

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Security vs. Privacy: Who is Winning?

SESSION ID: DSP-R01

Christopher T. Pierson, J.D., Ph.D.

EVP, Chief Security Officer &
Chief Compliance Officer
Viewpost

James T. Shreve, J.D.

Attorney
BuckleySandler LLP



Introductions & The Debate Rages On . . .

- ◆ Part 1 – The Debate All Around Us
 - ◆ In the News
 - ◆ Defining Privacy; Defining Security
- ◆ Part 2 – Tensions
- ◆ Part 3 – Convergence
- ◆ Part 4 – What's Next?
- ◆ Part 5 – How to Tackle

The opinions contained herein do not reflect the opinions and beliefs of the author's employers or associated agencies. All content contained herein is for informational purposes only and may not reflect the most current legal developments. The content is not offered as legal or any other advice on any particular matter.



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 1

The Debate All Around Us

In the News

- ◆ Is it a “versus”?
- ◆ Is it a balancing act?
- ◆ Is it a pendulum?
- ◆ Is it based off of harm?
- ◆ Is it proportional?
- ◆ If one wins do we lose?
- ◆ Is the debate all of the above?



Privacy In the News

Government Surveillance



Internet Tracking

Google to Pay \$17 Million to Settle Privacy Case

By CLAIRE CAIN MILLER
Published: November 18, 2013

SAN FRANCISCO — Google agreed on Monday to pay \$17 million to 37 states and the District of Columbia in a wide-reaching [settlement](#) over tracking consumers online without their knowledge.

[Enlarge This Image](#)



Lucas Jackson/Reuters
Eric T. Schneiderman, attorney general of New York, said Google violated not only users' privacy, but their trust as well.

Related

Bits Blog: Google and F.T.C. Set to Settle Browser Privacy Charge (July

The case involved Google's bypassing of privacy settings in Apple's Safari browser to use cookies to track users and show them advertisements in 2011 and 2012. Google has said it discontinued circumventing the settings early last year, after the practice was publicly reported, and stopped tracking Safari users and showing them personalized ads.

The fine is a tiny fraction of the billions of dollars that Google earns in advertising revenue each year. But the case is one of a growing pile of government investigations, lawsuits and punishments related to privacy matters at the company. They include cases involving a social networking tool [called Buzz](#), illegal data collection by [Street View](#) vehicles and accusations of [wiretapping](#) to show personalized ads in Gmail.

Location Tracking

Malls track shoppers' cell phones on Black Friday

CNNMoney

We are conducting an anonymous mobile phone survey to help us enhance your shopping experience.

All data is anonymous. No personal information is collected or stored.

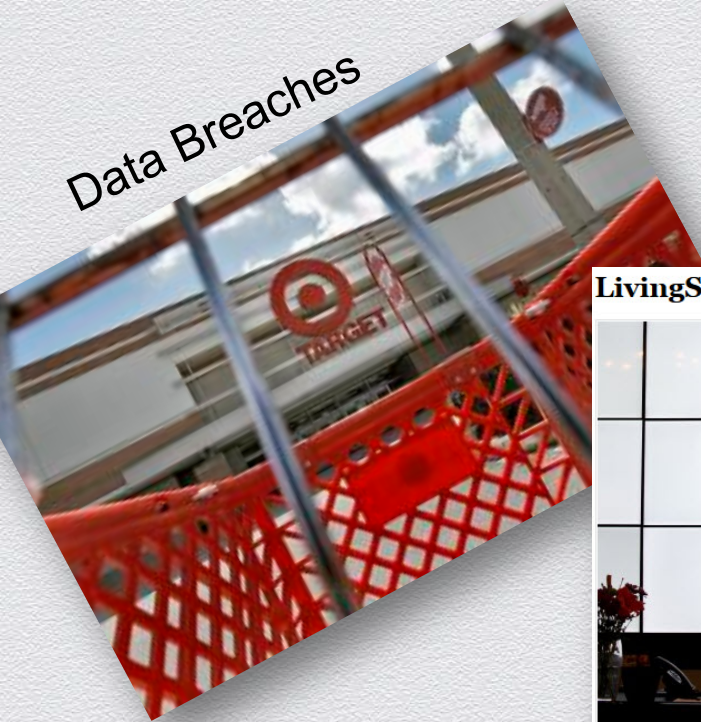
If you have any questions, please visit the Management Office or our website.
www.promenadetemecula.com/info/footpath

