

**TATA CONSULTANCY SERVICES**

Experience certainty

IT Services

Business Solutions

Outsourcing



# Social Media, Privacy & Security

Brian V. Cummings  
Tata Consultancy Services  
*"Transform with Certainty"*

Monday, August 12, 2013 11:00 a.m.  
Session Number 13703



# Slaying the Social Media Dragon



# Security Definition

**The state of being free from  
danger or threat**

# Information Security Definition



**The preservation of  
information Confidentiality,  
Integrity, and Availability**

# Privacy Definition



**The state or condition of  
being free from observation**

# Breach of Security – Definition



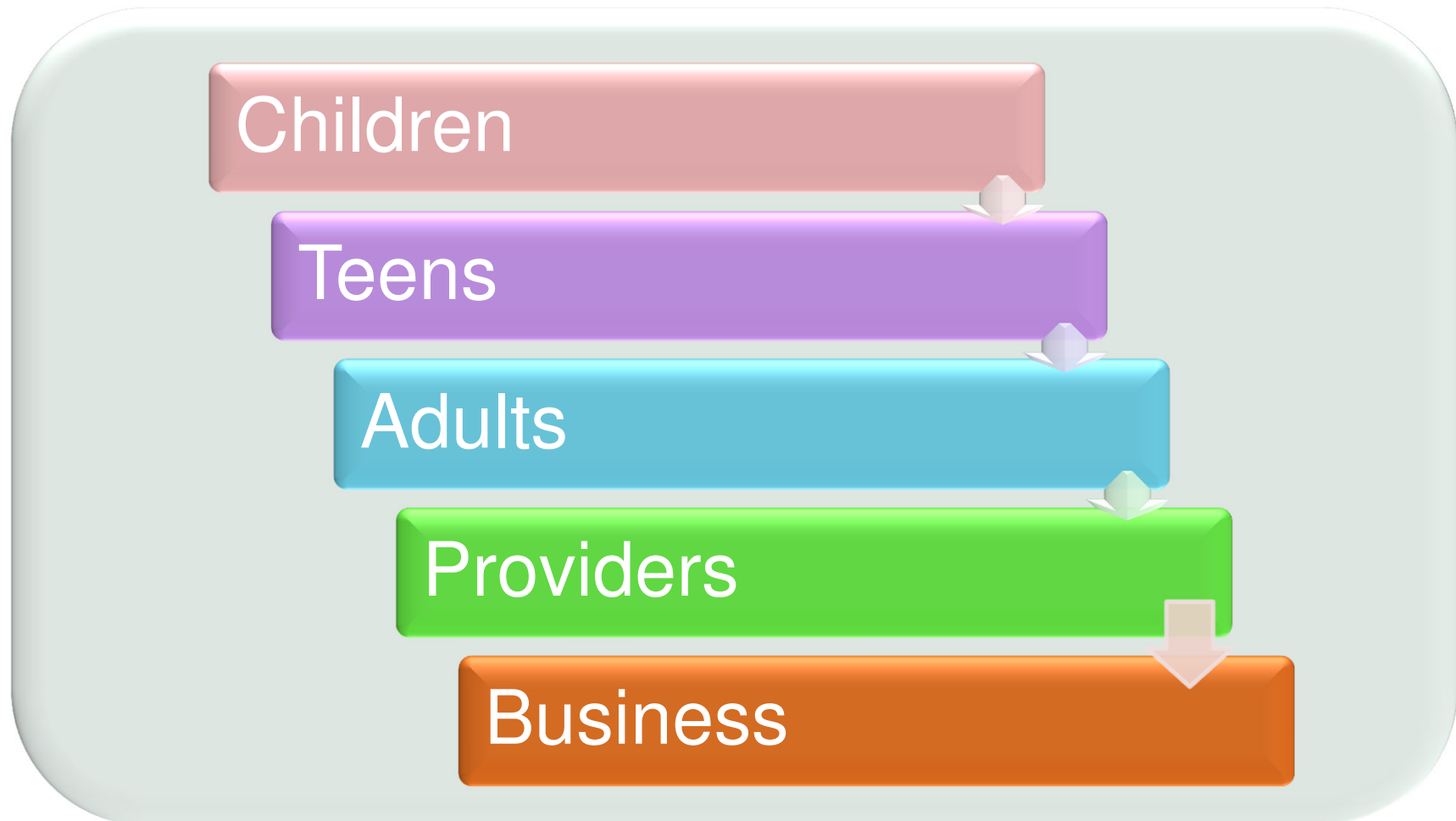
A situation in which someone gets into a place that is usually guarded, discovers information that should be kept secret, or modifies something without authorization.

