

Privacy Law Symposium

Enforcement, Litigation and Insurance Coverage

KELLEY
DRYE

April 23, 2012

Agenda

- Panel 1: 12:30 – 1:20 PM
 - Avoiding an FTC Privacy Investigation and What To Do When You Find Yourself the Target of One
 - Presented by Dana B. Rosenfeld and Alysa Z. Hutnik
- Panel 2: 1:20 – 2:05 PM
 - Top Issues in Class Action Lawsuits Arising Out of Privacy, Data Security and New Media Technology
 - Presented by Keri E. Campbell and Lauri A. Mazzuchetti
- Panel 3: 2:15 – 3:00 PM
 - Insurance Coverage for Data Privacy Liability – Do You Already Have It, and If Not, Can You Buy It?
 - Presented by Edward E. Weiman and Richard D. Milone

KELLEY
DRYE

2

Avoiding an FTC Privacy Investigation and What To Do When You Find Yourself the Target of One

KELLEY
DRYE

Topics of Discussion

- Sources of FTC scrutiny
- FTC Privacy Report - key themes
- 5 Privacy Triggers for Enforcement/Litigation
- Practical tips to avoid becoming a target
- Tips for responding to an FTC CID/access letter

KELLEY
DRYE

4

5

Sources That Trigger FTC Scrutiny

Media Coverage



Congress



Consumer Complaints



FTC's Top 10 List

Rank	Category
1	Identity Theft
2	Debt Collection
3	Internet Services
4	Prices, Sweepstakes and Lotteries
5	Shop-at-Home and Catalog Sales
6	Imposter Scams
7	Internet Auctions
8	Foreign Money/Counterfeit Check Scams
9	Telephone and Mobile Services
10	Credit Cards

KELLEY DRYE

5



"Companies that fail to implement reasonable security safeguards to protect consumer information will come under our scrutiny."

- FTC Commissioner Julie Brill, January 26, 2012

"[FTC] Staff has a number of active investigations into privacy issues associated with mobile devices, including children's privacy."

- Jessica Rich, Deputy Director of FTC Bureau of Consumer Protection, April, 2011

"All companies involved in information collection and sharing on mobile devices – carriers, operating system vendors, applications, and advertisers – should provide meaningful choice mechanisms for consumers."

- FTC Staff, December 2010

KELLEY DRYE

FTC Privacy Report – Action Items

- FTC requests as a call to action:
 - Companies to implement best practices on privacy, as set forth in Report
 - Congress to enact baseline privacy/data security legislation with civil penalties
 - Industry to accelerate pace of self-regulation
- Scope
 - Commercial entities collecting/using consumer data reasonably linked to specific consumer, computer, or other devices, *unless* collects only non-sensitive data from fewer than 5,000 consumers/year and does not share it with 3Ps
- Privacy framework and suggested best practices
 - Privacy by design
 - Simplified choice for businesses and consumers
 - Greater transparency



FTC Report: What To Watch For in 2012

- Do-Not-Track
 - FTC urges organizations to complete implementation of easy-to-use, persistent, and effective browser Do-Not-Track system
- Mobile
 - FTC to host May 30, 2012 workshop to address mobile disclosures
- Data brokers
 - Push for data brokers to be more transparent in their operations and disclosure of collection and use of consumer data
- Large platform providers
 - FTC to host public workshop in second half of 2012 to explore issues related to comprehensive tracking by platform providers, such as Internet Service Providers, operating systems, browsers, and social media companies
- Promoting self-regulatory codes
 - FTC to work with Commerce and stakeholders to develop industry-specific codes of conduct

Top 5 Privacy Triggers for Enforcement/Litigation

1. Material misrepresentation in privacy policy
2. Inadequate PII safeguards
3. Inadequate consumer choices/control re: use of their PII
4. Inadequate/ disclosures about PII sharing
5. Unauthorized third party access

→ Usually a combination of more than one of these that triggers attention

Lessons Learned: *Google, Facebook, Twitter*



- ✗ Misrepresentation in privacy policy
- ✗ Automatic user enrollment
- ✗ Public default settings
- ✗ Deceptive opt-out provisions



