

# Privacy is Dead Now What?

Mark D. Rasch  
Director, CyberSecurity and  
Privacy Consulting  
[MRasch2@csc.com](mailto:MRasch2@csc.com)

# Privacy Generally

- No General Legal Protections for Privacy
- Hodgepodge of Federal and State Laws
- Deal With Particular Subject Matters
- Constitutional *implied* or *penumbra* rights
  - Fourth Amendment Search and Seizure
  - Fifth Amendment Self Incrimination
  - Ninth Amendment – delegation
  - Griswald v. Conn., Doe reproductive rights cases
  - “right to be left alone”

# What do we MEAN by Privacy?

- Right to be left alone
- Right to integrity of person
- Right to CONTROL of data collected
- BUT
- Who OWNS the data about us?
- Who has a right to access?
- What circumstances?

# Threats to Privacy

- Data Collection
  - Voluntary collection
  - Compelled collection
  - “Ambient” information
  - “Public” information
  - Surveillance
- Data Dissemination
- Data non-anonymization
- Data Aggregation
- Subject profiling

# The Concept of Privacy

- Privacy: Moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations
- Information privacy: Includes both the claim that certain information should not be collected at all, as well as the claim of individuals to control the use of whatever information is collected about them

# E-commerce and Privacy

- Major ethical issue related to e-commerce and privacy: Under what conditions should we invade privacy of others
- Major social issue: Development of “expectations of privacy” and privacy norms
- Major political issue: Development of statutes that govern relations between recordkeepers and individuals

# Information Collected at E-commerce Sites

- Personally identifiable information (PII): Data that can be used to identify, locate, or contact an individual
- Anonymous information: Demographic and behavioral information that does not include any personal identifiers
- Almost all e-commerce companies collect PII and use cookies to track clickstream behavior

# What Information Do You REALLY Collect

- Name, Address, Order, E-Mail, Credit Card
- Tangential information
  - Browsing
  - Browser
  - Settings – references
  - IP Address – privacy?
  - Location Data
  - Type of Device
  - Cookie Data
  - Aggregated information



# Adding Data to What you Collect

- Data Analysis of YOUR data
- Data analysis of data subject
- Behavioral profiling
- Data sharing
- Adding “public” data – de-anonymizing
- Adding Google Street View information
- Adding Facebook and Twitter Feeds
- Geotracking (geolocation over time) – Loopt, 4Square

# Profiling and Behavioral Targeting

- Profiling: Creation of digital images that characterize online individual and group behavior
- Anonymous profiles: Identify people as belonging to highly specific and targeted groups
- Personal profiles: Add personal identifiers
- Advertising networks can:
  - Track both consumer behavior and browsing behavior on the Web
  - Dynamically adjust what the user sees on screen
  - Build and refresh high-resolution data images or behavior profiles of consumers

# Legal Protections for Privacy

- May be explicitly granted or derived from constitutions (U.S., Canada, Germany)
- May also be found in common law (U.S, England)
- In U.S, also found in federal and state laws and regulations

# Informed Consent

- Consent given with knowledge of all the material facts needed to make a rational decision
- Two models:
  - Opt-in
  - Opt-out
- Many U.S. e-commerce firms merely publish information practices as part of privacy policy without providing for any form of informed consent

# Statutory and Regulatory Protections of Online Privacy

- In U.S., Federal Trade Commission has taken lead in conducting research and recommending legislation to Congress
- FTC Fair Information Practice Principles (1998):
  - Notice/Awareness (Core)
  - Choice/Consent (Core)
  - Access/Participation
  - Security
  - Enforcement

# FTC's Fair Information Practice Principles

Table 8.5, Page 497

TABLE 8.5	FEDERAL TRADE COMMISSION'S FAIR INFORMATION PRACTICE PRINCIPLES
Notice/Awareness (Core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data
Choice/Consent (Core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/Opt-out must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulation.

# FTC Recommendations Regarding Online Profiling

Table 8.6, Page 498

TABLE 8.6	FTC RECOMMENDATIONS REGARDING ONLINE PROFILING
PRINCIPLE	DESCRIPTION OF RECOMMENDATION
Notice	Complete transparency to user by providing disclosure and choice options on the host Web site. "Robust" notice for PII (time/place of collection; before collection begins). Clear and conspicuous notice for non-PII.
Choice	Opt-in for PII, opt-out for non-PII. No conversion of non-PII to PII without consent. Opt-out from any or all network advertisers from a single page provided by the host Web site.
Access	Reasonable provisions to allow inspection and correction.
Security	Reasonable efforts to secure information from loss, misuse, or improper access.
Enforcement	Done by independent third parties, such as seal programs and accounting firms.
Restricted collection	Advertising networks will not collect information about sensitive financial or medical topics, sexual behavior or sexual orientation, or use Social Security numbers for profiling.

# Data Collection

- Website collection
  - EU Data Privacy Laws
  - US “Safe Harbor” Provisions
  - FTC Section 5 “false and deceptive trade practices”
    - Lilly Case
    - Do what you say – say what you do
    - Google Doubleclick – finalized March 10, 2008
  - Privacy policies



# Who owns collected data?

- Data Subject?
- Data Collector?
- Sale of Data?
- Data Sharing?
- Profiling?
- Mining?