## Invasion of Privacy – Definition (Legal)



Invasion of privacy is the intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded. It encompasses workplace monitoring, Internet privacy, data collection, and other means of disseminating private information.

# Whose Security & Privacy is at Risk?





# Two Privacy Perspectives

I don't want my Privacy invaded!  
By unknown parties



I don't want you to invade my Privacy!  
Tracking, Bubbling by known entities  
Parental, Employer, Commercial,  
Government Monitoring

# Who's doing what to Whom?

What we do to ourselves

What others do to us

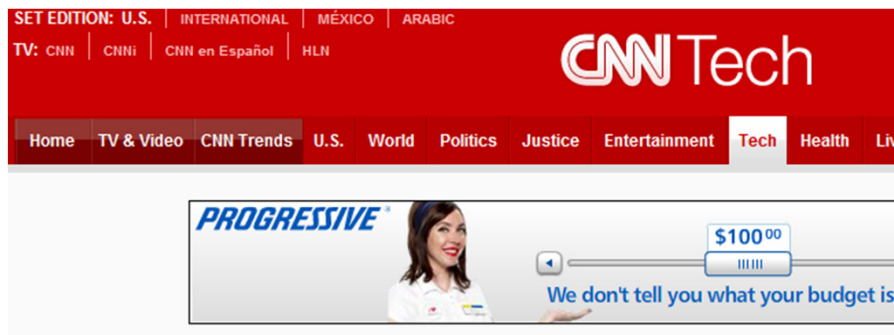
Commercial Tracking/Bubbling

Vendor/Enterprise Monitoring

Government Monitoring

What happens  
on Social  
Media stays  
on Social  
Media, and  
can go Viral !

# The Government!



## Library of Congress digs into 170 billion tweets



By Doug Gross, CNN

updated 12:18 PM EST, Mon January 7, 2013 | Filed under: [Social Media](#)

Osterberg wrote that the library has completed digitally archiving all of the tweets it currently possesses and is now working on how to best make them available to the public. The library already has received about 400 requests from researchers all over the world looking into topics ranging from the rise of citizen journalism to tracking vaccination rates to predicting stock market activity.

The archive promises to keep growing fast. Currently, the library is processing roughly 500 million tweets per day, up from about 140 million daily messages in 2011, according to the blog post.

(CNN) -- An effort by the Library of Congress to archive Twitter posts has amassed more than 170 billion tweets, which the library is now seeking to make available to researchers and other interested parties.

# The Government!



CNET › News › Security & Privacy › Newly leaked NSA program sees 'nearly everything' you ...

## Newly leaked NSA program sees 'nearly everything' you do

The X-Keyscore program, which has been revealed by NSA leaker Edward Snowden, may be the "widest-reaching" intelligence system yet uncovered.



by Don Reisinger | July 31, 2013 8:36 AM PDT

**“...the NSA can essentially see everything a person is doing on the Internet...”**

# Invasion of Privacy – Rereook



Invasion of privacy is the intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded. It encompasses workplace monitoring, Internet privacy, data collection, and other means of disseminating private information.