- ✗ Misrepresentation in privacy policy and other statements
- ✗ Inadequate safeguards
- ✗ Unauthorized third party access



- ✗ Misrepresentation in privacy policy and in other statements
- ✗ Inadequate safeguards
- ✗ Unauthorized access by third-party apps and advertisers
- ✗ Unauthorized access to deleted user info

Same Lessons Reflected in Other Actions

- **FTC v. Upromise, Inc.**
 - Accused of misleading users about the extent to which it collected and transmitted personal information
 - Allegedly failed to adequately secure the user information that was collected
- **FTC v. Chitika, Inc.**
 - Accused of tracking consumers' online activities even after they opted out of online tracking
- **FTC v. ScanScout, Inc.**
 - Accused of advising that Flash cookies could be removed through browser settings



Practical Tips To Avoid Becoming a Target

- “Bake it in” – privacy by design
- Empower consumers with real choices
- Say what you do and do what you say
 - Transparency
 - Disclosure
 - Consent

“Bake It In”: Privacy by Design



Means actually having a privacy program

- Designate trained employees
- Risk assessment of data linked to consumers in product design & PII use
- Risk assessment of organization's data security safeguards
- Implement controls and procedures
- Privacy controls as to selection/use of service providers
- Independent auditing of privacy program
 - ✓ *FTC urges Google/FB Settlement Terms be used as model for best practices*

Empower Consumer Choice



Controls

- Simplify choice
 - *So people can understand the choice and act on it*
- Opt-out provisions

Cautionary tale:
Congressional scrutiny
over changes to Google's
privacy policy that limits
consumers' ability to opt-
out

Congress of the United States
Washington, DC 20515
January 26, 2012

Mr. Larry Page
Chief Executive Officer
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Page:

On January 24, 2012, Google announced the consolidation of virtually all of its existing privacy policies into one main privacy policy for Google products. According to an article in *The Washington Post*, it became clear that Google, which can already "combine the information you submit under your account with information from other Google services or third parties."

Say What You Do & Do What You Say

- ✓ Transparency
 - Collection and protection of information
 - Consumer control and access
 - Accessibility to third parties

- ✓ New or additional sharing
 - Disclosures
 - Consent

Responding to a CID/Access Letter

- Initial steps
- CID/access letter scope
- ESI
- Production
- Privilege log
- Advocacy



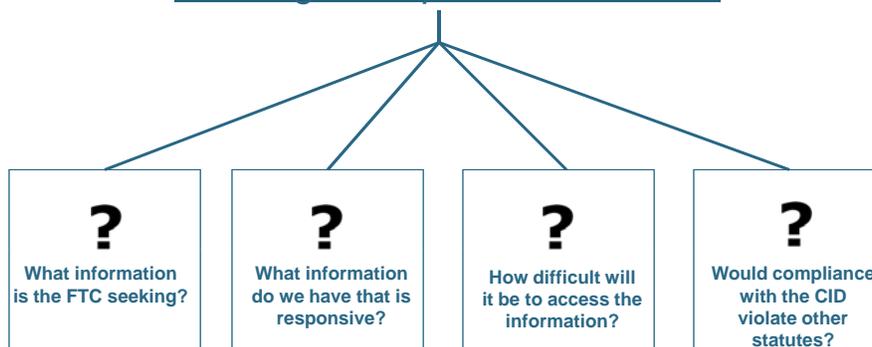
Initial Steps

- 20-day clock is ticking: take it seriously and take action immediately
- Review the document
 - Nature and scope of the Investigation
 - Definitions
 - Instructions
 - Interrogatories / Document Requests
- Hire expert counsel in FTC consumer protection matters
- Identify key internal team w/ knowledge



