Silicon Flatirons Center
A Center for Law, Technology, and Entrepreneurship at the University of Colorado

"Crash Course" on Data Privacy and Security

December 5, 2012

Jason Haislmaier
jason.haislmaier@bryancave.com
@haislmaier

BRYAN CAVE HRO

Data
Security
Privacy

BRYAN CAVE HRO

LinkedIn

May 19, 2011

BRYAN CAVE HRO

LinkedIn

June 7, 2012

BRYAN CAVE HRO

Broad and Fast

V

"Big Data"

Volume

Variety

Velocity

BRYAN CAVE

"Broad Data"

BRYAN CAVE

Increasing value
Increasing importance
Increasing scrutiny
Increasing responsibility
Increasing opportunity

BRYAN CAVE

What Should You Do?

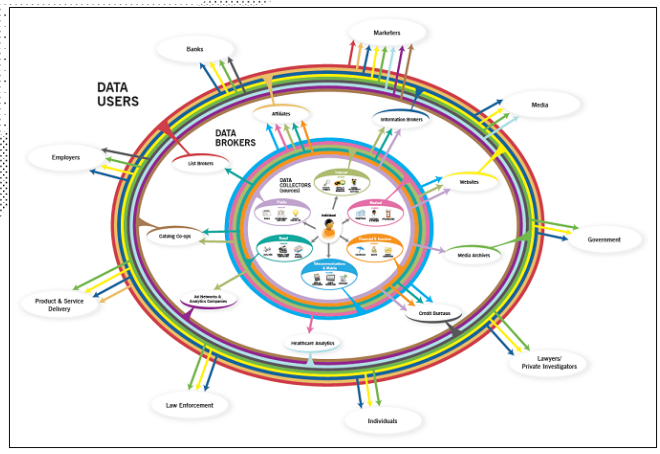
BRYAN CAVE

Know Your Data

Map Your Data "Ecosystem"

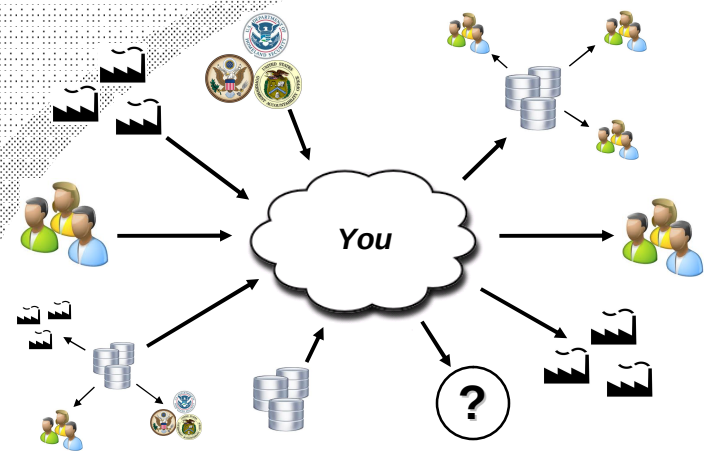
BRYAN CAVE HRO

Data Mapping



BRYAN CAVE HRO

Data Mapping



BRYAN CAVE

Legal Landscape

No specific comprehensive data privacy or security legislation (in the US)

BRYAN CAVE

Legal Landscape

Longstanding EU Regulations

- EU Data Protection Directive (95/46/EC)
- Regulates the processing of personal data of EU subjects
  - Broad scope of "personal data"
  - Restricts processing unless stated conditions are met
  - Prohibits transfer to countries not offering adequate levels of protection
- US Department of Commerce-negotiated "Safe Harbor Principles" enable transfers to US companies
  - Self-certification regime
  - Allows US companies to register as compliant
  - FTC oversight
- Proposed overhaul in the works (announced Jan. 25, 2012)

