Understanding the Difference Between Security and Privacy

Melvin Greer
Senior Fellow
Chief Strategist Cloud Computing
Certified Information Privacy Professional
Lockheed Martin

March 26, 2015
Inhibitors to Cloud Adoption

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

Security: 74.6%
Performance: 63.1%
Availability: 63.1%
Hard to integrate with in-house IT: 61.1%
Not enough ability to customize: 55.0%
Worried on-demand will cost more: 50.4%
Bringing back in-house may be difficult: 50.0%
Regulatory requirements prohibit cloud: 49.2%
Not enough major suppliers yet: 44.3%

Source: IDC Enterprise Panel, August 2008, n=244

What's inhibiting adoption?

- Security: 55%
- Regulatory/Compliance
- Lock-In
- Interoperability
- Privacy
- Network bandwidth
- Reliability

Copyright 2015 Lockheed Martin All rights reserved
Privacy Concerns Growing

Data paradoxically is both a crown jewel and a commodity. Consumers dependence on ubiquitous connectivity and frictionless access to data contrasts with important privacy and security practices, which unfortunately consider these advances as an obstacle.
Update to EU Privacy Regulation

The 2014 Cloud Computing Policy Conference USA
June 11, 2014 / W Washington DC Hotel

Comparative legislative timeline

- **Commission proposal**: 17/7/1990
- **Commission amended proposal**: 15/10/1992
- **Council Common Position - amendments**: 20/2/1995
- **Parliament 2nd reading - amendments**: 15/6/1995
- **DPD adopted**: 25/10/1995

Data Protection Directive

- **Commission proposal**: 25/1/2012
- **Parliament 1st reading – 207 amendments**: 12/3/2014
- **Council 1st reading - amendments inevitable**: ?
- **GDPR adopted**: ?

Draft General Data Protection Regulation

© 2015 Kuan Hon kuan0.com. You may copy/use this diagram under a CC BY 2.0 UK licence https://creativecommons.org/licenses/by/2.0/uk/ retaining the attribution in this paragraph.

Copyright 2015 Lockheed Martin All rights reserved
EU General Data Protection Regulation

Notice—data subjects should be given notice when their data is being collected

Purpose—data should only be used for the purpose stated and not for any other purposes

Consent—data should not be disclosed without the data subject’s consent

Security—collected data should be kept secure from any potential abuses

Disclosure—data subjects should be informed as to who is collecting their data

Access—data subjects should be allowed to access their data and make corrections to any inaccurate data

Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles

The United States prefers what it calls a 'sectoral' approach to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather than governmental regulation alone
Who is Really at Risk?

Heartland Payment Systems, 2008-2009: 130 million user credit and debit cards compromised

Target Stores, 2013: 110 million customer full names, addresses, email addresses and telephone numbers had been compromised.

Sony online entertainment services, 2011: 102 million users login credentials, names, addresses, phone numbers and email addresses had been exposed

Anthem, 2015: 69 million to 80 million customer names, addresses, dates of birth, Social Security numbers and employment histories records were compromised
Privacy Awareness

Secondary Use of Data

Super Cookies

Transparency Reports

Mass Digital Forensics and Surveillance

GeoLocation

Data Breaches

Profiling

Wearable Tech, IoT, Personalized Marketing, Medicine, etc.
Case Study: Personalization

Aggregating information from online and offline purchase data, supermarket savings cards, white pages, surveys, sweepstakes and contest entries, financial records, property records, U.S. Census records, motor vehicle data, automatic number information, credit card transactions, phone records, credit records, product warranty cards, the sale of magazine and catalog subscriptions, and public records.

There are 3.3 billion loyalty program memberships in the US, an average of 29 per household.
Case Study: Personalization

Elite Suburbs (Blue Blood Estates, Winner's Circle, Executive Suites, Pools & Patios, Kids & Cul-de-Sacs).
Urban Uptown (Urban Gold Coast, Money & Brains, Young Literati, American Dreams, Bohemian Mix).
2nd City Society (Second City Elite, Upward Bound, Gray Power).
Landed Gentry (Country Squires, God's Country, Big Fish Small Pond, Greenbelt Families).
Affluentials (Young Influentials, New Empty Nests, Boomers & Babies, Suburban Sprawl, Blue-Chip Blues)
Inner Suburbs (Upstarts & Seniors, New Beginnings, Mobility Blues, Gray Collars).
Urban Midscale (Urban Achievers, Big City Blend, Old Yankee Rows, Mid-City Mix, Latino America).
2nd City Center (Middleburg Managers, Boomtown Singles, Starter Families, Sunset City Blues, Towns).
Exurban Blues (New Homesteaders, Middle America, Red White and Blues, Military Quarters).
Country Families (Big Sky Families, New Eco-topia, River City USA, Shotguns and Pickups).
Urban Cores (Single City Blues, Hispanic Mix, Inner Cities).
2nd City Blues (Smalltown Downtown, Hometown Retired, Family Scramble, Southside City).
Working Towns (Golden Ponds, Rural Industria, Norma Rae-ville, Mines and Mills).
Heartlanders (Agri-Business, Grain Belt).
Rustic Living (Blue Highways, Rustic Elders, Back Country Folks, Scrub Pine Flats, Hard Scrabble).

There are federal and state legal restrictions that prevent the government from building dossiers on individuals without cause. However, these protections do not prevent the private sector from building comprehensive profiles on individuals. The government can then purchase this information from the private sector.
Security and Privacy

Security: freedom from danger, risk, etc.; safety, the right to have some control over how your personal information is collected and used.

Privacy: The state of being free from unsanctioned intrusion

Confidentiality: spoken, written, acted on, etc., in strict privacy or secrecy, information, the unauthorized disclosure of which poses a threat
Cloud Security

- Public cloud’s multi-tenant, dynamic characteristics may put sensitive, or regulated data at risk

- Vendor viability creates strategic risk

- Denial of service attacks could create systemic risk

- A lack of transparency and accountability about security from cloud vendors lowers trust
Cloud Privacy

• Use and governance of personal data

• Laws and guidance ensuring cloud data is being collected, shared and used in appropriate ways

• Legal not Technical

Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit. While security is necessary for protecting data, it’s not sufficient for addressing privacy.
Privacy Considerations

• Standardized rules explaining when and if they may utilize cloud computing and for what data.

• Read the Terms of Service. Then read the Terms of Service again.

• Ensure you are not violating any law or policy, by putting or pulling cloud data

• Consult with your technical, security or corporate governance advisors about the advisability of putting or pulling cloud data

The executive and judicial branches have repeatedly taken the position that data stored in the cloud does not have the same assumptions of privacy and due process as does data stored in your own infrastructure – ACLU report on Cloud Computing and privacy
• Impact of Privacy Regulations – Gerald Spada

• Information Governance – Jason R. Baron

• The Electronic Communications Act – Harley Geiger

• Healthcare Data – Sarbari Gupta

• NIST Insights – Michaela Iorga

• Cloud Provider Panel
Melvin Greer
Senior Fellow
Lockheed Martin
melvin.greer@lmco.com