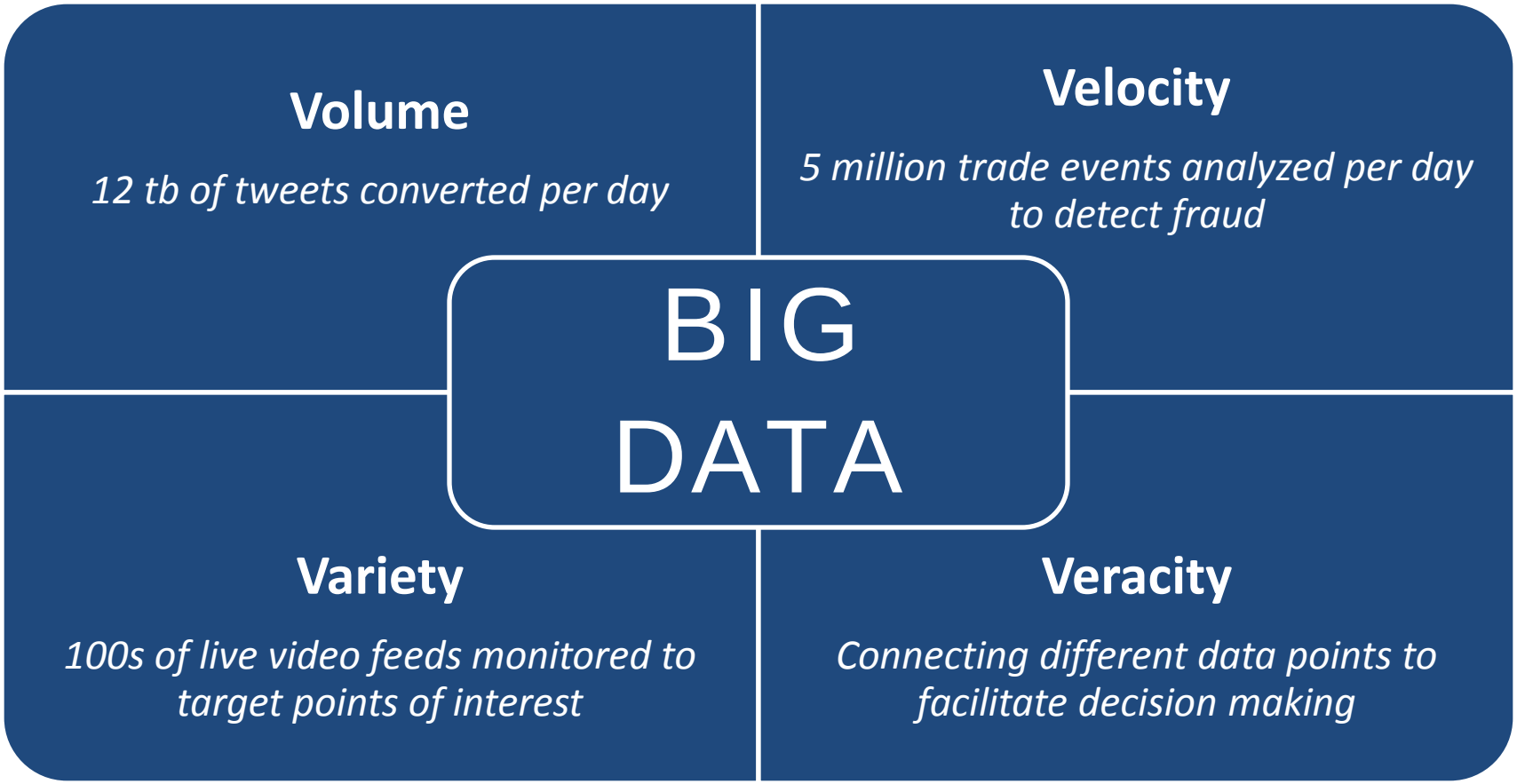
Legal Challenges for Big Data Companies

August 21, 2013

Satya S. Narayan
SNarayan@rroyselaw.com
Phone: 650.521.5745

ROYSE LAW
Royse Law Firm, PC

"Big Data is a term that describes large volumes of high velocity, complex, and variable data that requires advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information." - TechAmerican Foundation.