Assess Investigation Scope

Creating a Response Framework



CID Scope *cont.*

Burden Letter

- Identify which requests present an unreasonable burden (& be realistic on what is actually going to be considered burdensome)
- Develop a detailed narrative and quantify the burden
- Propose reasonable alternatives
- Submit to the FTC early in the process and keep it rolling – Need to demonstrate cooperation and taking the CID seriously
- Also have a good idea of what you can produce soon and when that production will occur



Accounting for ESI

- Legal hold memo
 - Immediately prepare & send to relevant employees and officers
 - Specify dates and types of information covered by the hold
- Suspend auto-delete features where applicable
- Identify internal email custodians & databases/systems



Production of Responsive Documents

- Follow the new BCP Production Guide or work to resolve with Staff if there are issues with compliance
- Provide a letter that explains the scope of your response to each request for information within the CID
- Respond on time
- Assert confidentiality protections and protections against FOIA requests and SAFE-WEB ACT sharing



Advocacy- Tell Your Side of the Story

- Provide written narrative (the white paper)
 - Craft a positive story with key facts; avoid data dump
 - Send soon after you've completed the final document production
- Discuss built-in privacy protections (privacy by design)
 - Data collection, purpose, and retention; secure consumer and third-party access; consumer experience
- Address compliant company practices
 - Scope of data collected and permitted uses; contractual protections/monitoring; risk assessment
- Include new initiatives
 - Based on industry guidelines/best practices
- Request meeting
 - Ask for a meeting with staff to discuss the case (and your side of the story)

Questions?



Dana B. Rosenfeld

PARTNER
Privacy & Information Security
Advertising & Marketing
(202) 342-8588
drosenfeld@kelleydrye.com



Alysa Z. Hutnik

PARTNER
Privacy & Information Security
Advertising & Marketing
(202) 342-8603
ahutnik@kelleydrye.com

Connect with Kelley Drye

Web: www.KelleyDrye.com

 /KelleyDryeAdLaw

Blog: www.AdLawAccess.com

 @KelleyDryeAdLaw

KELLEY
DRYE

Top Issues in Class Action Lawsuits Arising Out of Privacy, Data Security and New Media Technology

KELLEY
DRYE

If it isn't the Government ...

- Increase in Class Actions in the areas of privacy and data security
- Cases are predominantly being filed in Federal Court
- The areas of primary focus:
 - “Flash Cookies” and behavioral advertising
 - Mobile devices and mobile device applications
 - Data breaches
- Harm alleged is unexpected collection and use of personal information

Topics of Discussion

- What has the response been to these class actions?
- What are some common defenses being asserted?
- How are the Courts handling these class actions?
- What are common claims asserted by Plaintiffs and how are Defendants responding?

How are Defendants Responding?

- Defendants moving to dismiss prior to class certification
- Primary argument is that Plaintiffs lack Article III standing
- Federal Courts in California (in both the Central and Northern District) seem to be in agreement with Defendants

Article III Standing

- To satisfy Article III, a plaintiff must show:
 - “(1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical;
 - (2) the injury is fairly traceable to the challenged action of the defendant; and
 - (3) it is likely, as opposed to merely speculative that the injury will be redressed by a favorable decision.”

Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc., 528 U.S. 167, 180-81 (2000).

Standing in Class Actions

- At least one named plaintiff must have suffered an injury in fact. *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F. 3d 1018, 1022 (9th Cir. 2003).
- The named plaintiff must allege a concrete, particularized injury to him or herself, as opposed to “consumers” in general.

In re iPhone Application Litig., 11-MD-2250, 2011 WL 4403963 at *4 (N.D. Cal.); *Birdsong v. Apple, Inc.*, 590 F.3d 955, 960-61 (9th Cir. 2009).

Case Study: In re iPhone Application Litig.

- In re iPhone Application Litig., 11-MD-2250, 2011 WL 4403963
- Apple’s Operating System allowed third party applications to collect and transmit personal information stored on an iDevice, without user consent or knowledge
- Defendants’ successfully moved to dismiss on the grounds that:
 - Plaintiffs lacked standing because they did not suffer an injury in fact
 - Plaintiffs failed to state a claim as to each cause of action

Case Study: In re Facebook Privacy Litig.