# On what should we focus?

What we can control

Business Information

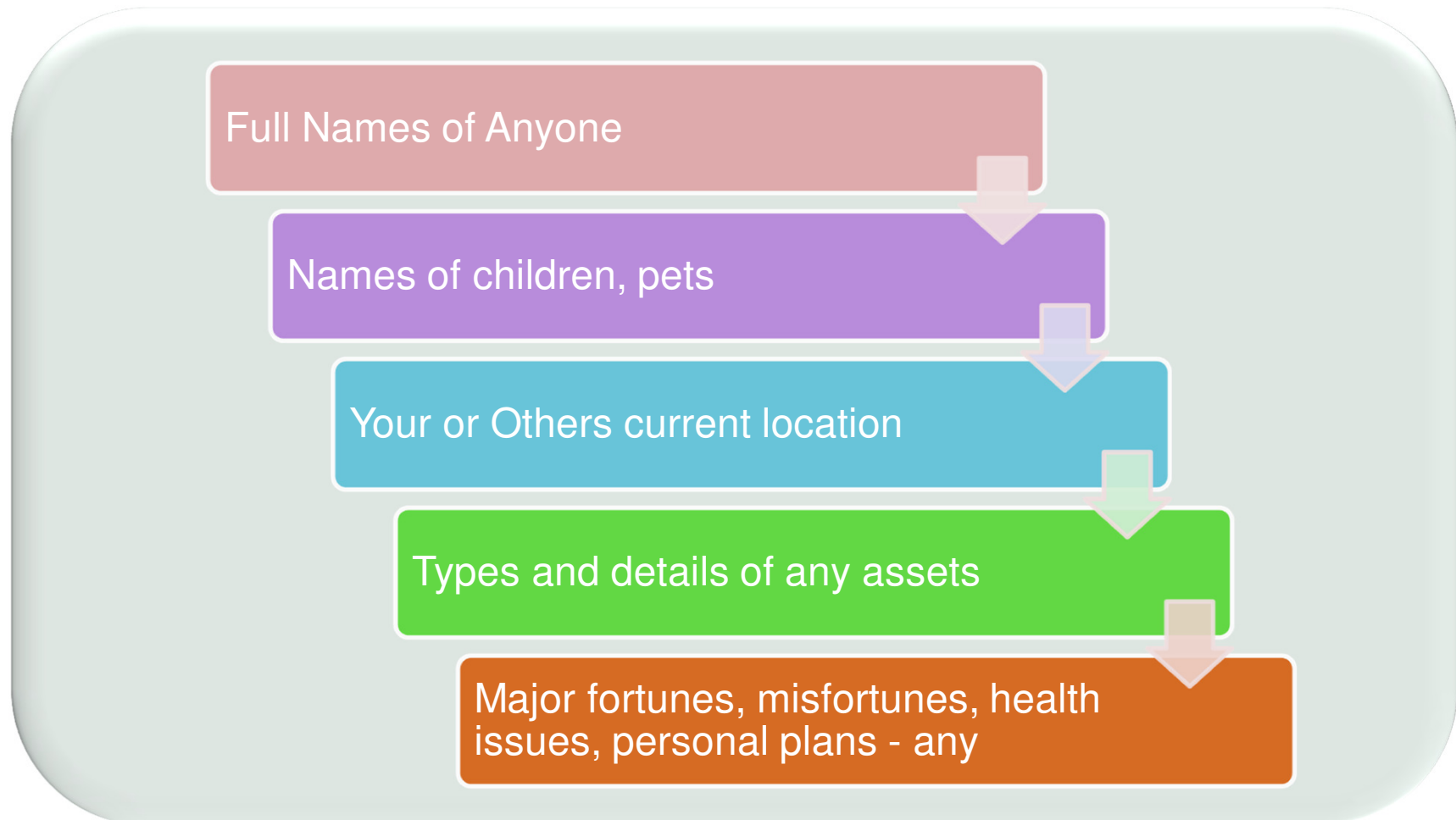
Privacy of Business Constituents

Infrastructure Security

User Behavior



# Users: How much “I” is “TMI”?



## Users: How much “I” is “TMI”?



**If it's socially acceptable to say “TMI” to someone who shares too much, then so it should be with Social Media**



# Users: Going Viral!



*Take a pillow to the roof of an office tower. Rip it open and let the feathers fly.*

*Next, go and try to retrieve all of the feathers.*

*Going “Viral” takes your information to places unknown and unintended, and irretrievably.*

## Users: It all starts with the Networker



**Is it possible to secure the privacy of someone who is too open and sharing?**

*Users have always been and will always be a weak link in the chain of Security & Privacy. They need better and more help to understand when they engage in poor practices.*

*Parents absolutely need to regularly and frequently monitor the social media and networking activities of their children.*

# Users: The T-H-I-N-K Protocol

T: Is it True

H: Is it Helpful

I: Is it Inspiring

N: Is it Necessary

K: Is it Kind

The golden rule of online communication:

Don't post, tweet, blog, email anything on your own behalf or about others that you...