# Anonymity

- Anonymous speech
- Postings
- Blogging
- Takedown notices
- Copyright infringement
- P2P
- Defamation?
- As a general rule – anonymity loses

## Fourth Amendment

- “The Right of Persons to be secure in their persons, places houses and effects shall not be abridged, no warrant shall issue except upon a finding of probable cause issued by a neutral and detached magistrate..”

# Katz v. United States

- Fourth Amendment protects PERSONS not places
- Two part test
  - Does the person have a subjective expectation of privacy? (DO THEY THINK IT IS PRIVATE?)
  - Is that expectation of privacy objectively reasonable?

# Fingerprints or DNA

- Useful tools
- Who Owns it
- Any Expectation of Privacy?
- Any limits on use?
- No law on it..

## Some Practical Advice

- Consider the privacy implications of what you do
- Business models
- Implementation
- Security and Privacy Relationship
- “can we protect it?”
- Not “can we” but “should we?” – “is this a good idea?”
- Unintended uses – unintended consequences.

# The risks of non-compliance

## Privacy regulators' action

- Inspection and audit
- Enforcement (e.g. stop processing, stop transfers, close databases)
- Prosecutions and sanctions – individual employees and/or Accenture

## Individuals' action

- Compensation - in many countries, individuals have a right to sue for violations
- Complaints

## Bad publicity

- Brand erosion
- Negative impact on client work
- Loss of revenue and decline in share price

# Privacy Principles





# Basic Privacy Principles

- 1. Is There A Lawful basis for Collection/Use-** Use of personal data is not allowed unless there is a specific, lawful basis for it. For example:
  - Legal requirements (tax ID number to meet tax reporting laws)
  - Consent of the individual (photographs on an website or for collection of sensitive personal data)
  - Necessary for performance of employment contract (performance data, banking details to pay the salary)
  - Needs of the business that do not unfairly infringe on privacy rights (emergency contact information)
  
- 2. Proportionality** - all personal data must be relevant to the purposes for which they are collected, and not excessive to those purposes. For example:
  - Include only minimum personal data in systems and excel; Do you need personnel number in HR reports, at reception desks, when booking taxi in an office?

# Basic Principles

- 3. Notice** – Tell individuals, before or at the time their personal data is collected or used of: **who** will have the data, **why** it is being collected and what it will be used for, **to whom** the data will be disclosed, If there is **global sharing of data** and of their data privacy **rights** (access, correction).
- 4. Purpose Limitation** - personal data may be used only for the purposes for which they have been collected in the first place, as described in any notice to individuals and within the scope of their consent.

# Privacy Principles

**5. Accurate, kept no longer then necessary** – personal data must be kept accurate and must not be kept indefinitely

- **Example:** Set retention periods for all data in accordance with a business need, or legal requirement and delete obsolete data, wherever data are held; Require third party processors to do the same.

**6. Rights of individuals** - individuals have a right to access their personal data, and correct it if it is inaccurate and object to use of their data for marketing.

**7. Data security** –protect personal data from loss, destruction, or from unauthorized access, use, or disclosure

**8. Cross-border data transfers restrictions** - Europe, Canada, others

- Global sharing of data must not be a default, unless there is a functional need for it

# Location Privacy



# What's the Problem?

- The location information privacy conundrum
  - Should location information be considered private?
    - What is the expectation of privacy for location data?
    - What if the subject is in a public space?
    - What if the subject is in a sensitive location (e.g., AIDS clinic)?
    - Collection of Data about others – (Merger and Acquisition)
  - Should the accuracy of the location information matter?
  - Does obfuscating actual identity matter?
  - Is real-time location information more sensitive than prior location information?
  - Is informed consent enough?
    - From whom must consent be obtained?
    - Should certain practices be banned?

# Sources of Location Data

- IP Address Location – Geolocation By IP Address
- WiFi Geolocation – more specific
- Voluntary Transmission of Geolocation Data to You
- Is it REALLY Voluntary
- Geolocation by Inference
- Geolocation by Cell tracking – triangulation
- Geolocaition by GPS
- Geolocation by HotSpot
- Geolocation by Website Posting – Loopt, 4Square, Google
- Geolocation by price-match – barcode scanning, etc.
- Database of Geolocation

# Is Geolocation Legal

- DC Case – police obtain invalid warrant to put device on car to track
- Install device in open area
- Track suspect for months
- Is tracking legal?