- The Court denied motion to dismiss for lack of Article III standing
- The Court found that Plaintiffs had injury in fact based on alleged violations of The Wire Tap Act and the SCA
- Court granted motion to dismiss for failure to state a claim
 - Plaintiffs had not adequately pled the statutory claims
 - Not entitled to relief under the UCL personal information does not constitute property for the purposes of the UCL
 - Not entitled to relief under the CLRA because not consumers

Other Cases Dismissed For Lack of Standing

- *Low v. LinkedIn Corporation*, Case No. 11-CV-1468, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011)
 - Plaintiffs only allegation of harm was the unauthorized collection of personal data
 - Court found that unauthorized collection of personal data, by itself, does not create an economic loss
- *LaCourt v. Specific Media*, Case No. CV-10-1256, 2011 WL 2473399 (C.D. Cal. April 28, 2011)
 - No standing because no allegation that named plaintiff was actually harmed by defendant's conduct
 - Plaintiffs only alleged general, unspecified harm by the use of their personal information such as "opportunity costs," "value for value exchange" and "consumer choice"

Exception – Data Theft Cases

- *Krottner v. Starbucks*, 628 F.3d 1139 (9th Cir. 2010)
 - Company laptop containing social security numbers and employment information of 97,000 employees was stolen
 - Standing satisfied by allegations of generalized anxiety and emotional distress as result of the data theft. These allegations were insufficient to state a claim for negligence and the dismissal of the claims was upheld.
- *Ruiz v. Gap*, 380 F. Appx. 689 (9th Cir. 2010)
 - Theft of a laptop computer which contained Plaintiffs' personal information, including social security numbers of 750,000 applicants
 - Future risk of identity theft sufficient to establish standing for negligence claim but claim ultimately dismissed because increased risk of identity theft insufficient to establish damages for negligence

Exception – Data Theft Cases

- *Anderson v. Hannaford Brothers Co.*, 659 F. 3d 151 (1st Cir. 2011)
 - Theft of customer's credit card and debit card information
 - First Circuit reinstated Plaintiffs' claims for negligence and implied contract
 - Alleged monetary damages relating to costs in replacing credit cards and debit cards, as well as the premiums paid by victims for the purchase of identity theft insurance were sufficient to state claims for negligence and implied contract

Standing Through A Statutory Violation

- The injury required by Article III can exist solely by virtue of statutes creating legal rights, the invasion of which creates standing. *Warth v. Seldin*, 422 U.S. 490, 500 (1975).
- A finding that plaintiff has standing does not equate with a finding that they have stated a claim. *Doe v. Chao*, 540 U.S. 614, 624-25 (2004) (a plaintiff may have “injury enough to open the courthouse door, but without more [may have] no cause of action” under which he can successfully obtain relief.”)

Claims Asserted By Class Action Plaintiffs

- Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 *et. seq.*
 - Provides a civil remedy against whoever intentionally accesses a computer without authorization or exceeds authorization and obtains information from a protected computer
 - Requires a plaintiff to show that he or she suffered economic damages or loss of at least \$5,000 in a one-year period in order to maintain a claim
- Electronic Communications Privacy Act
 - Title I -- The Wiretap Act, 18 U.S.C. 2511 *et. seq.*
 - Forbids intentionally divulging the contents of a communication while in transmission other than to the addressee or intended recipient
 - Title II -- Stored Communication Act (SCA), 18 U.S.C. § 2702 *et. seq.*
 - Forbids knowingly divulging the contents of a communication in electronic storage except: to an addressee or intended recipient

Claims Asserted By Class Action Plaintiffs

- California Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et. seq.*
- California Consumer Legal Remedies Act (CLRA), Cal. Civil Code § 1750 *et. seq.*
- Computer Crime Law, Cal. Penal Code § 502
- Common law claims for negligence, breach of contract and breach of the implied covenant of good faith and fair dealing

Case Study: In re Facebook Privacy Litig.