#RSAC

RSACONFERENCE2014

Security In the News

Data Breaches



Passwords
Compromised

LivingSocial deals with hacking fallout

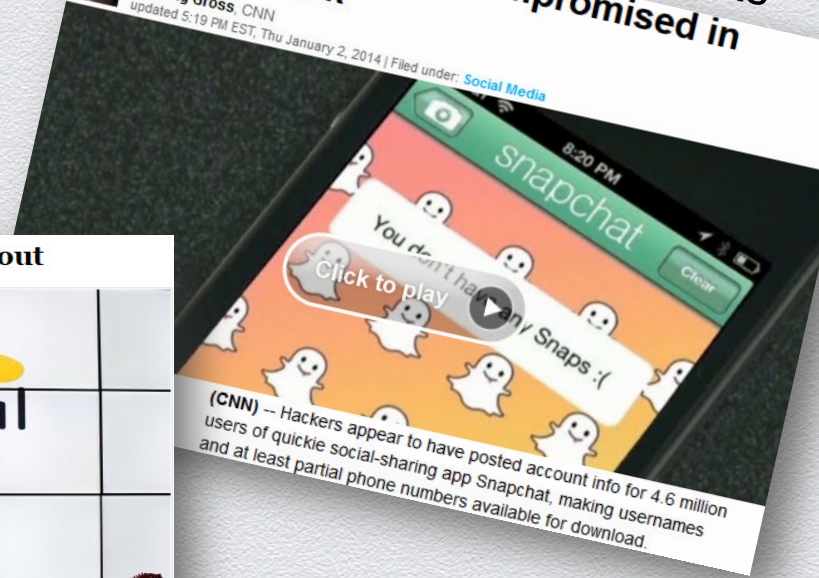


NICHOLAS KAMM/AFP/GETTY IMAGES - View of the reception desk at Living Social in Washington on June 26, 2012.

Compromised Accounts
Millions of accounts compromised in
Snapchat hack



By Doug Gross, CNN
updated 5:19 PM EST, Thu January 2, 2014 | Filed under: [Social Media](#)



(CNN) -- Hackers appear to have posted account info for 4.6 million users of quickie social-sharing app Snapchat, making usernames and at least partial phone numbers available for download.

Defining Privacy

- ◆ As a Human Right
- ◆ Right to be Left Alone
- ◆ Property Right
- ◆ Privacy from Whom?
 - ◆ Government
 - ◆ Companies
 - ◆ Other People



Defining Security

- ◆ Security defined:
 - ◆ Under CIA Triad
 - ◆ Confidentiality
 - ◆ Integrity
 - ◆ Availability
 - ◆ By many CISOs as “not being on the front page of the newspaper”
 - ◆ By absence of a reportable data breach
 - ◆ Data breach laws are privacy laws
 - ◆ Is privacy the lack of a data breach?





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 2

Tensions

Tensions Overall

- ◆ Depends on Risks
 - ◆ Imminence of Threat
 - ◆ Severity of Threat
 - ◆ Likelihood of Threat
 - ◆ Impact of Threat
- ◆ Depends on perceived intrusion
 - ◆ Home, Car
 - ◆ Computer, Phone (i.e. computer)
 - ◆ Social Media, Browsing History



Sharing of Intelligence – Balancing Act

- ◆ Corporate Citizen
 - ◆ Sharing Attacks and Vectors
 - ◆ Partnering with Government
 - ◆ Cybersecurity Executive Order
 - ◆ ISACs
- ◆ Legal/Regulatory
 - ◆ Protection of Intellectual Property
 - ◆ Material Risks under SEC Guidance
 - ◆ Disclosure of Potential Data Breach/Intrusion



Scenario 1 - Tensions with Govt. Surveillance

Surveillance by governments or other state actors

- ◆ Within legal limits?
- ◆ Checks and balances
 - ◆ Rights
 - ◆ Harms
 - ◆ Always Exceptions
- ◆ Example: RFPA