# Privacy Laws



# Relevant Privacy Laws

- FTC Act, and Related Guidelines
  - FTC Act grants the FTC broad powers to protect consumers against unfair, deceptive acts or practices
  - Personal information collection best practices for adult consumers
    - Notice/awareness
    - Choice/consent
    - Access/participation
    - Integrity/security
    - Enforcement/redress

# Relevant Privacy Laws

- FTC
  - Additional information collection best practices for children
    - Parental Notice/Awareness and Parental Choice/Consent
    - Parental Access/Participation and Integrity/Security Access

# Relevant Privacy Laws

- FTC

- Under the FTC Act, the FTC actively pursues unfair and deceptive practices related to personal information
  - Deceptive practices include a company's failure to follow or implement its own privacy policy to the detriment of consumers
- Unfair practices include failure to adopt minimal levels of security (BJ's case)
  - *De facto* standard directs companies to implement reasonable information security programs to protect consumer personal information

# Relevant Privacy Laws

- FTC
  - FTC promotes effective industry self regulation
    - New behavioral marketing guidelines
      - Issued principles after town hall meeting in 2007
      - Staff report on Self-Regulatory Principles for Online Behavioral Marketing issued February 2009
  - Currently considering location information privacy issues
    - FTC Town Hall meeting held May 6, 2008 discussing privacy implications of location information tracking services

# Relevant Privacy Laws

- FTC
  - *Remedies for violations of the FTC Act*
    - FTC may seek relief in a civil suit based on the nature of the violation
    - Types of relief available to the FTC include
      - Contract rescission or reformation
      - Refunds to affected consumers
      - Payment of damages
      - Public notification of the violation
    - No private rights of action under the FTC Act
    - FTC Act does not permit exemplary or punitive damages

# Superior's Website



The banner features the Superior Mortgage logo on the left, with the letters 'S' and 'M' in a large, stylized font. To the right of the logo, the text 'Superior Mortgage' is written in a large, serif font. Below this, the tagline 'Our Success Is Built On Service' is displayed in a smaller, italicized font. On the far right of the banner is a black and white photograph of three people (two women and one man) smiling and looking at each other.

**SM** Superior Mortgage  
*Our Success Is Built On Service*

If you are already dealing with a loan officer at Superior Mortgage, please [click here](#) to go to his/her page first.

For your convenience we've provided this Online Application Form. If you prefer, we can mail (or e-mail) you a form that may be completed offline. If you have any questions, please call the office number provided at the bottom of this page to speak to one of our helpful loan consultants.

After completing this form, you will be presented with a disclosure statement in which you must acknowledge reading, else your application **WILL NOT** be submitted to Superior Mortgage.

(All information submitted is handled by SSL encryption - see the yellow padlock at the bottom of your browser)

**To Apply For A Loan**  
**Mortgages 101**  
**Buying A Home**  
**Refinancing A Home**  
**Office Locations**  
**About Us**

# Relevant Privacy Laws

- Electronic Communications Privacy Act (ECPA)
  - *Who must comply?*
    - ISPs, online service providers (wired and wireless), and remote computing service providers
    - But only if they provide services to the public
  - *What activities and information are covered?*
    - Disclosure of any wireless or wired transmission
    - Access to electronically stored information



# Relevant Privacy Laws

- ECPA

- *What are the key rules?*

- No person or entity may intercept electronic communications without authorization
    - Service providers may not knowingly use any electronic, mechanical or other devices to intercept, use or disclose contents of in-transit or stored electronic communications including customer account records *unless a statutory exception applies*

# Relevant Privacy Laws

- ECPA
  - Service provider exceptions for stored information
    - Customer's intended recipients
    - Prior consent
    - As required to forward messages automatically
    - Provider's employees as necessary to provide customer its services in the normal course
    - Protection of service provider's property or rights
    - Law enforcement
      - Inadvertently obtained by provider and evidence of a crime
      - Warrant, subpoena, court order
      - Collection (but not disclosure) and retention (up to 180 days) pending issuance of valid order, subpoena or warrant

# Relevant Privacy Laws

- ECPA
  - Service provider exceptions for customer records
    - Customer's prior consent
    - Protection of service provider's property or rights
    - Disclosure to *any person* or entity other than the government
    - Law enforcement under limited circumstances
      - Inadvertently obtained by provider and evidence of a crime
      - Compliance with a warrant, subpoena, or court order
      - Reasonable belief that disclosure in light of an emergency involving death or serious bodily injury is required

# Relevant Privacy Laws

- ECPA
  - *Penalties and remedies for violations*
    - Private parties adversely affected can seek compensatory and punitive damages, injunctive relief and attorneys fees
    - Criminal fine and/or up to 5 years' imprisonment for the first offense and up to 10 years' imprisonment for repeat offenders

# Relevant Privacy Laws

- Computer Fraud and Abuse Act (CFAA)
  - *Who must comply?*
    - Generally applicable federal criminal statute
  - *What activities and information are covered?*
    - Accessing protected computer resources
    - Intercepting information or communications
    - Accessing government computers or national security information
    - Accessing computers to commit a crime
    - Causing damage to a protected computer
    - Trafficking in passwords
    - Threatening computer resources to cause damage

# Relevant Privacy Laws

- CFAA
  - *What are the key rules?*
    - May not access computer resources (without authorization) to intentionally engage in any of prohibited acts
    - Exceeding authorization and then engaging in prohibited act is also a crime
    - Damage threshold of \$5,000 over 12 month-period for civil actions and felony criminal prosecution
    - Does CFAA apply to unauthorized collection of personal information without notifying customers?
      - Probably, but satisfying the loss threshold is the trick
      - Aggregating claims across victims and time requires a single act