...would not want to see in the newspaper headlines!

# Providers



## Twitter's Tony Wang issues apology to abuse victims

COMMENTS (983)

**The boss of Twitter UK has said sorry to women who have experienced abuse on the social networking site.**

Tony Wang said the threats were "simply not acceptable" and pledged to do more to tackle abusive behaviour.

The apology came as Twitter updated its rules and confirmed it would introduce an in-tweet "report abuse" button on all platforms, including desktops.



Stella Creasy: "An apology [from Twitter] of the matter"

"The abuse they've received is simply not acceptable. It's not acceptable in the real world, and it's not acceptable on Twitter."

"There is more we can and will be doing to protect our users against abuse. That is our commitment."

Minister for Women and Equalities Jo Swinson said unchecked Twitter abuse had been a problem for a long time and she was "delighted" the company was apologising and taking action.

Ms Mayer, Europe editor of Time magazine, said she had yet to receive a personal apology from Twitter, despite contacting the website on Wednesday evening.



Tony Wang said Twitter would do more to tackle abusive behaviour

# Providers: Alcohol-style Warning



## Uber-Blogger Social Networking

**Warning:** Socialize responsibly. Use of social media and networking may result in personal damages including but not limited to: Loss of privacy; abuse; personal embarrassment; ruined friendships; reputation damage; identity theft; government profiling and sanctions; financial loss; and job loss. Remember: T-H-I-N-K

