Social and Mobile and Clouds, Oh My!

Emerging Privacy Issues

&

The Challenge of Globalizing Technology

Presented by

Joseph I. Rosenbaum

Partner & Chair

Global Advertising Technology & Media Law Practice

Reed Smith LLP

IAPP Canada Privacy Symposium 2012
10 May 2012; Toronto, Ontario, Canada
Is it the Information or Control of the Information that is Game Changing?

http://www.youtube.com/watch?v=oKprr3tEBew
Pay no attention to that man behind the curtain!

The emergence and convergence of innovative digital technology

Social Networks
Mobile Platforms
Cloud Based Computing

continues to challenge our legal & regulatory systems, creating confusion amongst and between search, surveillance, privacy & data protection

“What chance has the ignorant, uncultivated liar against the educated expert? What chance have I . . . . against a lawyer?” Mark Twain, “On the Decay of the Art of Lying,” 1882
Technologies Can Change the Game

US Nuclear Chain of Command

- President
- Secretary of Defense
- Unified Combat Commanders

Engineer who installed the red button
Changing the Tires on a Moving Car?

Governmental intervention may be necessary to protect consumers from abuse, but can a concretized, codified piece of legislation remain relevant as innovation and technology remains unpredictable?

Consumer privacy, data protection and surveillance have always been context specific and continues to evolve. How can they be harmonized across nations, cultural and local boundaries?

Distinctions between desktop computing and home entertainment become irrelevant; Mobile devices will increase the ability to capture consumer information; Cloud computing makes content, application programming and processing accessible anywhere, anytime, effectively outsourcing the evolution of technology making distinctions among devices irrelevant;

Business models and legal frameworks continue to change; metrics and quantification methodologies continue to be debated; roles of advertisers, agencies, media buyers, broadcast and publishing networks, as well as ISPs, search engine, browser and web hosting companies – the technology players – continues to change.
Convergent Digital Technology is Transforming

Trademark and Service Mark Protection into Brand and Reputation Management

Copyright Protection into Artistic Expression and Innovation

Search, Context & Location Behavior into Surveillance, Privacy and Data Protection
Cloud Computing is: “Dynamically scalable virtualized information services delivered on demand over the Internet.”

Cloud Computing

What Me Worry?

Privacy & Data Security
Regulatory Compliance
Intellectual Property
Performance Metrics
Jurisdiction
Litigation & Government
Termination
Tax
Business Continuity
Insurance

Antitrust – Competition
Pricing
Shared Applications
Shared Infrastructure
Shared Data Resources
Competitive Issues
Enforcement Issues
&
The 800 Pound Gorilla in the Room:
Interoperability
Availability & Access

iapp
ReedSmith
Cloud Trends to Watch

Government regulation, perhaps akin to FCC or PTT type interexchange, availability and data regulation, as well as tax considerations are likely to emerge.

Telecom providers will close the gap between public and private cloud environments

Cloud providers and infrastructure builders will invest in security and compliance management

Clouds are inherently multi-jurisdictional, interoperable and subject to varied governmental legislation, regulation and judicial oversight.
“The web is more a social creation than a technical one. I designed it for a social effect – to help people work together – and not as a technical toy.”

Traditional Media is Passive

Social Media is Different . . .

- Attract
- Monitor
- Engage
- Respond
- Interact
- Transact
- React
- Retain
- Improve

"Didn't you get my e-mail?"
Social Networking Has Changed the Balance of Power

Content    Context    Control
Enable Conversations
Influence Conversations
Monitor Conversations
React to Conversations
Monetize Conversations

http://www.youtube.com/watch?v=D3qltEtl7H8
It’s All About the Conversation
Most social networks have no way to qualify friendships and if they do, they are generally ineffective, ignored or rarely used.

Individuals are much more relaxed about interacting and sharing information with strangers in an online environment than in person.

Social networks provide a game-like atmosphere. Collecting friends, building large followings, game participants, networks, circles, common interest and activity groups – even people ‘ing’ is considered desireable.

Social Media Can Target Demographics & Individuals

- Age
- Preferences
- Gender
- Relationship Status
- Activities
- Location
- And more . . . . 
Peer to Peer Social Climbing?