- In re Facebook Privacy Litig., Case No. C10-2389, 791 F. Supp. 2d 705 (2011 N.D. Cal.); also 2011 WL 6176208 (N.D. Cal.)
- Plaintiffs alleged that Facebook transmitted user's personal information to third-party advertisers without the user's knowledge or consent
- Plaintiffs asserted causes of action under the Wire Tap Act, the SCA, the Computer Crime Law, the UCL, the CLRA and common law claims.
- Harm alleged was the diminution in value of the Plaintiffs personal information

Case Study: In re Facebook Privacy Litig.

- The Court denied motion to dismiss for lack of Article III standing
- The Court found that Plaintiffs had injury in fact based on alleged violations of The Wire Tap Act and the SCA
- Court granted motion to dismiss for failure to state a claim
 - Plaintiffs had not adequately pled the statutory claims
 - Not entitled to relief under the UCL personal information does not constitute property for the purposes of the UCL
 - Not entitled to relief under the CLRA because not consumers

Plaintiffs' Success – California Civil Code Section 3344

- *Fraleigh v. Facebook*, 11-CV-1726, 2011 WL 6303898 (N.D. Cal.) Class certification motion set for May 24, 2012
- Plaintiffs allege that the unauthorized use of their name and likeness in Facebook's "Sponsored Stories" violated California Civil Code § 3344.
- The Court found that Plaintiffs had standing based on their Civil Code Section 3344 claim
- "Plaintiffs articulated a coherent theory of how they were economically injured by the misappropriation of their names, photographs and likenesses for use in paid commercial endorsements ... without their consent." *Id.* at *9.

Standing v. Failure to State A Claim

- Distinction made by Court's in standing v. failure to state a claim analysis can be close
 - *Gaos v. Google, Inc.*, C-10-4809 (2011 WL 7295480) (N.D. Cal.) Claim under the SCA dismissed for lack of standing because Plaintiff failed to "plead facts sufficient to support a claim for violation of her statutory rights." *Id.* at *3.
 - *In re Zynga Privacy Litigation*, C-10-4680 (2011 WL 749170 (N.D. Cal.) Standing based on allegation of violation of the The Wire Tap Act but Court still dismissed for failure to state a claim

Pitfalls In Commonly Pled Statutory Claims

- CFAA
 - Plaintiffs cannot establish \$5,000 in economic loss
 - Plaintiffs often agree to the complained of behavior in click-through "Terms of Use" and therefore defendants have not acted "without authorization"
- SCA and The Wire Tap Act
 - Allows transmission to the addressee or the intended recipient of the communication
 - Plaintiffs actions – such as clicking on ad banners – make a third party an intended recipient of the communication
- California Computer Law
 - Limited to circumstances where access is gained by overcoming technological barriers (hacking)

Pitfalls – Unfair Competition Laws

- CLRA
 - Protects consumers from deceptive actions relating to the sale of goods or services
 - Computer software is not a “good” or “service”
 - Individuals who register for free on websites are not consumers
- UCL
 - Must show a loss of “money” or “property”
 - Personal information is not “property”

Concepcion and Agreements to Arbitrate on an Individual Basis

Before *Concepcion* . . .

- 1925 → Federal Arbitration Act (FAA)
- Businesses begin including arbitration provisions in their consumer agreements in the 1990s
- Plaintiffs' response → the clauses are unenforceable
 - State law unconscionability theories
 - Barred by statute
- Mixed results in the courts
- *Green Tree Financial Corp. v. Bazzle*
 - Plurality held that where an arbitration agreement was silent regarding the availability of class-wide relief, an arbitrator, and not a court, must decide whether class relief is permitted
 - Lower courts began sending businesses with "silent" arbitration clauses to arbitration

Before *Concepcion* . . .

- AAA and other arbitration providers promulgate rules for class arbitrations
 - AAA Rule → it was the initial duty of an arbitrator to "determine as a threshold matter, in a reasoned, partial final award on the construction of the arbitration clause, whether the applicable arbitration clause permits the arbitration to proceed on behalf of or against a class"
- Many businesses are forced into class arbitration
 - From 2003 to 2009, the AAA issued 135 Clause Construction Awards; on only 7 occasions that the arbitration clause did not permit the arbitration to proceed on behalf of a class
- Business responds → revise arbitration agreements to include class action waivers

Before *Concepcion* . . .