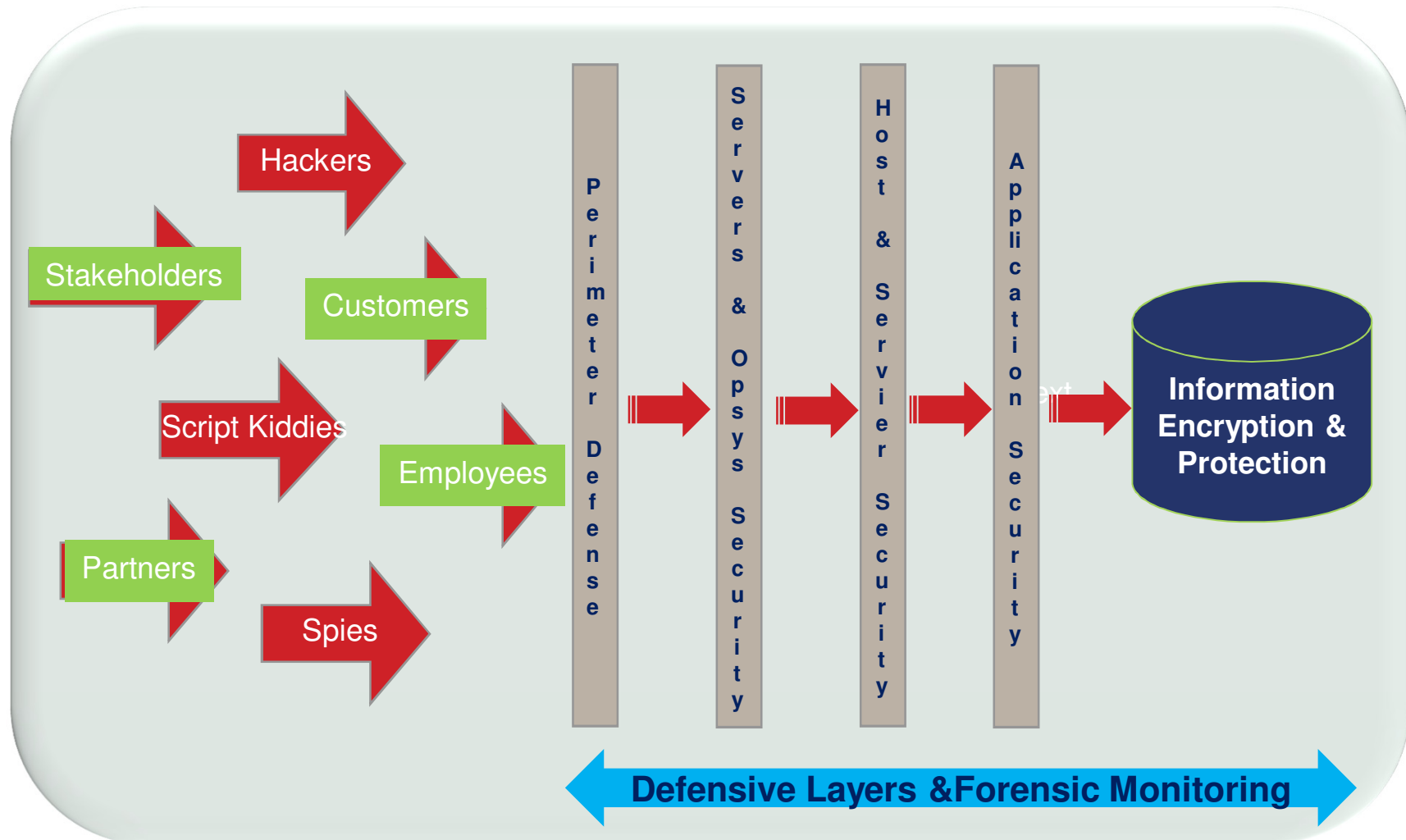
# Providers: Miranda-style Warning



## Uber-Blogger Social Networking

**Warning:** You have the right and the responsibility to manage and limit the personal information you share through this service. Your use of this service and any profile information you provide or any other sharing of your personal information privately or publicly is vulnerable to unauthorized or unintended discovery and can be used against you possibly resulting in minor to significant personal or financial loss. In certain circumstances, you may have the right to legal remedies, but such an effort can be costly and take significant time, providing that you can identify the person(s) or entity responsible for your loss.

# Providers





# Forensic Monitoring

## Captures User Actions

What record(s) did the user touch?

What action did the user take with the record?

## Tamper Proof

Secure capture of activity with encrypted storage into a repository that cannot be modified by any user.

## Maintains Chain of Evidence

Ownership, Security, Control over evidence:

- Collection
- Storage
- Analysis
- Preservation
- Transportation
- Presentation



# Providers: Conclusion

Recognize that they have a primary imperative to help protect their customers private information and communications

Provide robust security capabilities including Strong Authentication and including alerts on weak, moderate, and strong security settings

Advise customers when their profile information or settings have been changed

Help their customers understand when they engage in communications that could be dangerous to their privacy

Encrypt data at rest to provide infrastructure level data protection

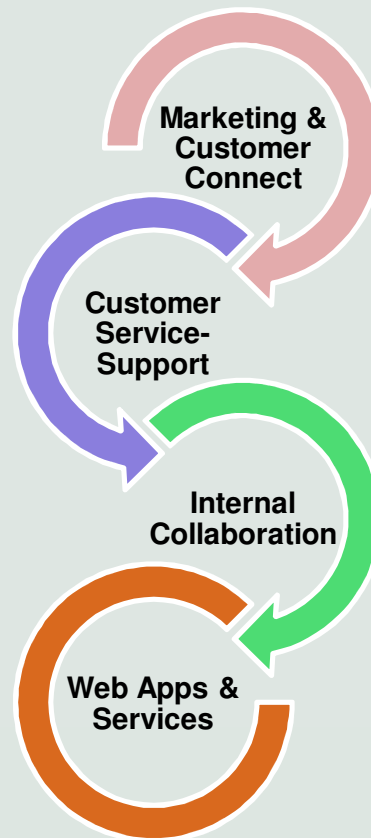
The “Wiretap” Right: Have a right to “just say no” to government intrusion in the absence of a court order that directs the disclosure of specific, discrete information

## Business: RSA Security Breach (2011)



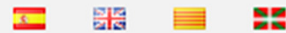
**Started with a spearfishing  
attack against employees  
who were identified using  
Social Media**

# Business



# Yahoo Embraces Brick & Mortar

Home | Latest News | Periodicals



Log

**TheyAreNews.com**

**Business**

Wednesday, July 31 2013

Home | News | Business | Culture | Sports | Science & Technology | Environment | Health

Print Send - +

## Yahoo requires its home-employees to return to the office

The management of Yahoo has required its employees working from home to return to office.