# Relevant Privacy Laws

- CFAA
  - *Penalties for violations*
    - Private parties adversely affected can seek compensatory damages, injunctive relief and equitable remedies
    - Criminal fine and/or up to 10 years' imprisonment for the first offense and up to 20 years' imprisonment for repeat offenders

# Relevant Privacy Laws

- Children's Online Privacy Protection Act (COPPA)
  - *Who must comply?*
    - Operators of commercial web sites and online services satisfying either of the following:
      - Directed at children
      - General purpose service with actual knowledge that children are providing personal information
    - FTC is preparing “clarifications” to the rules for application to mobile services
  - *What activities and information are covered?*
    - Collection of personal information from children under 13



# Relevant Privacy Laws

- COPPA

- *What are the key rules?*

- Safe harbor for complying with FTC approved self-regulatory program
    - Outside of the safe harbor, operator must follow COPPA
      - Post a policy
      - Notice to parents with prior verifiable consent
      - New consents when there is a material change in practices
      - Grant parents access to collected information
      - Allow parents to revoke consent and remove child's personal information

# Relevant Privacy Laws

- COPPA
  - *Exceptions to the rules*
    - Response to one-time request from the child
    - As required to provide notice to parents
    - Safety of the child
    - Regular newsletters if the parents are notified and can opt out for their child
  - *Penalties for violations*
    - FTC initiated civil action with fines up to \$11,000 per violation

# Relevant Privacy Laws

- EU Data Directive 95/46/EC
  - *Who must comply?*
    - Any person or entity can be subject to the EU Data Directive, even companies without operations in the EU
  - *What activities and information are covered?*
    - Transfer of personal data from any EU Country
    - Covered data is information that personally identifies an individual
  - *What are the key rules?*
    - Personal data from the EU may not be transferred to any country unless that country has adequate privacy protections
    - Conflict over whether the U.S. laws are adequate

# Relevant Privacy Laws

- EU Data Directive 95/46/EC
  - To provide U.S. companies clarity, U.S. and EU agreed on certain safe harbor principles
    - They do not apply to non-U.S. companies, or transfers within and between EU member states
    - Compliance with principles is presumptive compliance with EU Data Directive
    - Methods of compliance
      - Participate in self-regulatory industry standards
      - Self-certify with submission to U.S. DoC

# Relevant Privacy Laws

- EU Data Directive 95/46/EC
  - Safe harbor principles (must be declared publicly)
    - Notice/Choice (opt-out is good enough)
    - Onward transfer to compliant 3<sup>rd</sup> parties
    - Security and data integrity
    - Provide access to data subjects
    - Enforcement of the principles
  - *Penalties for violations*
    - Civil action by the FTC under the FTC Act for companies using the Safe Harbor
    - For companies that don't use the safe harbor, EU Data Directive remedies may apply (e.g., private rights action, civil fines, and data transfer embargos)

# Relevant Privacy Laws

- The European Commission Directive on Privacy and Electronic Communications 2002/58/EC
  - Covers real-time and historic location information
  - Providers can process location information to enable transmission, process bills, and manage traffic
  - Location data (other than traffic data) can be processed (without consent) if the individual isn't identified
  - For value added services, location can be tracked with informed consent of the user or subscriber
  - User or subscriber must be able to withdraw consent
  - Use of non-anonymous location data only to the extent necessary to provide the value-added service within the scope of the consent
  - Does it reach U.S. companies like the EU Data Directive 95/46/EC?

# Relevant Privacy Laws

- Invasion of privacy under state common law
  - Elements: (1) unauthorized intrusion; (2) level of intrusion is offensive to a reasonable person; (3) intrusion relates to private matters; and (4) results in anguish or suffering
  - Most states recognize the tort
    - NY - no
    - CA - yes

# Relevant Privacy Laws

- 45 States (+P.R.) have breach - notice Laws
- Typical statutory elements
  - Protected personal information covered
    - Name plus one or more identifying element
      - SS#, driver's license #, other government ID #, financial account numbers and account access credentials
    - Health insurance or medical records
    - Applies to owners or delegated custodians of covered personal information of a citizen of the state
    - Location information not widely recognized . . . yet
  - Notice triggering events
    - Actual unauthorized access or disclosure of unencrypted personal information
    - Reasonable belief of unauthorized access to such data



# Relevant Privacy Laws

- Typical statutory elements (cont'd)
  - Nature of the notice
    - Expeditiously inform affected individuals unless law enforcement directs otherwise
    - Some require notice to attorney general's office or equivalent
    - First class mail, email if used in normal course and customer prior consent, if large number of affected consumers, public notice may be permitted.
  - Other factors and obligations
    - Some states require automatic notice when breach occurs (e.g., CA, NY)
    - Other states allow data handler to assess risk before issuing notice (e.g., CT, NJ, WA)
    - Data handlers required to employ reasonable safeguards to prevent breaches

## EU – US Safe Harbor

- Benefits for companies joining Safe Harbor program
  - All 15 Member States of the European Union will be bound by the European Commission's finding of adequacy
  - Companies participating in the safe harbor will be deemed adequate and data flows to those companies will continue;
  - Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and
  - Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to limited exceptions.