BRYAN CAVE

Legal Landscape

Growing Array of Relevant State Laws

- State consumer protection statutes
  - All 50 states
  - Prohibitions on "unfair or deceptive" trade practices
- Data breach notification statutes
  - At least 46 states (DC and various US territories)
  - Notification of state residents (and perhaps regulators) affected by unauthorized access to sensitive personal information
- Data safeguards statutes
  - (Significant) minority of states
  - Safeguards to secure consumer information from unauthorized access
- Data privacy statutes
  - Online privacy policies covering use and sharing of consumer information
  - Use of personal information for direct marketing purposes

BRYAN CAVE

Legal Landscape

Industry-specific Federal Statutes

- Consumer credit - Fair Credit Reporting Act (FCRA)
- Financial services - Gramm Leach Bliley Act (GLBA)
- Healthcare providers - Health Insurance Portability and Accountability Act (HIPAA)
- Children (under 13) - Children's Online Privacy Protection Act (COPPA)
- Video content - Video Privacy Protection Act
- Others statutes covering education, payment processing, etc.

BRYAN CAVE

Legal Landscape

Federal Trade Commission Act (FTCA)

(15 U.S.C. 41, et seq)

"Unfair or deceptive acts or practices"

BRYAN CAVE

Legal Landscape

Federal Trade Commission Act (FTCA)

- No specific privacy or security requirements
  - Broad prohibition on "unfair or deceptive acts or practices in or affecting commerce" (Section 5)
    - Failures to implement "reasonable and appropriate" data security measures
    - Deceptive data privacy policies and promises
  - Constituting unfair or deceptive acts or practices
- Increasingly active enforcement
  - More than 40 actions to date
    - More than 25 in the last 6 years
    - Many more investigated but not brought
  - Covering largely electronically stored data and information
  - Targeting security breaches as well as privacy violations

BRYAN CAVE HRO

FTC Compliance

BRYAN CAVE HRO

FTC Compliance

Emerging Model for Settlement and Compliance

- 20 year term
- Cease misrepresentations regarding practices for information security, privacy, confidentiality, and integrity
- Conduct assessment of reasonably-foreseeable, material security risks
- Establish comprehensive written information security and privacy program
- Designate employee(s) to coordinate and be accountable for the program
- Implement employee training
- Conduct biannual independent third party audits to assess security and privacy practices
- Implement multiple record-keeping requirements
- Implement regular testing, monitoring, and assessment
- Undergo periodic reporting and compliance requirements
- Impose requirements on service providers

BRYAN CAVE

FTC Compliance

"Promises"

not just

Policies

BRYAN CAVE

FTC Compliance

"Facebook is obligated to keep the ***promises about privacy*** that it makes to its hundreds of millions of users."

Jon Leibowitz
Chairman of the FTC
Speaking on the facebook settlement

BRYAN CAVE

FTC Compliance

"Innovation does ***not*** have to come at the expense of consumer privacy."

Jon Leibowitz
Chairman of the FTC
Speaking on the facebook settlement

BRYAN CAVE

FTC Compliance

"We've made a bunch of ***mistakes***."

Mark Zuckerberg
CEO of Facebook
Speaking on the facebook settlement

BRYAN CAVE

FTC Compliance

Scope of
"Personal Information"

BRYAN CAVE

FTC Compliance

"Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above.

In the Matter of UPromise, Inc. **(FTC File No. 102 3116, Jan. 5, 2012)**

BRYAN CAVE HRO

FTC Compliance

1. "Personally identifiable information" or "personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) an Internet Protocol ("IP") address or host name that identifies an individual consumer; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) or any information that is combined with (a) through (g) above. Provided that, this definition shall not include personally identifiable information about physicians, nurses, or other health care professionals, or their staff, that is collected in connection with such persons' professional duties.