**Monday, March 4 2013**

**Yahoo.-** American computing giant Yahoo has required its hundreds of employees who work from home to return to the office.

This decision has been taken after several research projects taken on board from the company from California revealed that employees boost their creativity when spending time together at the office. However, different studies also emphasize the fact that working from home is equal to a higher level of productivity.

The decision has been taken by the new Chief Director of Yahoo, Marisa Meyer, who has hired by the

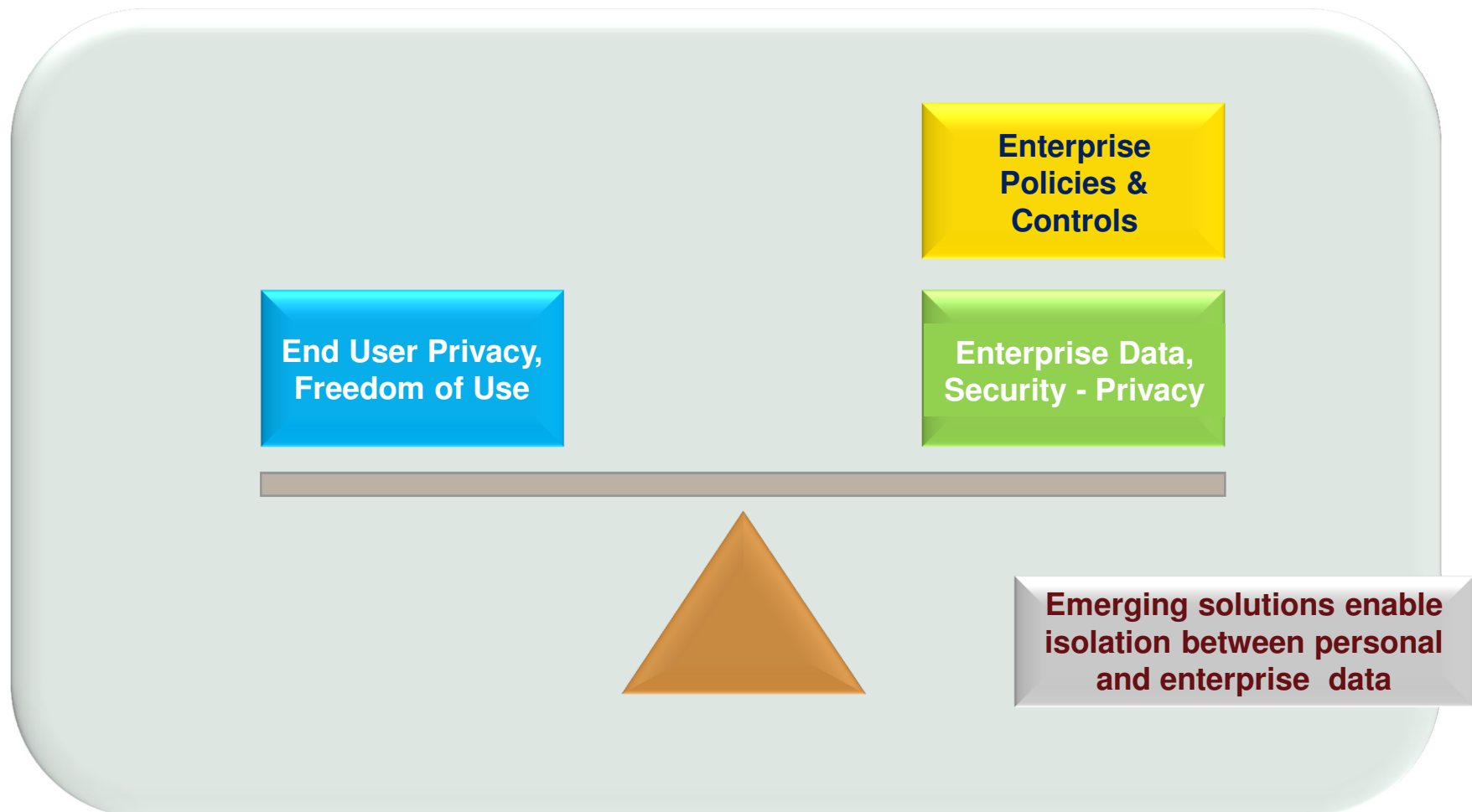


Yahoo! Author: Yahoo! Pressebilder on www.flickr.com

# Global Firm Embraces Social Networking



# BYOD End Point Management



# Business: Conclusion

Need to help their users and customers to network securely and with privacy.