## EU – US Safe Harbor

- Requirements for companies joining Safe Harbor program
  - Notice
  - Choice
  - Onward Transfer
  - Access
  - Security
  - Data integrity
  - Enforcement
- Self regulated, but if commitments broken FTC can fine \$12,000 per day

# International Laws

- OECD Privacy Principles
  - Governing transborder flows of personal data
  - Similar to EU directive
- United Nations Guidelines Concerning Computerized Personal Data Files
  - Adopted by general assembly 1990
  - Lawfulness, Fairness, Accuracy, Purpose specification, Access, Non-Discrimination, Exceptions, Security, Supervision and Sanctions, Transborder Data flows, Field of Application

# Canadian Privacy Law

- Federal Laws
  - Privacy Act (1983)
  - Personal Information and Electronic Documents Act (2001 – 2004)
- Provincial Legislation
- Sector Specific Legislation
  - Personal Health Information Act
  - Federal Bank Act

# Sliding Scale for Notice and Choice

Type of Advertising	Definition	Obligation
Sensitive Personally Identifiable Information Advertising	The use of sensitive personally identifiable information for the purpose of behavioral advertising.	Opt-in consent
Personally Identifiable Advertising	The merger of information that, by itself, can be used to identify someone – such as name, e-mail address, physical address, or telephone number – with data collected through multi-site or behavioral advertising for the purpose of ad targeting.	Prospective use: Opt-out choice Retroactive use: Opt-in consent
Behavioral Advertising	The tracking of a consumer's activities online across multiple, unrelated sites – including the searches the consumer has conducted, the web pages visited, and the content viewed – by a third party in order to deliver advertising across multiple, unrelated sites targeted to the individual consumer's interests.	Opt-out choice
Multi-site Advertising	Online advertising across multiple, unrelated third-party sites.	Pass-through notice: make reasonable efforts to require website operators to link to a privacy notice on their home page
Online Advertising	The logging of page views or the collection of other information about an individual consumer or computer for the purpose of delivering ads or providing advertising-related services.	Link to privacy notice on home page; follow reasonable security and data retention obligations

Source: Microsoft Corporation

[My eBay](#) > [My Account](#) > [Preferences](#) > **Advertising Preferences**

**eBay AdChoice**

We may use information we have about you to make sure that the ads we show you are as relevant to you as we can make them. We think these relevant AdChoice ads will improve your shopping experience. Any information we use for AdChoice follows the eBay [Privacy Policy](#).


We may work with other companies, like website operators and our ad network partners, to share information with other website operators and our ad network partners. We may share information about you (like eBay search terms, demographics and categories of interests) with these companies. We don't share your personal information with any of these companies for identifying you.

You have choices about whether we use your information in the way described above. If you opt out of AdChoice, you can tell us not to use your information with our ad network partners and you can tell us not to use your information with our ad network partners. Anywhere you see the advertising link, you can click on it to change your AdChoice. If you opt out of AdChoice, you'll still see ads, they just won't be tailored to you.

☒ Yes, please use my information to show me relevant ads on eBay.

☒ Yes, please use my information to show me relevant ads on other websites.

[Cancel](#)



**AdChoice**

We may use information we have about you to make sure that the ads we show you are as relevant to you as we can make them. We think these relevant AdChoice ads will improve your shopping experience. Any information we use for AdChoice follows the eBay [Privacy Policy](#).

Look for the "ADVERTISEMENT (about)" label on ads to learn how your information is used.

Yahoo! is our ad network partner for this ad. We may share only anonymous information about you, like eBay search terms and categories of interests. Yahoo! may also use this information about its own users to select which ads to display. We don't share your personal information with any of these companies for identifying you. About Yahoo!'s ad practices, including how to opt out, see [Yahoo!'s privacy policy](#).

**AdChoice Preferences**

If you're an eBay user, you can also manage your [My eBay](#) account.

☒ Yes, please use my eBay information to show me relevant ads on eBay's ad network partners.

If you opt out of AdChoice, you'll still see ads on eBay, but we won't send any information to Yahoo! to customize those ads. Due to Yahoo!'s current systems, information we've already sent may continue to influence the ads you see for up to three months. You can tell Yahoo! to immediately stop customizing your ads on eBay by using their [opt out](#).

ADVERTISEMENT (about)


wireless  
your way


Add a line to your account and get the Samsung A737


**FREE\***


Get the wireless package


Signif. restrictions apply














be unique for less

# Opt-In for 3<sup>rd</sup> Party Sharing: Disclosures for Beacon Advertisers

SHOP.COM™

## i. Facebook Beacon

SHOP.COM is a [Facebook Beacon](#)-enabled site. Facebook Beacon allows you to share information about your purchases on SHOP.COM through Facebook. When you make a purchase you are logged-in to Facebook and whether your privacy preferences on SHOP.COM with your Facebook friends and network members. If you are on SHOP.COM and if your privacy preferences in your Facebook Profile (as your Facebook Profile) and shares it with your Facebook friends and network members. If you are not a Facebook user or logged into your Facebook account a notice will be displayed asking you to discard the information SHOP.COM has sent to it. To learn more about

Facebook has recently created an FAQ page with a tutorial describing how users can either universally opt-out or, on a partner-by-partner basis, appear in their newsfeed.