ROYSE LAW

Key Legal Concerns

- Data privacy and security
- Compliance issues
- Service levels
- Reliability and other warranties
- Indemnification and Limitations of Liability

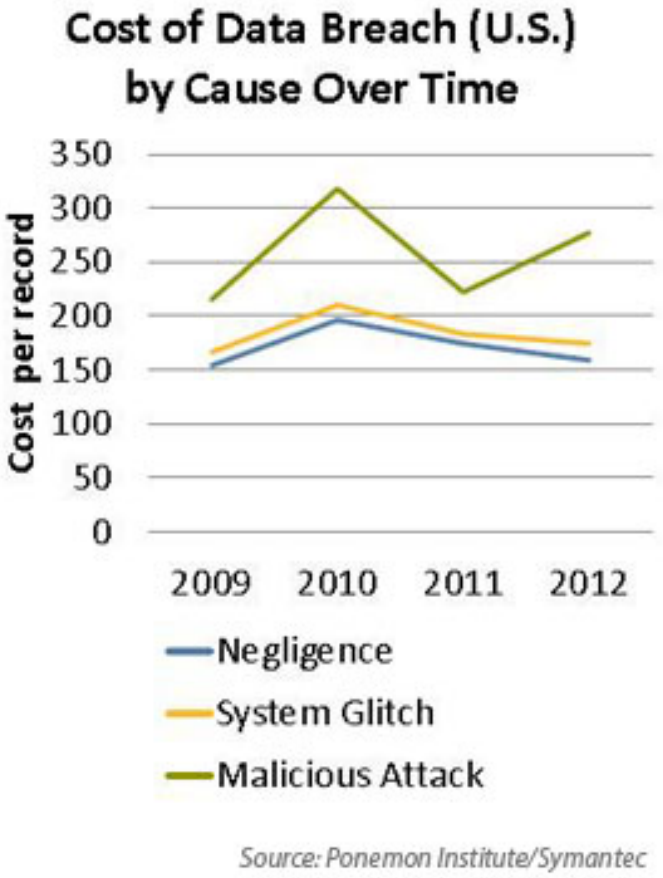
Data Privacy

- *Personal information "is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." – National Institute of Standards and Technology*
- Data handling permissions; usage restrictions
  - End user's permission
  - Fair Credit Reporting Act
    - Consumer's right to correct personal information
  - Do Not Target v. Do Not Collect debate
  - Is de-identification/ anonymization of data done properly to prevent re-identification
- Whose privacy policy should apply?
  - Is Customer's privacy policy too restrictive?
  - What permissions does Customer need to obtain from end users?

