Big Data vs. Big Brother: The fine line of personalization and privacy

Dr. John Schibrowsky, Faculty Mentor, Department of Marketing & International Business, Lee Business School

ABSTRACT

Purpose - To review privacy issues surrounding Big Data and creating recommendations to aid in resolving these issues.

Approach - Reviews current literature regarding Big Data and its implication on privacy.

Findings - Regulation changes/additions not as beneficial as some researchers believe. Creating and streamlining one universal regulation to better protects consumer privacy information may gain back consumer confidence.

INTRO/PURPOSE OF THIS STUDY

Consumer privacy issues to public due to negative publicity: (Cannon 2002, Kroft 2014)
- Corporation Big Data usage questionable
- Data broker methods; collect, house, distribute
- Emergence of Internet increased collection with issues resulting from:
  - Lack of secure data storage result = data breaches
  - Use/share of data for marketing purposes
  - 9/11 - USA PATRIOT ACT & FISA amendment
  - IRS tax profiling uproar
  - Expanded use and distribution of consumer data by database marketers

Examples: (Duhigg 2012, Reuters 2014)
- Target and Pregnant Teen
- Google Lawsuit - co-mingling of data

LITERATURE REVIEW

BIG DATA
Arthur (2013) – Collection of data retrieved from varied sources serving as basis for endless discovery and analysis with three Key characteristics - the “3 V’s”: Volume, Velocity, Variety (Podesta et. al. 2014)
- George et. al. (2014) – Five key sources of high volume data:
  1. Public Data
  2. Private Data
  3. Data Exhaust
  4. Community Data
  5. Self-Quantification Data

Promise of Big Data
- Wu (2014) – Potential to generate unmatched knowledge for society
- Hirsch (2014) – To be fundamental resource to power information economy.

Issue of Big Data – Balance of rewards and stakeholder risk protection is needed (Sloan & Warner 2014)
Richards and King (2014) suggest three paradoxes to realize true nature of Big Data issue:
- The Transparency Paradox: Collection efforts invisible
- Identity Paradox: Extreme difficulty creating, separating, keeping consumer identities private.
- Power Paradox: Privilege of power

PRIVACY
- Smith et. al. (2011) – Numerous unsuccessful attempts made to merge privacy perspectives; “fragmented concepts, definitions, and relationships” not empirically validated
- Charters (2002) – Privacy not clearly defined; “weaker right;” lacks good individual protection

Why is Information Privacy an Issue?
- Aaken (2014) – Consumers realize in order to gain access to services they must “voluntarily” provide information
- Lesk (2013) - Consumers lack understanding of collection and control over data usage; Huge amounts of consumer data sold
- Brookman & Hans (2014) - consumer/organization concerns center around five threat models: 1) data breach; 2) internal misuse; 3) unwanted secondary use; 4) government access; & 5) chilling effects

Past Recommendations: Big Data Privacy Issue
- Brookman & Hans (2014) - Consumers need privacy interest in commercial data collection
- Colonna (2014) - Theory shift from “data protection” to “data empowerment” revealing better link with “technological reality”
- “Hiding From Big Data,” (2014) - Privacy products market focus
- Tene & Polonetsky (2012) – Model balancing organization data benefits & consumer privacy rights; data collection justification
- Thierer (2014) – “Bottom up” approach to privacy

CONCLUSION
- Endless exponential Big Data growth with consumer privacy as shadow
- Significant potential in gaining stakeholder value
- Scholars and government entity regulations – numerous challenges or too broad, allow entities ways around them
- Several proposals and regulations have significant discrepancies or require further primary research to substantiate them
- Privacy not clearly defined, hard to see what is or is not a violation

RECOMMENDATION & FURTHER STUDY
- Businesses must streamline all privacy efforts
- Privacy must be better well-defined; should distinctly state any collected personal data having potential of causing harm to its owner be omitted from collection
  - To include financial, health, sexual orientation, race, etc. data.
- No collection of data for those under 18 yrs of age
- Further study: Ways to handle personal data already in possession of government and other entities