The tutorial can be found here: <http://www.facebook.com/beacon/faq>

### We've added more privacy controls

[Close](#)

- Friend of friend privacy: expand who can see your profile, photos, notes and other content.
- Friend list privacy: control exactly who can see what by including or excluding certain friends or friend lists. Look for the "Customize" options.

### Privacy



#### Profile ▸

Control who can see your profile and personal information.



#### Search ▸

Control who can search for you, and how you can be contacted.



#### News Feed and Mini-Feed ▸

Control what stories about you get published to your profile and to your friends' News Feeds.



#### Applications ▸

Control what information is available to applications you use on Facebook.

### Block People

If you block someone, they will not be able to search for you, see your profile, or contact you on Facebook. Any ties you currently have with a person you block will be broken (friendship connections, relationships, etc).

### Block List

You have not blocked anyone.

Person:

Add



## Don't give visitors and customers any reason to worry about data collection and use practices.

- Go beyond the privacy statement
  - Matter-of-factly incorporate some disclosure of tracking and targeting as part of your product or service value proposition.
- Provide a “what is this” button to explain how your customization works.
  - Primary purpose on websites is not to read notices but to transact and build experiences
  - Opt-out rates are low but address the vocal minority
- Make sure your service providers, agencies, and others are following industry standards for privacy notice and disclosure.
  - Many of the serious complaints or issues TRUSTe encounters are privacy breaches by marketing vendors.

# Social Media



- 1. Transparency (disclosing “material connections”);**
- 2. Accuracy (communicating truthful information);**
- 3. Honesty (avoiding misleading or deceptive communications); and**
- 4. Respect (recognizing the personal or property rights of others).**

# FTC Blogging Initiative

The FTC Guides raise liability issues: Now, all stakeholders - - whether advertisers, brands/companies, ad agencies, and bloggers (or other agents) - - are liable for (i) their failure to disclose “material connections” and (ii) the speaker's making unsubstantiated claims about the products/services of the advertiser or brand.

And

The FTC mandates that advertisers and brands develop policies that:

1. educate their agents/endorsers about the responsibilities; and
2. monitor the communications/statements/claims by their agents/endorsers.

# Setting the Stage: An Overview of the FTC Guides Governing the Use of Testimonials and Endorsements

In other words, brands/advertisers must develop a formal policy that trains and monitors their endorsers and agents.  
Which means: you must develop a “Social Media Policy” by creating standards of conduct for your sponsored speakers.

## **For employees**

Example 8 in 16 C.F.R. Part 255.5 illustrates that both the employee and employer are potentially liable for an employee's failure to disclose her material connection with the employer.

## **For third parties and agencies**

Training for your speakers and bloggers  
Monitoring their communications

# Recent Investigation by the FTC involving Ann Taylor

On April 20, 2010, the FTC closed its investigation involving an Ann Taylor promotion

Issue: whether Ann Taylor violated the FTC Act where company provided gifts to bloggers who company expected would blog about company's LOFT division.

Some bloggers failed to disclose they had received free gifts from LOFT.

FTC staff determined not to recommend enforcement action, because, in part, "LOFT adopted a written policy . . . stating that LOFT will not issue any gift to any blogger without first telling the blogger that the blogger must disclose the gift in his or her blog."

FTC said it expects company to monitor bloggers' compliance with obligation to disclose gifts they receive from LOFT.



# Appendices



## Reference Material

- The Communications Act and CPNI Rules
  - The Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039
  - The Communications Act of 1996, 47 U.S.C § 222
  - FCC Report and Order and Further Notice of Proposed Rulemaking in CC Docket No. 96-115 & WC Docket No. 04-36 (April 2, 2007)



## Reference Material

- FTC
  - The FTC Act, 15 U.S.C. §§ 41 et seq.
  - FTC's Fair Information Practice Principles, see <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>
  - FTC Staff Report Beyond Voice: Mapping the Mobile Market Place (April 2009), see <http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf>
  - FTC Staff Report on Self-Regulatory Principles for Online Behavioral Marketing (February 2009), see <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>
  - Fighting Fraud with Red Flags Rule: A Guide for Business, see <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

## Reference Material

- ECPA
  - Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712
  - Portions of ECPA addressing stored information are known as the Stored Communications Act
  - ECPA is an extension of the Wiretap Act, 18 U.S.C. §§ 2701-2712
- CFAA
  - The Computer Fraud and Abuse Act, 18 U.S.C. § 1030
  - *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 497 (S.D.N.Y. 2001)

# Reference Material

- COPPA
  - The Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 *et seq.*
  - Children's Online Protection Rules, 16 C.F.R § 312.5
- EU Data Directive and U.S. Safe Harbor
  - EU Privacy Directive 95/46/EC
  - U.S. – European Safe Harbor Framework, see [http://www.export.gov/safeharbor/eu/eg\\_main\\_018365.asp](http://www.export.gov/safeharbor/eu/eg_main_018365.asp).
  - U.S. – Switzerland Safe Harbor Framework, see <http://www.export.gov/safeharbor/swiss/index.asp>

# Reference Material

- State Breach - Notice Laws

[Alaska](#) (ALASKA STAT. § 45.48.010 et seq.)