Scenario 2 - Tensions with Personal Monitoring

Monitoring of persons and devices increasing


- ◆ Increased Awareness
- ◆ Assists in Suspect Apprehension
- ◆ Captures Unknowing Persons
- ◆ Storage, Over-Capture, Use not addressed



Scenario 3 - Tensions with Insider Risks

Fraud prevention

- ◆ Use monitoring
 - ◆ Acceptable Use
 - ◆ Data Leakage
 - ◆ HR Harms
- ◆ Location monitoring
 - ◆ GPS Tracking
 - ◆ Fleet Monitoring
- ◆ Employment Concerns




**DON'T BE A TARGET OF
FRAUD**

Waterloo Regional Police Service INVITES YOU
to a free information seminar to make you
aware of potential threats of fraud
in your area and how to protect yourself.

Tuesday, November 27
3:00 pm to 4:00 pm

Linwood Community Centre
Community Hall
5279 Ament Line, Linwood

For more information, contact:
Cst. Andrew Abra, North Division, 519-650-8500, ext 3399
or e-mail: andrew.abra@wrps.on.ca



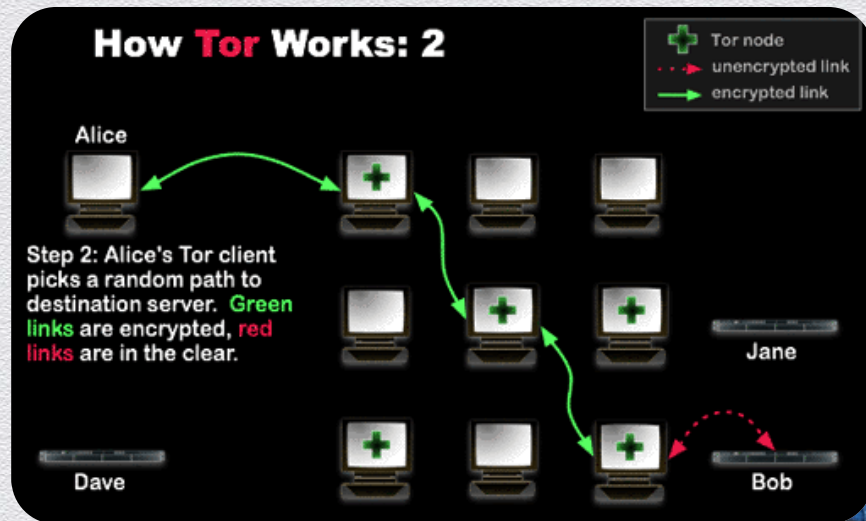
WATERLOO REGIONAL POLICE SERVICE



Scenario 4 - Tensions with Anonymity

Acting anonymously

- ◆ Browsing
- ◆ Commenting
- ◆ Tracking Cookies
- ◆ Marketing
- ◆ Buying and Selling
 - ◆ Desire or need for anonymous payment
 - ◆ Requirements to prevent financial crimes





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 3

Convergence

Physical Security & Access Controls


- ◆ Using Complimentary Technology (Personal Location and Badge)
 - ◆ Tie virtual and physical worlds:
 - ◆ Dual Factor Technology
 - ◆ Proximity Chips/RFIDs for Admin Rights
 - ◆ RFID for physical access
 - ◆ Cameras linked to access points
 - ◆ Increase certainty of identity
 - ◆ Biometrics
 - ◆ Out of wallet questions
 - ◆ Background checks



Monitoring Employees

Preventing insider threats

- ◆ Data Leakage Prevention
 - ◆ E-mail – retention period
- ◆ Proxy Web Traffic
 - ◆ https://
 - ◆ Limit banking, medical



DLA INSIDER THREAT AWARENESS

Indicators of Potential Violence or Terrorist Activity

All DLA personnel are responsible for doing their part in identifying individuals exhibiting indicators of potential violence and reporting appropriate information to their Chain of Command, DOD Law Enforcement, Force Protection Authorities, Counter-intelligence Authorities, or Local Authorities, as appropriate.