Given that studies consistently show consumers trust other consumers – their peers – more than advertisers (and government) when it comes to product and service recommendations, does it come as any surprise that ‘influence’ peddling has now been extended to consumers?
Social Media Participants Express Concern Over Privacy

**BUT**... *The Wall Street Journal*, just a few days ago, reported that in the Proceedings of the National Academy of Sciences, "Talking about ourselves--whether in a personal conversation or through social media sites like Facebook and Twitter--triggers the same sensation of pleasure in the brain as food or money." Scientists have found that bragging and boasting feels so rewarding, at the level of brain cells and synapses, we can't help sharing our thoughts.

(WSJ; D1; *Science Reveals Why We Brag So Much*, May 8, 2012, Robert Lee Hotz)
Digital Technology Combined With Social Networking Shifts Social Expectations

We traditionally (“normally”) assume that our conversations are private and made public only when one or more of the participants takes some affirmative action.

In the online environment conversations are public by default and and you have to work to make them private

BUT

we are still confused!
You are being exposed in new ways and...
Managing Social Reputations
Is Now an Integral Part of Privacy Expectations

Is anyone electable anymore?
If I Only Had A Brain . . . .

The Rise of Mobile

- Discount Coupons
- Tickets to Events
- Newspapers & Magazines
- Web Access
- Search & E-mail
- Text, Image & Voice
- Payments
- Books
- Currency
- Bluetooth
- ID & Security
- GPS
- TV, Radio & Movies
- Music
- Prescriptions
- DVR
- Podcasts
- TV, Radio & Movies
- Music
- Prescriptions
- DVR
- Podcasts
Web Technology, GPS, RFID, Bluetooth, QR Codes, Augmented Reality and Virtual Reality
Further Blur Distinctions Between Privacy, Data Protection, Search and Surveillance

- User Search & Input
- Social Networking with Location Sharing
- Geo Targeting – Location, Location, Location
- Coupling Location with Context
- Coupling Location with Behavior
- Coupling Location with Content
- Location Sharing Capabilities
Rise of Mobile: A Historical View

Effective Regulation
Mobile Is . . . .

- Personal – always attributable to an individual
- Pervasive – one screen unites everything
- Instant – here and now
- Local – it goes where you go

First thing you check when you wake,
last thing you check before going to bed!

Within reach over 80% of every day ! !

92% of owners cannot get through a typical day without using their mobile phone


Why do you think they call it a ‘sell’ phone ?
‘Checking in’ is motivated by value exchange: Deals, information, interaction, bragging rights, notariety
Wiretapping refers to the contemporaneous simultaneous or recorded eavesdropping of actual conversations as they occur.

“Location technology” or mobile surveillance refers to the use of a “pen register” or “trap-and-trace device” to identify the physical location of a specific device at an exact moment in time.

Past: Historical data

Present: Ping data

Future: Tracking movement and usage patterns, mapping both individual and group traffic, it may be possible to predict statistically where people, and perhaps a particular person, is going to be!
Surveillance – the strong monitoring the weak; the powerful watching ordinary folks, the rich and government officials, tracking and tracing each other.

Sousveillance – a term coined by Steve Mann, a professor at the University of Toronto, that refers to inverse surveillance - ordinary citizens monitoring, watching and recording the strong and the powerful.

Coveillance – peers stalk and monitor and watch their peers.

Counter surveillance – the practice of avoiding surveillance or making surveillance difficult.
Yeah, There’s an App for That . . .
Lions and Tigers and Bears, Oh My!

Content = Intellectual Property

Context = Search, Surveillance

Control = Privacy & Data Protection

Control = $$$$$$$
Classic Privacy Rights

“Privacy is the right to be alone--the most comprehensive of rights, and the right most valued by civilized man.” Louis D. Brandeis

Intrusion on solitude or private affairs
Public disclosure of embarrassing private facts
Publicity placing one in a false light
Appropriation of name or likeness for commercial advantage
A personal ‘privacy’ right, which has morphed into a property right

Factors v. Pro Arts, 597 F.2d 215 (2d Cir. 1978) Confirmed property right as surviving death of celebrity (Elvis Presley)
Privacy Worldwide

Legal Overview

UK and 47 European States:
Article 8 of the European Convention on Human Rights

Australia:
Privacy Act of 1988

Canada:
Personal Information Protection and Electronic Documents Act 1995-2004
An Act Respecting the Protection of Personal Information in the Private Sector (Quebec)
The Personal Information Protection Act (British Columbia)
The Personal Information Protection Act (Alberta)
The Personal Health Information Protection Act (Ontario)