[Idaho](#) (IDAHO CODE ANN. § 28-51-104 et seq.)

[Nebraska](#) (NEB. REV. STAT. § 87-801 et seq.)

[Rhode Island](#) (R.I. GEN. LAWS § 11-49.2-3)

[Arizona](#) (ARIZ. REV. STAT. ANN. § 44-7501(h))

[Illinois](#) (815 ILL. COMP. STAT. ANN. 530/5, /10)

[Nevada](#) (NEV. REV. STAT. 603A.010 et seq.)

[South Carolina](#) (S.C. Code § 37-20)

[Arkansas](#) (ARK. CODE ANN. § 4-110-101 et seq.)

[Indiana](#) (IND. CODE § 24-4.9)

[New Hampshire](#) (N.H. REV. STAT. ANN. § 359-C:19 et seq.)

[Tennessee](#) (TENN. CODE ANN. § 47-18-21)

[California](#) (CAL. CIV. CODE § 1798.82)

[Iowa](#) (SF 2308)

[New Jersey](#) (N.J. STAT. ANN. § 56:8-163)

[Texas](#) (TEX. BUS. & COMM. CODE ANN. § 48.001 et seq.)

[Colorado](#) (COLO. REV. STAT. § 6-1-716)

[Kansas](#) (KAN. STAT. ANN. § 50-7a01-02)

[New York](#) (N.Y. GEN. BUS. LAW § 899-aa)

[Utah](#) (UTAH CODE ANN. § 13-44-101 et seq.)

[Connecticut](#) (CONN. GEN. STAT. § 36a-701b)

[Louisiana](#) (LA. REV. STAT. ANN. § 51:3071 et seq.)

[North Carolina](#) (N.C. GEN. STAT. § 75-60 et seq.)

[Vermont](#) (VT. STAT. ANN. tit. 9, § 2430 et seq.)

[Delaware](#) (DEL. CODE ANN. tit. 6, § 12B-101)

[Maine](#) (ME. REV. STAT. ANN. tit. 10, § 1346 et seq.)

[North Dakota](#) (N.D. CENT. CODE § 51-30-01 et seq.)

[Virginia](#) (Va. Code § 18.2-186.6)

[District of Columbia](#) (District of Columbia B16-810, D.C. Code § 28-3851)

[Maryland](#) (MD Stat. Ann. § 14-3504)

[Ohio](#) (OHIO REV. CODE ANN. § 1349.19)

[Washington](#) (WASH. REV. CODE § 19.255.010)

[Florida](#) (FLA. STAT. § 817.5681)

[Massachusetts](#) (Massachusetts General Laws Ann. 93H § 1 et seq.)

[Oklahoma](#) (Okla. Stat. § 74-3113.1)

[West Virginia](#) S.B. 340

[Georgia](#) (GA. CODE ANN. § 10-1-911)

[Michigan](#) (Michigan Compiled Laws Ann. 445.72)

[Oregon](#) (S.B. 583)

[Wisconsin](#) (WIS. STAT. § 134.98)

[Hawaii](#) (Hawaii Revised Stat. § 487N-1 et seq.)

[Minnesota](#) (MINN. STAT. § 325E.61)

[Pennsylvania](#) (73 PA. CONS. STAT. ANN. § 2303)

[Wyoming](#) (W.S. 40-12-501 through 40-12-509)

[Montana](#) (MONT. CODE ANN. § 30-14-1704)

[Puerto Rico](#) (Law 111 and Regulation 7207)

# Outline

- US Privacy Laws
- European Data Protection Directive
- Safe Harbor
- Canadian Laws
- Personal Information Protection and Electronic Documents Act
- Conclusions

# US Privacy Law

- Patchwork of sector specific laws and regulations – no comprehensive national law
  - 1970 fair credit reporting act
  - 1974 code of fair practices and privacy act
  - 1978 right to financial privacy act
  - 1982 debt collection act
  - 1984 cable communications act
  - 1986 electronic communications privacy act
  - 1987 computer security act
  - 1988 computer matching and privacy protection act
  - 1994 communications assistance for law enforcement act
  - 1994 driver's privacy protection act
  - 1996 communications decency act
  - 1998 identity theft and assumption deterrence act
  - 1998 children's online privacy protection act

# Lawsuits in USA

- Need a degree in law to understand all the legal implications for privacy in USA
- Litigation seems the preferred form of regulation
- Litigation usually filed under deception:
  - Misrepresentation of privacy promises
  - Failure to Disclose
  - Children (COPPA)
  - Identity Theft
  - Cookies and Web Bugs
- For cases see: Freeman, Nemiroff, “Privacy Law in Q1 2002”, [www.privacylawplaybook.com/documents/PRIV\\_Privacy\\_Law\\_Primer\\_2002\\_Q1.PDF](http://www.privacylawplaybook.com/documents/PRIV_Privacy_Law_Primer_2002_Q1.PDF)