In the Matter of Eli Lilly and Company **(File No. 012 3214, Januray 18, 2002)**

BRYAN CAVE HRO

FTC Compliance

Scope of
"Sensitive Information"

BRYAN CAVE

FTC Compliance

Sensitive Information

- States have defined "sensitive information" to include SSN, drivers license number, and financial account information
- FTC has broadened this definition to include
  - Health information
  - Information regarding children
  - Geo-location information
- Trend is toward more activity in these areas
- Practical considerations
  - Know when/where you collect sensitive information
  - Consider seeking consent when using sensitive data for marketing purposes
  - Ensure that WISPs appropriately protect sensitive information
- Note that these categories of sensitive information may not trigger a data breach notification requirement under state laws

BRYAN CAVE

FTC Compliance

WISPs

(Written Information Security Plans)

BRYAN CAVE

FTC Compliance

WISPs

- The "Safeguards Rule" under GLBA requires implementation of "written information security plans"
  - Describing the company's program to protect customer information
  - Appropriate to the company, nature and scope activities, and level of sensitivity of information
- FTC consent orders now generally impose similar requirements
  - Implementation comprehensive information security program
  - Fully documented in writing
  - Reasonably designed to protect the security and privacy of covered information
  - Containing controls and procedures appropriate to the
    - Size and complexity of the business
    - Nature and scope of activities
    - Sensitivity of the covered information
- Mass. state regs. also now require WISPs

BRYAN CAVE

FTC Compliance

"Reasonable and appropriate" security measures

FTC Compliance

In the Matter of UPromise, Inc.
(FTC File No. 102 3116, Jan. 5, 2012)

U.S. v. RockYou, Inc.
(N.D. Cal. Mar. 26, 2012)

In the Matter of Complete, Inc.
(FTC File No. 102 3155, Oct. 22, 2012)

FTC Compliance

Reasonable and Appropriate Security

- Settlements provide guidance on what is *not* reasonable or appropriate
  - Collecting PII from consumers unnecessarily
  - Not taking steps to avoid collection of PII
  - Failing to test applications to ensure they are not collecting PII
  - Not training employees about security risks
  - Transmitting or storing sensitive information in unencrypted form
  - Failing to segment servers
  - Leaving systems susceptible to hacking (e.g., SQL injection attacks)
  - Failing to ensure that service providers use reasonable and appropriate security
- They also raise practical considerations
  - Understand the data you are collecting, storing, accessing, and sharing
  - Draft WISPs to prohibit unreasonable practices
  - Educate and train employees
  - Enforce and update applicable policies

BRYAN CAVE

FTC Compliance

COPPA

(Children's Online Privacy Protection Act)

BRYAN CAVE

FTC Compliance

United States of America v. Artist Arena, LLC
(U.S. Dist., SDNY Oct. 2, 2012)

FTC Compliance

Aggressive COPPA Enforcement

- Artist Arena to pay $1 MM civil penalty to settle FTC complaint for COPPA violations
  - Operates fans sites: BieberFever.com; SelenaGomez.com; RihannaNow.com; DemiLovatoFanClub.com
  - Permitted users to join fan club, create profiles and post on members' walls
  - FTC: knowingly registered over 25,000 children under age 13 and collected and maintained personal information from almost 75,000 additional children who began, but did not complete the registration process.
- "Marketers need to know that even a bad case of Bieber Fever doesn't excuse their legal obligation to get parental consent before collecting personal information from children," said FTC Chairman Jon Leibowitz
- "The FTC is in the process of updating the COPPA Rule to ensure that it continues to protect kids growing up in the digital age."

FTC Compliance

FTC Issues Revised COPPA Regulations

- Expands definition of "personal information" to include:
  - Persistent Identifiers (i.e., IP addresses, Device ID's)
  - Customer numbers held in cookies
  - Geo-location information
- Requires more effective means of obtaining parental consent (i.e. "no more email plus")
- Data minimization requirement
- Requires all operators of an online service or website to provide contact information
  - Ad networks
  - Analytics providers
  - Other content providers

BRYAN CAVE

FTC Compliance

Revised COPPA Regulations

- Practical Implications for Sites/Apps "targeted to children"
  - Apps that utilize device ID's could violate COPPA unless advance parental consent
  - Must think creatively to ensure effective parental consent
  - Must justify data retention and implement effective data disposal policies and procedures
  - Know your partners (analytics companies, third party marketing partners) and ensure downstream controls through contractual provisions
- Intense industry criticism
  - "The 90's called and they want their apps back"

BRYAN CAVE

FTC Compliance

Downstream obligations. . .

