NEMC 2015
Privacy Considerations and Big Data, Friends or Foe
Regulated Industry Perspective

Jennifer Barrett Glasgow, CIPP
Global Privacy and Public Policy Executive

Updated January 2015
Big Data Opportunities and Challenges

• Technology Trends
• Policy Implications
  – Private Sector Frameworks
  – Government Sector Frameworks
  – Cross-jurisdictional Considerations
• Improving Outcomes
Technology Trends

• **Big Data = Big Security**
• Data volumes and velocity skyrocketing
  – Sensors everywhere (ABI estimates 40.9 billion sensors by 2020 & 400 million smart cars by 2030)
• Increasingly complicated ecosystem
  – Many new players in the marketplace (> 4 million Apps on top 5 stores)
• Data sharing on the rise
  – “Anonymous” data more often shared/posted
• Analytic tools much easier to use
  – Don’t require a trained “data scientist”
Big Data Analytics

Phase 1: Discovery

Collection/Acquisition → Pre-processing → Integration → Analysis [Correlations, Trends, Patterns] → Interpretation [Quality evaluation]

Algorithm [Model]
- Classification
- Regression
- Segmentation
- Association
- Sequence

Iterative process: Quality Not Sufficient or New Questions Arise

http://informationaccountability.org/
Big Data Analytics

Phase 1: Discovery

Collection/Acquisition ➔ Pre-processing ➔ Integration ➔ Analysis
[Correlations, Trends, Patterns] ➔ Interpretation [Quality evaluation]

Iterative process: Quality Not Sufficient or New Questions Arise

Phase 2: Application

Data, some linked to individuals ➔ Input ➔ Apply Algorithm ➔ Output
Tailored Results

Algorithm [Model]
Classification
Regression
Segmentation
Association
Sequence

Refresh Algorithm

http://informationaccountability.org/
Private Sector Legal Framework

Out of date and modernizing slowly…

• Laws protecting sensitive data
  – HIPAA: health care
  – GLBA: financial services

• Laws governing eligibility decisions
  – FCRA: credit, insurance, employment, rentals

• Laws protecting vulnerable classes
  – COPPA: children
  – Lending Laws: discrimination

• Laws governing certain aggressive practices
  – TCPA and DNA Registry: telemarketing
  – CAN SPAM: email marketing
Private Sector Self-Regulatory Frameworks  *Rapidly expanding*…

- Self-regulatory codes governing marketing
  - Direct Marketing Association (DMA)
  - Digital Advertising Alliance (DAA)
  - Network Advertisers Initiative (NAI)

* * * * * * * * * * * * * * * * * * * * *

- Notice (transparency)
- Choice (company & industry)
  - Opt-in for sensitive data (e.g. health, precise location)
  - Opt-out for all other non-sensitive data
Private Sector Self-Regulatory Frameworks

- Information Accountability Foundation
  - Big Data Ethics Initiative

Ethics
- Beneficial
- Progressive
- Sustainable
- Respectful
- Fair

Sources → Prep (ETL) → Insights → Application

Fairness
- Project Purpose
- Legal Obligations
- Accountability
- Stakeholders
- Benefits/Risks/Mitigation

Rapidly expanding…

http://informationaccountability.org/
Private Sector Self-Regulatory Frameworks  
*Rapidly expanding…*

- Future of Privacy Forum
  - Impact and Benefit/Risk Analysis for Big Data Projects

* * * * * * * * * * * * * * * *

- Privacy Impact Assessment (PIA)
- Data Benefit Analysis (DBA)

http://www.futureofprivacy.org
Private Sector Self-Regulatory Frameworks  *Rapidly expanding…*

- Modernizing OECD Privacy Principles
  - Data Protection Principles for the 21st Century

  * * * * * * * * * * * * * * *

- Balance privacy and the free flow of information so we don’t suppress innovation, the original OECD goal.
- Reduce the focus on collection limitations by emphasizing a contextual assessment of the benefits and risks.
- Reduce the role of the purpose specification and use limitation principles which allow only uses that are “not incompatible”.
- Make data **users** more accountable for the personal data they access, store, and use, and hold them liable when harm to data subjects occurs.
- Adopt a broader definition of “harms” arising from inappropriate uses of personal data and mitigate those harms.

Private Sector Anonymization Challenge

Ease of Technical Re-identification

100%

0%

PII / Personal

ANl / Anonymous

Technical & Administrative De-Identification

Notice

Choice

© 2013 Acxiom Corporation. All Rights Reserved.
## Private versus Government Frameworks

<table>
<thead>
<tr>
<th>Laws &amp; Regulations</th>
<th>Private Sector</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓ +</td>
<td>✓ +</td>
</tr>
</tbody>
</table>

| Self-Regulation    | ✓ +++          | ?           |
Cross-jurisdictional Considerations

- Security – Security – Security
- Different social norms about privacy
  - Fundamental human right (EU)
  - Consumer protection (US)
  - Confidence in ecommerce (Asia)
- Different legal systems, laws and regulations
  - Striving for interoperability (not consistency)
Improving Outcomes

Government should.....

✓ Promote responsible data driven environmental innovation

✓ Help define “ethical uses” of big data

✓ Fund/train more expert “data scientists”
“Like a force of nature, the digital age cannot be denied or stopped”

“Being Digital” (1995) by Nicholas Negroponte

Thank You!

Jennifer Barrett Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation
Email: jennifer.glasgow@acxiom.com
Phone: 501-252-2316