US:
Multiple Federal Laws in 14 categories
Multiple State Laws (Hint: California has over 80)
US Legal Landscape:

Representative Privacy Laws

U.S. Constitution, 4th Amendment
Privacy Protection Act of 1980 (42 U.S.C. 2000aa);
Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 note);
E-Government Act of 2002 (44 U.S.C. 9501 et seq.);
Defense Production Act of 1950 (50 U.S.C. App. 2061 et seq.)
Federal Trade Commission Act
Communications Act Federal Communications Commission
State Consumer Protections, Unfair and Deceptive Acts or Practices Statutes, Privacy & Identity Theft Statutes
Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”) and corresponding FTC rules
The Telephone Consumer Protection Act of 1991 (“TCPA”) and the corresponding FCC rules
Do-Not-Call Rules
Customer Proprietary Network Information (“CPNI”) rules
And of course there are Industry Self-Regulatory Guidelines – e.g., ANA, IAB, MMA, DMA, AAAA, CARU, CTIA.
1996-Health Insurance Portability and Accountability Act (HIPAA)
1974 The National Research Act
1970 Bank Secrecy Act
1998 Federal Trade Commission
1999 Gramm-Leach-Bliley Act-GLB
2002 Sarbanes-Oxley Act-SOX
2003 Fair and Accurate Credit Transactions Act
1986 Electronic Communications Privacy Act-ECPA-pen registers
1986 Stored Communications Act-SCA
1978 Foreign Intelligence Surveillance Act (FISA)
1984 Cable Communications Policy Act
1986 Electronic Communications Privacy Act (ECPA)
1994 Digital Telephony Act - Communications Assistance for Law Enforcement Act-“CALEA” 18 USC 2510-2522
2005-6 CALEA expansions
1974 Family Educational Rights and Privacy Act-FERPA
2001-US Patriot Act – expanded pen registers
2005 Privacy Act - Sale of online PII data for marketing
1974 Privacy Act
Privacy in an Analog World
On the Internet, nobody knows you’re a dog.

Peter Steiner, published by The New Yorker on July 5, 1993
How Quickly Our Expectations of Privacy Change

1988: In the battle to block Robert Bork from the Supreme Court, someone leaked his video rentals. In response, Congress banned video stores from disclosing titles of films people rent.

"You have zero privacy anyway. Get over it."
Scott McNealy, Chairman, Sun Microsystems, 1999

"The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy."
Larry Ellison, CEO, Oracle, 2001

2008: A federal judge hearing a $1 billion copyright complaint by Viacom ordered YouTube to turn over online records (computer addresses) used to watch videos. The judge dismissed privacy concerns as "speculative"

[P.S. The judge graduated law school before the photocopier was invented!]
Privacy in a Digital World
For Those of You Zealously Guarding Your Privacy . . . .

If I search for you on Google and don’t find you . . . do you exist?
Cookies

Cookies can only be set and read by the same domain

- A cookie set on mail.yahoo.com can be read by my.yahoo.com
- A cookie set on yahoo.com cannot be read by washingtonpost.com

Web coding language (HTML) allows for multiple domains to be shown in a browser on a single webpage

- An ad is usually served on a primary site by a hosted third-party provider, such as Atlas or DoubleClick
- This ad gets shown on a site like nytimes.com through a seamless “window” that is actually a view into an Atlas/DoubleClick “webpage”
- Other than ads, content from third parties, including news wires, widgets, stock information, etc, can be displayed in the same way
- When the third-party ad/content shows up in the browser, the third-party domain can read its own cookies, even though the browser location bar says the webpage being visited is another domain (http://www.washingtonpost.com vs. http://www.doubleclick.net)
“Holes” in the washingtonpost.com are filled with ads. These ads are actually on other “sites” and that is how cookies from other sites can be set/read on the washingtonpost.com
BUT – Most Secure Sites Use Server-Based Login Software

Sites that require logins, including web mail, news content, banking, etc, can track almost all user activity and link it directly to any user-entered profile data.

This software cannot be stopped from tracking user activity by having the browser block cookies.

Data collected by logged-in environments cannot be shared with other domains through a browser.
On the Internet, everybody knows you’re a male beagle who prefers dry dog food, sneaks into the master’s bedroom, lying on the bed watching cable and who wears a specially designed, hypo-allergenic flea collar.
What Does Privacy Mean Today?