FTC Compliance

Requirements for Service Providers

- FTC settlements require contractual restrictions on third party service providers

III.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

A. …

B. …

C. …

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

In the Matter of Google, Inc. **(FTC File No. 102-3136, March 30, 2011)**

FTC Compliance

Requirements for Service Providers

- FTC settlements require contractual restrictions on third party service providers
- Parallel newly effective Mass. regulation (201 CMR 17.03)
  - Requiring companies providing service providers with personal information about Mass. residents to contractually require the providers to "implement and maintain . . . appropriate security measures"
  - Went into full effect on March 1, 2012
- Practical implications
  - Understand what service providers you are using
  - Revise and amend form agreements (develop form paragraphs)
  - Maintain a WISP with applicable policies
  - Conduct risk employee training
  - Investigate incidents and document follow-up action

BRYAN CAVE

FTC Compliance

Respecting consumer choice. . .

BRYAN CAVE

FTC Compliance

U.S. v. Google, Inc.
(Case No. 5:12-cv-04177-HRL, N.D.Cal. August 9, 2012)

BRYAN CAVE HRO

FTC Compliance

Respecting Consumer Choice on Privacy

- *U.S. v. Google, Inc.*, Case No. 5:12-cv-04177-HRL, N.D.Cal. (August 9, 2012)
- FTC charged Google with violation of Google (Buzz) Consent Order
  - Privacy policy permitted opt out
  - Google exploited loophole in Safari browser default DNT settings to drop Doubleclick tracking cookies
- Google to pay $22.5mm to settle charges
- Remediation measures
- Self-reporting of compliance with remediation

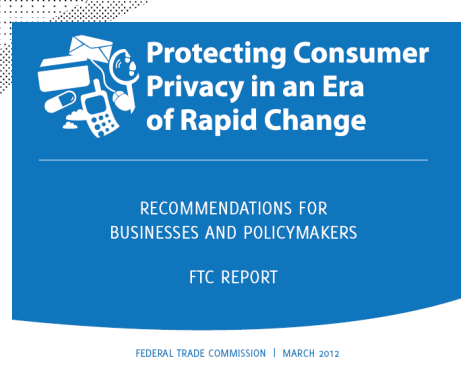
BRYAN CAVE HRO

Where are we headed?

. . . and what should you do?

BRYAN CAVE

FTC Report



March 26, 2012

BRYAN CAVE

FTC Report

Background

- Based on a yearlong series of privacy roundtables held by the FTC
- Extensive comment period (more than 450 comments received)
- Provides best practices for the protection of consumer privacy
- Applicable to both traditional (offline) and online businesses
- Intended to assist Congress as it considers privacy legislation
- Not *intended* to serve as a template for law enforcement actions (but what about plaintiffs attorneys?)

BRYAN CAVE

FTC Report

Privacy Framework

- Proposed framework is based on several core concepts
  - Simplified consumer choice

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

BRYAN CAVE

FTC Report

Privacy Framework

- Proposed framework is based on several core concepts
  - Simplified consumer choice
  - Transparency

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

B. Access

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

BRYAN CAVE

FTC Report

Privacy Framework

- Proposed framework is based on several core concepts
  - Simplified consumer choice
  - Transparency
  - Privacy by design

PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

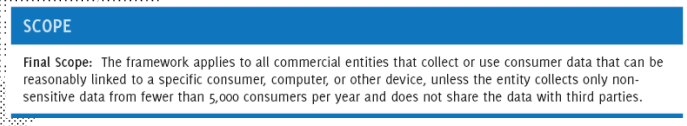
Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

BRYAN CAVE

FTC Report

Scope of Personal Information

- Continued expansion of "personal information"



- Codification of the definitions used in FTC settlements
- Shades of the definition in the EU Data Protection Directive
- Blurring of the line between PII and non-PII
- When is information *not* PII?