The following may indicate an individual at risk of developing into an insider threat:

- Encouraging disruptive/disobedient behavior.
- Expressing hatred or intolerance of American society and culture.
- Expressing sympathy for organizations that promote violence.
- Refusing to deploy for political reasons.
- Associating with terrorists.

Indicators continue on back

*** This list is not all-exclusive nor all-encompassing ***

DLA INSIDER THREAT AWARENESS

Indicators continued

- Browsing or visiting websites without official sanction in the performance of duty that promote or advocate violence directed against the United States or U.S. Armed Forces, or that promote international terrorism or terrorist themes.
- Expressing support for terrorists.
- Expressing outrage against U.S. military operations.
- Expressing a "Duty" to protect a foreign community, when the expressed "Duty" conflicts with current mission and/or U.S. National Interests.
- Possessing or seeking items that would be useful to terrorists, but are not required for the performance of normal duties.
 - Night Vision Goggles or Military GPS Devices.
- Advocating unlawful violence, the threat of unlawful violence, or the unlawful use of force to achieve goals that are political, religious, or ideological in nature.
- Seeking spiritual sanctioning for unlawful violence.

*** This list is not all-exclusive nor all-encompassing ***

Anti-Malware

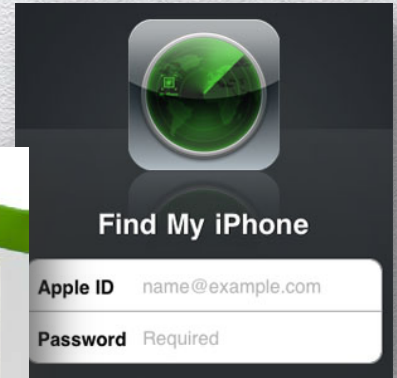
- ◆ Examination of all:
 - ◆ Traffic
 - ◆ Email
 - ◆ USB inserts
 - ◆ Printing
 - ◆ DLP for key fields
 - ◆ Active Recording



Convergence Between Security & Privacy

Monitoring of persons and devices

- ◆ Personal Devices
- ◆ Homes
- ◆ Cars
- ◆ Family Members
- ◆ RFID Assets
- ◆ Travel Itinerary
- ◆ Facial Recognition



Similarities & Differences

- ◆ Input into decisions
 - ◆ Decide to use new product/service
 - ◆ Government – no input
- ◆ Carelessness about policies and secondary use of data
 - ◆ Uproar around certain types of data
 - ◆ Give all personal information away to social media sites, GPS to apps



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 4

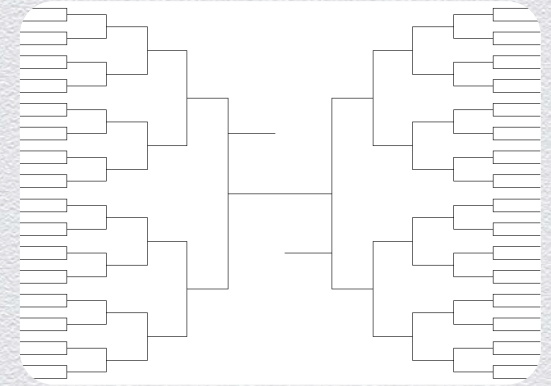
What's Next

Privatization

- ◆ Consumer records kept by private industry
 - ◆ Axiom, Lexis (Reed Elsevier/ChoicePoint), etc.
 - ◆ Much is public data
 - ◆ More privacy pitfalls when aggregated with other data sets
 - ◆ Increasing legislative and regulatory scrutiny

What's Next

- ◆ Consolidation of players in the data marketplace
 - ◆ Fewer companies performing broader functions
- ◆ Big data
 - ◆ Opportunities and concerns for both privacy and security





RSA[®]CONFERENCE2014

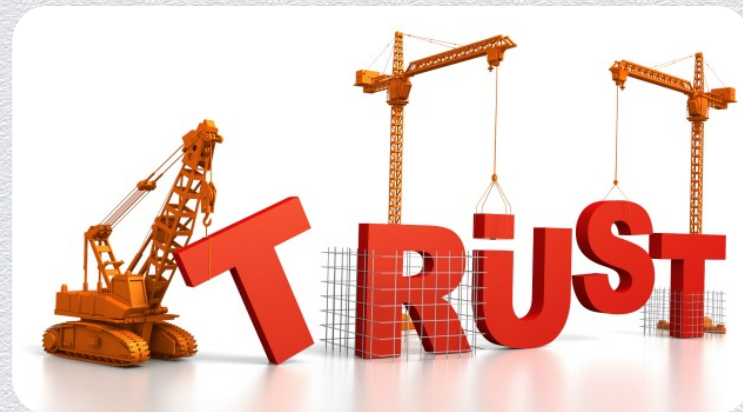
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 5