Provide strong end-point management, authentication, and data leak protection within the scope of mobile applications and services.

Link encryption has become a standard. Apps should minimize data volume, retained data, and encrypt data on the end point

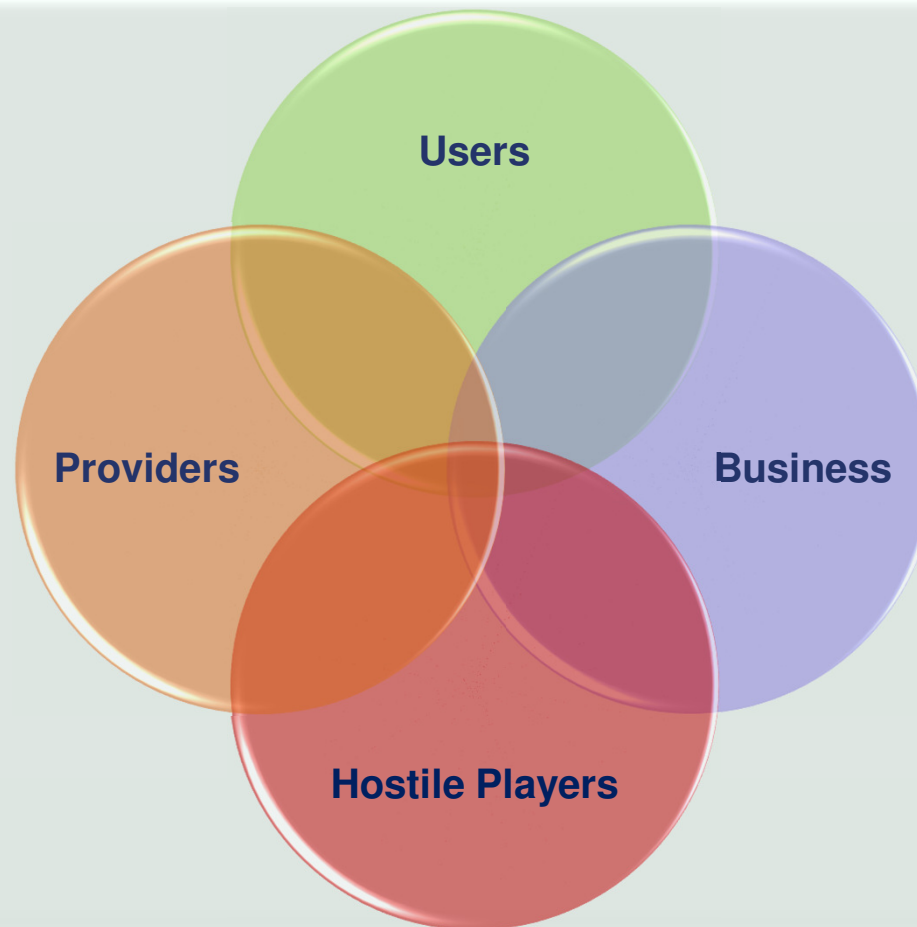
Isolate enterprise data from private data for focused control and protection

Provide total erase capability for lost devices.

Provide partial erase capability for terminations (employees, contractors, etc.)



# Presentation Conclusion



**We socially network  
in a hostile  
environment.**

**All players must do  
their part to assure  
security and  
privacy.**

**Providers and  
Business need to  
provide robust  
security and privacy  
controls.**

**Providers and  
Business need to  
help users network  
responsibly.**





**Thank you!**