BRYAN CAVE

FTC Report

De-Identification of Personal Information

- Data is not PII if it is *not reasonably linkable* to a specific consumer, computer or other device
- Breaking the link
  - Take reasonable measures to ensure that data is de-identified
  - Publicly commit to not try to re-identify
  - Contractually prohibit downstream recipients from trying to re-identify
  - Take measures to silo de-identified data from PII
- Cannot remove concerns by simply envisioning the sharing of only "de-identified" or anonymous data
- Must actually follow FTC guidance
  - Prohibitions in privacy policies against re-identification
  - Provisions in vendor contracts regarding re-identification
  - Systems designed to silo off de-identified data

BRYAN CAVE

FTC Report

Requirements for Affiliates and Subsidiaries

- Historically, divergent privacy policies and practices regarding information sharing with corporate affiliates and subsidiaries
- FTC Report views affiliates as "third parties" unless the affiliate relationship is "clear to consumers"
- Common branding is cited as sufficient to make a relationship clear
- Uncertainty remains
- Practical implications
  - Disclose affiliate sharing in privacy policy
  - Consider opt-in for sharing sensitive information with affiliates
  - Opt-out for non-sensitive information

BRYAN CAVE HRO

White House Privacy Framework

"Consumer Privacy Bill of Rights"

BRYAN CAVE HRO

White House Privacy Framework

Consumer Privacy Bill of Rights

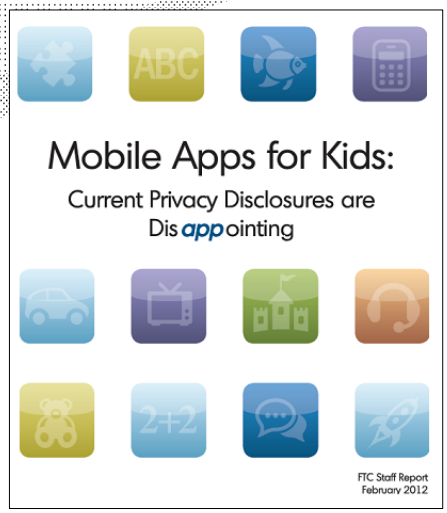
- Combined effort of the White House, Department of Commerce, and the FTC
- Provides a framework for consumer privacy protections
- Establishes principles covering personal data
- Proposes voluntary industry "codes of conduct" for privacy and security
  - Encourages inclusive and transparent process
  - Safe harbor status for compliance with an approved code

BRYAN CAVE

Mobile Applications

BRYAN CAVE

Mobile Applications



BRYAN CAVE

Mobile Applications

Increasing Activity In Mobile Privacy

- FTC report on Children's Mobile App's and Privacy (Feb. 16, 2012)
  - Large number of apps (75%) targeted at children (under 13)
  - Apps did not provide good privacy disclosures
  - Will conduct additional COPPA compliance reviews over the next 6 months
- FCRA Warning letters (Feb. 2012)
  - FTC sent letters to marketers of 6 mobile apps
  - Warned that apps may violate Fair Credit Reporting Act (FCRA)
  - If apps provide a consumer report, must comply with FCRA requirements
- FTC Workshops
  - New guidance for advertisers on online and mobile disclosures
  - Updates on the 2000 FTC "Dot Com Disclosures" guidelines for online ads
  - Emphasizing that consumer protection laws apply online and in mobile

BRYAN CAVE

Mobile Applications

Increasing Activity In Mobile Privacy

- States have become active as well
- California Attorney General (AG) announced that California state privacy law (Cal OPPA) applies to mobile applications (February 22, 2012)
- Cal OPPA requires conspicuous posting of privacy policy on mobile applications
- California AG issued warning letters to 100 mobile app developers in violation of Cal OPPA (October 24, 2012)
  - United Airlines, Delta Airlines, Open Table among those targeted
  - Threatens civil penalties of up to $2,500 for each download of non-compliant app