How to Tackle Privacy & Security

Addressing the Areas of Tension

- ◆ Joint teams
 - ◆ Security, Privacy, Legal, Operational, Compliance
- ◆ Over-communication of the issues
 - ◆ Advocates and decision makers
 - ◆ Awareness through open discussion
 - ◆ Establishment of process to vet issues
 - ◆ Inclusion of external participants
- ◆ Example: BYOD policies
 - ◆ Need for “brutal honesty”

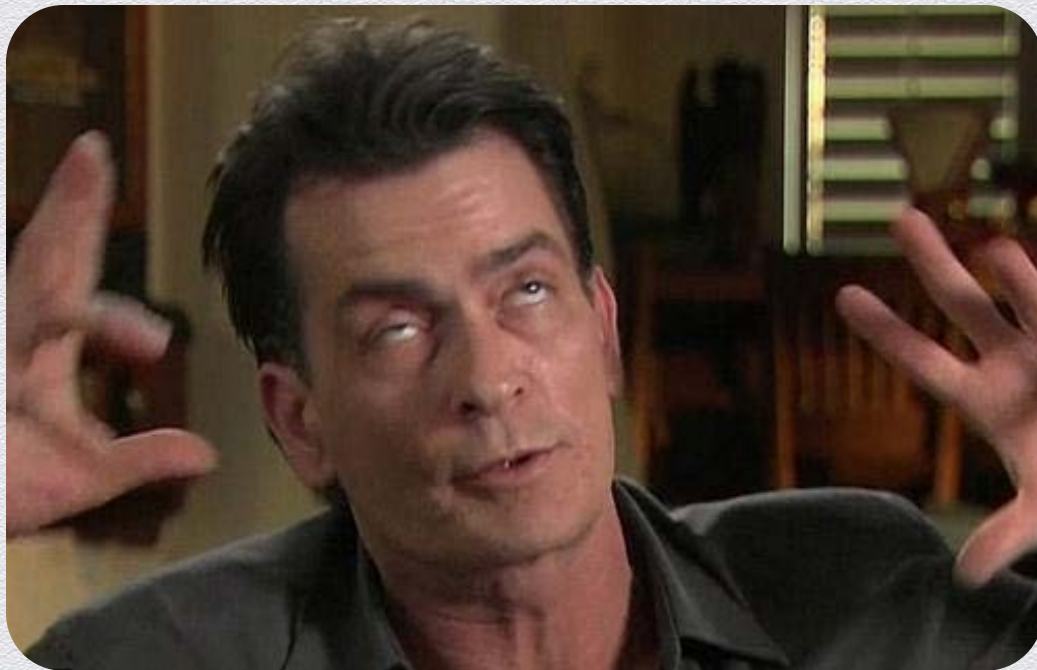


The Need for Checks and Balances

- ◆ Division of authority
 - ◆ Clear roles
 - ◆ Value in certifications
- ◆ Advocates/champions for each side
- ◆ No unwatched watcher or unchecked decider
- ◆ Act as though the decision making will become public
- ◆ Proper structure more likely to consistently produce good results than “doing the right thing now”



Who is Winning?



Contact Information

Christopher T. Pierson

Viewpost

EVP, Chief Security & Chief Compliance
Officer

407.515.6727

cperson@viewpost.com



James T. Shreve

BuckleySandler LLP

Attorney

202.346.4314

jshreve@buckleysandler.com



Additional Links

- ◆ Privacy - <https://www.privacyassociation.org/>
- ◆ SecureWorld Blog - <http://www.secureworldexpo.com/>
- ◆ Privacy and Civil Liberties Oversight Board - <http://www.pclob.gov/>