# European Law

- EU Data Protection Directive (1998)
  - EU member states must adopt regulations that forbid the transfer of data to non-member countries, if those non-member countries fail to provide adequate protection
  - Exceptions: data transfer is permissible if:
    - Data subject consents to transfer
    - Transfer is necessary to perform contract
    - Transfer serves the interests of the subject
    - Recipient provides sufficient guarantees to privacy



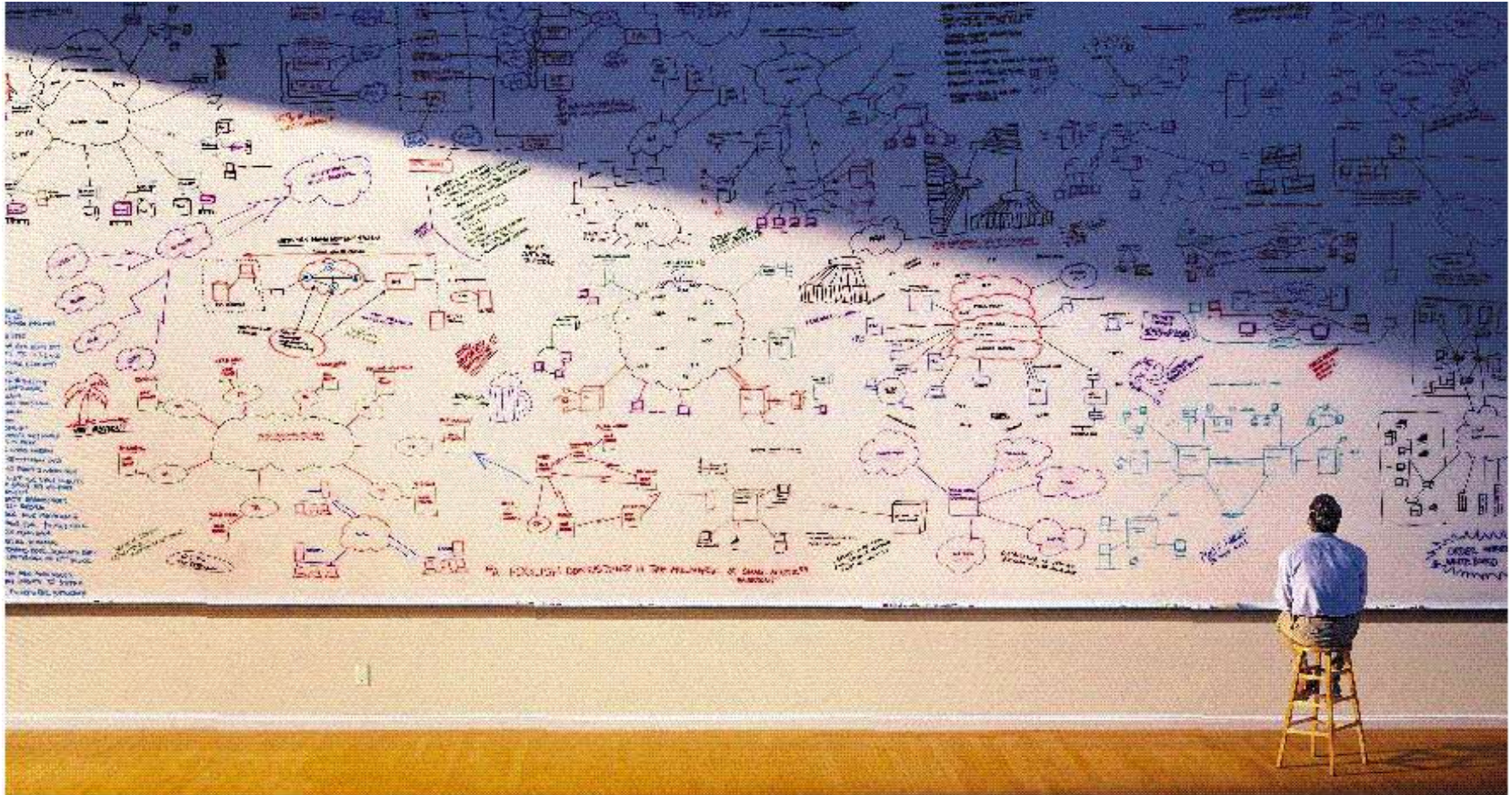
# European Law

- EU Data Protection Directive (1998)
  - Adequate level of protection: individuals must be able to:
    - Withhold consent to process their data
    - Access the data collected about them
    - Correct inaccuracies in the data
    - Bring a complaint and seek redress for misuse of data
  - Data collector must provide individuals with:
    - Notice of the purposes for which the data is collected
    - The intended uses of the data
    - Any other recipients of the data

# European Law

- EU Data Protection Directive (1998)
  - Canada has been declared adequate as of Jan 14, 2002
  - EU officials determined that US protections are not adequate
    - To prevent a trade war “Safe Harbor” agreements were made between US and EU
    - Companies comply individually with directive requirements
    - 170 have joined ([www.export.gov/safeharbor](http://www.export.gov/safeharbor))

# There is real complexity – we can help...



Mark D. Rasch  
Director, CyberSecurity and Privacy  
Consulting  
CSC  
[MRasch2@csc.com](mailto:MRasch2@csc.com)  
(301) 547-6925