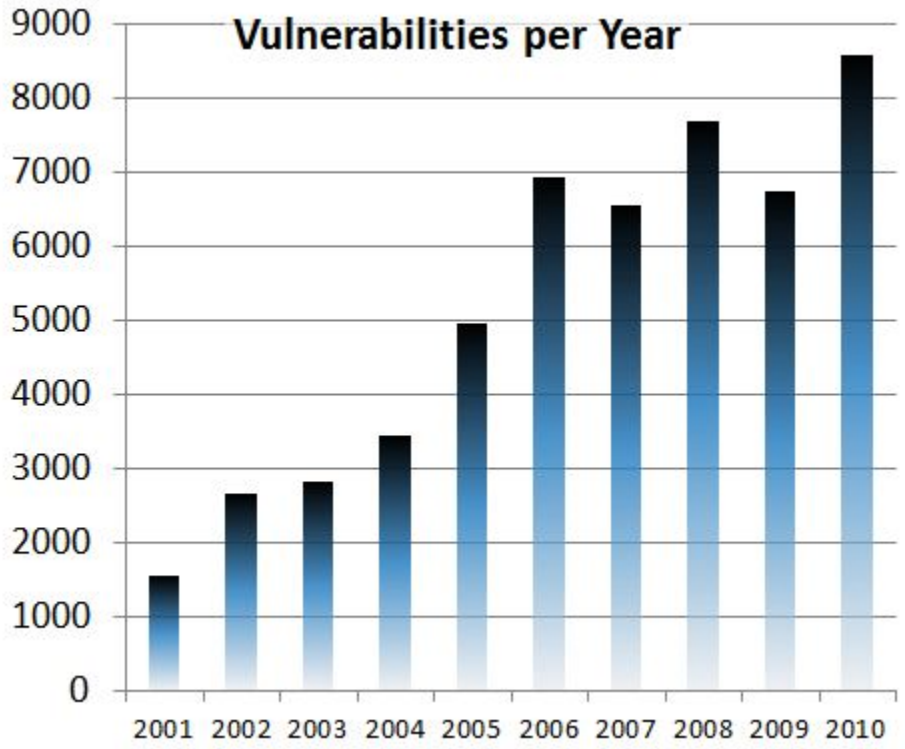
Data Security

- “Reasonable/ appropriate” security measures – not good enough
- Whose privacy policy and security policy should apply?
  - Customer’s data security questionnaires and data privacy schedules
- Security audits
- To what extent should Customer be responsible for data security and privacy issues?
- Who bears the risk of a “no-fault” breach?

Costs of Data Security Breaches



Source: Ponemon Institute/Symantec



ROYSE LAW

Data Security

- Data security related potential costs; can these costs be shared?
  - Data security breach costs
    - Notification related costs
    - Support costs (e.g., help desk and credit monitoring services)
    - Fines and litigation
  - Security audit costs
    - SSAE (16) Type II Audit
      - Enterprise customers, particularly publicly traded customers, will often ask for this audit if Provider performs outsourced services that affect the customer's financial statements
      - $20,000 – $50,000 (depending on type of business, number of locations, number of employees, number of applications, and deadline for completion)
  - Implementation costs of new security measures

Compliance issues

- What is the Provider's role in data-related compliance?
  - Data privacy and security
  - E-discovery and document preservation
  - Regulatory compliance in specific industries (for example, pharma and automotive industries; banking and financial industry)

Service Levels

- What performance guarantees should a Provider give?
  - Uptime, throughput, mean-time-to-restore, latency, and bandwidth guarantees
  - Customer may ask for warranties
  - Criticality of service to Customer's end-user interactions
- Limitations/ exclusions (for example, Provider's hosting provider's failures)
- Remedies
  - Service credits; fixing the issue; contract termination
  - Are your remedies exclusive?
  - Is payment of service credits automatic?
- Customer duties and responsibilities

Reliability and Other Warranties

- Warranties
  - Data accuracy and completeness?
  - Software performance?
  - Warranties implied by law
- Exclusions
- Disclaimer

Indemnification & Limitations of Liability

- Provider indemnification:
  - Breach of privacy or security?
  - Third-party intellectual property infringement?
  - Customer's customer issues (for example, from a breach of a service level)?
  - Exclusions
- Should the Customer indemnify the Provider?
- Limitations on Provider's liability:
  - Consequential damages disclaimer (for example, lost profits of Customer arising from a data security breach)
  - Caps on liability
  - Exclusions from liability limitations
- Insurance

Additional Customer Asks

- Post-termination transition/ migration assistance
- Return of Customer data
- Source code/technology escrow
- Business continuity/exit plans
- Change of control consent/ notice

Concluding Comments

As a Provider, pay close attention to:

- obtaining adequate data permissions
- proper de-identification/ anonymization of data
- specifying a uniform security standard
- specifying uniform service levels and remedies
- assessing risks and developing a playbook for warranty, indemnity, and liability negotiations; identify your maximum risk undertaking threshold
- obtain adequate insurance
- watch for new FTC and privacy legislation and guidance

Satya S. Narayan
SNarayan@rroyselaw.com
Phone: 650.521.5745

Royse Law Practice Areas

Corporate Securities
Tax
Mergers & Acquisitions
Fund Services
Intellectual Property
Technology Transactions
Labor & Employment
Immigration
Litigation
Estate, Trust & Wealth Strategy
Real Estate
International

ROYSE LAW
Royse Law Firm, PC

PALO ALTO
1717 Embarcadero Road
Palo Alto, CA 94303

LOS ANGELES
11150 Santa Monica Blvd.,
Suite 1200
Los Angeles, CA 90025

SAN FRANCISCO
135 Main Street,
12th Floor
San Francisco, CA 94105