BRYAN CAVE

Mobile Applications

BRYAN CAVE

Mobile Applications

FTC Guide To Marketing Mobile Apps

- Released September 5, 2012
- Reiterates that the mobile market is not different from the Internet
- General "guidelines" or "principles" for mobile app developers
  - Tell the Truth About What Your App Can Do
  - Disclose Key Information Clearly and Conspicuously
  - Build Privacy Considerations in From the Start
  - Offer Choices that are Easy to Find and Easy to Use
  - Honor Your Privacy Promises
  - Protect Kids' Privacy
  - Collect Sensitive Information Only with Consent
  - Keep User Data Secure
- Acknowledges there can be no "one-size-fits-all" approach
- But also states that the laws apply to all companies

BRYAN CAVE

Civil Litigation

BRYAN CAVE

Data Breach/Privacy Litigation

Current State of Privacy Litigation

- Unprecedented number of filed cases (both data breach and unauthorized collection/use of personal information
- Emergence of a dedicated privacy plaintiffs' bar
- Not all bad news for defendants
  - Cases are routinely dismissed at the pleading stage (on Article III standing or inability to meet "actual injury" element of claim)
  - No out-of-pocket damages = No claim
- But the tide seems to be turning in favor of plaintiffs

BRYAN CAVE

Data Breach/Privacy Litigation

Current State of Privacy Litigation

- *Empirical Analysis of Data Breach Litigation,* Carnegie Mellon/Temple University Study (*February 19, 2012)*
- Monetary recovery/settlement positively correlated with number of records compromised, actual misuse of data, statutory damages
  - 3.5x more likely to draw a lawsuit if financial harm present
  - 6x lower when companies provide free credit monitoring
- Mean settlement value of $2,500 per affected individual
- Mean attorneys' fee figure of $1.2 MM
  - Google Buzz: $2.5mm
  - TD Ameritrade: $500K (knocked down from $1.8mm)
  - Facebook Beacon: $2.8mm (currently on appeal)
  - Facebook Sponsored Stories: $10mm?
- Cy pres settlements ranging from $50K to $9.5 MM

BRYAN CAVE

Insurance Coverage

BRYAN CAVE

Data Breach/Privacy Litigation

Does Insurance Cover Losses?

- Most comprehensive general liability (CGL) policies do not cover data losses
  - Only insure against claims for "bodily injury", "property damage", and "personal and advertising injury“
  - Many also exclude state unfair practices claims
- Lawsuits by insurers for a determination of non-coverage are becoming common
- More insurers are offering data breach and “cyber-liability” policies
  - Options and alternatives are growing
  - Choose wisely as exclusions may limit the benefits of coverage

BRYAN CAVE

What Should You Do?

BRYAN CAVE

Conclusion

Lessons Learned

- Increasing value means increasing scrutiny
- Enforcement will continue (and may increase)
  - Actual security breaches are not required
  - Focus is on reasonable and appropriate measures
  - Companies held to privacy-related promises
  - Scope of personal information is growing
- Enforcement actions are influencing and defining industry expectations (user and customer expectations too?)
- Your enforcement issue may not come from the FTC, but from a potential customer, financing source, or acquirer
- Premium on increased transparency into data practices

BRYAN CAVE

Conclusion

Best Practices

- Know your data (map data collection, usage, and sharing)
- Collect the data you need and hold it only as long as you need it
- Institute procedures to secure personal information and sensitive information
- Implement “privacy by design” concepts
- Prepare for a breach and adopt a written information security plan (WISP)
- Educate and train employees
- Manage and monitor vendors and contractors

BRYAN CAVE HRO

Thank You.

Jason Haislmaier
jason.haislmaier@bryancave.com
@haislmaier