILITY’S ESSENTIAL ELEMENTS

Essential elements defined by a multi-national and multi-stakeholder process in 2009

1. A commitment to accountability and an internal policy that links to external criteria (in Colombia that means the data protection law)
2. Programs to put the policy into effect including privacy by design
3. Monitoring to assure the program is effectively protecting privacy
4. Individual participation (for example access and correction or deletion where appropriate)
5. Enforcement, mitigation and the ability to demonstrate a program to regulators
EFFECTIVE PROTECTION IS THE OBJECTIVE

• Accountability requires a comprehensive program so a company can demonstrate effective data stewardship
• It fills the gaps when creating and using observation and inferences to originate and use data
• Pathfinder global companies have established accountability programs
• International privacy authorities are moving in this direction
PROOF POINTS

• EU papers on big data, legitimate interests, and compatible use
• Canadian “Getting Accountability Right with a Privacy Management Program”
• Hong Kong “Privacy Management Programme”
DATA INNOVATION AND BIG DATA

• Reticence risk kills innovation and this impacts people as much or more than lose of privacy

• Innovation requires more thoughtful data protection

• Accountability creates the infrastructure for innovation with effective protections

• Accountability requires legal structure that accommodate it
  • Such as legitimate interests as a legal means to process with the demonstration of appropriate balancing of interests
ACCOUNTABILITY, BIG DATA AND THE INTERNET OF THINGS

• Rule one, individuals are negatively impacted both by reticence in using data, and the misuse of that same data

• To be accountable one needs to understand the risks of both using and not using data (essential element 2)

• There needs to be a legal means to create permissions to use data when data is at a distance from the individual

• We need to creatively use governance, such as codes of conduct, to create those legal means

• This rests on accountability
FIND MARTIN ABRAMS

- mabrams@informationaccountability.org
- www.informationaccountability.org
- Key papers are on the website