References to privacy are consistently and persistently used to refer to everything from true privacy, to data protection, digital search, video cameras, wireless access, open ID and browser data collection, surveillance, data matching, data mining, profiling, geo-targeting, behavioral data gathering, cookies, web beacons, invisible GIFs, web bugs, online and mobile, transactional activity, data sharing, processing, identity theft and compromised databases, to name the most obvious.

In the exchange of value, real or perceived by the consumer, privacy has become synonymous with the right to exploit the value of information about that individual, her or his relationships, activities, behaviour and preferences, whether or not personally identifiable and whether or not sensitive or confidential.
It’s All About the Information!!!
“Privacy” Appears Paradoxical

People SAY they cherish privacy as a right and principle. BUT in their daily lives, they often act in ways that allow, even encourage, others to monitor and track them, to know their preferences, exactly where they are and what they are doing.

People express generalized anxiety about the consequences of inappropriate personal information disclosure: to businesses; to people they don’t know; to computer hackers; to data mining and companies that analyzed their information in order to display ads based on the information obtained . . .

BUT in their daily lives, they often disclose information virtually indiscriminately to strangers, both individual and commercial, and most people aren’t actually sure that any actual harm has occurred.
Is it a Paradox or Simply Incorrect Attribution?

People SAY they care about the pervasive collection of information about them and ‘dossier effect’ of the web . . .

BUT most people don’t opt out, don’t turn off cookies, don’t read privacy policies and don’t know or take the time to try and understand tracking or information sharing policies of the websites with which they interact.

People SAY they would prefer to limit the amount of information that is easily obtained about them. . .

BUT most people seem disturbed if they search for themselves and don’t find much, will almost always search for information about an individual they are planning to meet or speak with, rarely change their privacy settings and almost never define their relationships and information sharing within those relationship by personal knowledge.
We Now Use the Term ‘Privacy’ To Mean Many Things

**Anonymity/Pseudonymity:** A persona, but ostensibly neither data nor behavior identifiable with the real individual behind the persona.

**Confidentiality:** Control over the use of information; protection from the collection, sharing and abuse of information about them.

**Security:** Protection from disclosure, impersonation and identity theft in ways that can cause harm.
People ascribe importance to some types of information and not to others. Often the degree of perceived required protection may vary by age, status, culture, societal norms, nationality, gender and a variety of factors.

BUT most people (and regulators) agree that health and financial information, information about children, personal and family secrets should be protected.

Almost everything else is open for discussion!
Context Is Important,
But Not Always in the Same Way to Different People

People are often willing to forego some degree of privacy and control and even the exploitation of information, IF, for example, it would help to:

Combat pedophiles and child predators;
Prevent terrorism and other criminal activity;
Make public places and transportation safer;
Prevent or detect stalking.

People also voluntarily forego some degree of privacy in order to obtain some commercial or personal benefit.

Highly Individualized and Context Sensitive
Does This Make You Happy
or Make You Nervous?

Pizza Palace ‘30 Minutes or it’s Free’

Want to stop this
from happening?

Take Action!

Replay the movie?
I Have a Feeling We’re Not In Kansas Anymore

Privacy is no longer just about our right to be let alone or to prevent facts and observations about us from being perceived, used or shared.

Our legal and regulatory systems have become schizophrenic and inconsistent in our use of terminology and in distinguishing between personal and personally identifiable information, differences in how we refer to the various capabilities and platforms spawned by innovative digital technology.

It is indeed, all about the information – the right to control, exploit and obtain value from information about us . . . even if that information is publicly available and even if it is neither confidential, nor sensitive.

Social and Mobile and Clouds, Oh My!

Sometimes I lie awake at night and ask “Where have I gone wrong?” Then a voice says to me, “This is going to take more than one night.” Charlie Brown, from Peanuts, by Charles Schulz
Resources—More Information

www.reedsmith.com/networkinterference

Coming Soon:
Mobile Mayhem: A Legal Guide to a Wireless World

What I’ve Been Reading
An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government, and Other Goliaths
Glenn Reynolds

Database Nation: The Death of Privacy in the 21st Century
Simson Garfinkel

http://www.reedsmith.com/cloudcomputing
Thank You!

Questions??

Joseph I. Rosenbaum
Partner & Chair
Advertising Technology & Media Law Practice
T: 212 702—1303  M: 646 522-0083
jrosenbaum@reedsmith.com
www.LegalBytes.com