- California, New Jersey and minority of jurisdictions hold that, at least in some circumstances, class action waivers are unconscionable or barred by statute
 - *Discover Bank* Rule
- Majority view: arbitration agreements containing class action waivers are enforceable when:
 - The consumer's share of arbitration costs is capped at or below the equivalent court filing fee; and
 - Remedies not limited in arbitration

Stolt-Nielsen: April 27, 2010

- “a party may not be compelled under the FAA to submit to class arbitration unless there is a contractual basis for concluding that the party *agreed* to do so.”
- forcing parties to submit to class arbitration in the absence of such contractual language is “fundamentally at war with the foundational FAA principle that arbitration is a matter of consent.”
- But . . . *Stolt-Nielsen* did not solve the *Discover Bank* problem

The USSC's Decision in *Concepcion*

- California's *Discover Bank* rule is preempted by the FAA
- “Requiring the availability of class-wide arbitration interferes with the fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA.”
- Majority decision expressly rejects dissent's argument regarding the possibility of exculpatory effect of class-action waivers:

“The dissent claims that class proceedings are necessary to prosecute small-dollar claims that might otherwise slip through the legal system. But States cannot require a procedure that is inconsistent with the FAA, even if it is desirable for unrelated reasons.”

A Year In Review. . .

- Plaintiffs get creative
 - Attempt to distinguish the *Discover Bank* rule from other similar state law rules
 - Argument regarding the vindication of federal or state law statutory rights
 - Argument that the arbitration provision/contract is unconscionable on other grounds
 - Argument that *Concepcion* does not apply to injunctive or representative relief claims

A Year In Review. . .

- Most federal courts read *Concepcion* broadly
 - *Cruz v. Cingular Wireless LLC*, 648 F. 3d 1205, 1214 (11th Cir. Aug. 11, 2011)
 - *Litman v. Cellco P'ship*, 655 F.3d 225, 231 (3d Cir. Aug. 24, 2011)
 - *Kilgore v. Keybank Nat'l Ass'n*, 673 F.3d 947 (9th Cir. Mar. 7, 2012)
 - *Quilloin v. Tenet HealthSystem Philadelphia, Inc.*, 673 F.3d 221 (3d Cir. Mar. 14, 2012)
 - *Conneff v. AT&T*, 2012 WL 887598 (9th Cir. Mar. 16, 2012)

A Year In Review

- Some judicial hostility towards *Concepcion*
 - Acceptance of waiver arguments on hyper technical grounds
 - California state court holds that Private Attorney General Act (PAGA) claim cannot be required to be arbitrated on an individual bases. See *Brown v. Ralph's Grocery*, 197 Cal. App. 4th 489 (2011); but see *Quevedo v. Macy's Inc.*, 2011 WL 3135052 (C.D. Cal. June 16, 2011)
 - Courts refuse to enforce "illusory" agreements where drafter reserves the right to change agreement. See *Carey v. 24 Hour Fitness USA, Inc.*, 669 F.3d 202 (5th Cir. 2012)
 - Vindication of statutory rights/costs of arbitration arguments gain traction
 - *In re Am. Express Merchants' Litig.*
- Acceptance of other unconscionability arguments
 - *Sanchez v. Valencia Holding Co.*, 132 Cal. Rptr. 3d 517 (Cal. Ct. App. 2011)
 - *In re Checking Account Overdraft Litigation MDL*

A Year In Review . . .

- Two Important Ninth Circuit cases last month. . .
 - *Coneff* rejects plaintiffs' argument regarding the inability to effectively vindicate statutory rights
 - *Kilgore* holds that *Broughton* and *Cruz* rules did not survive *Concepcion*
- California Supreme Court will review *Sanchez*

A Year In Review. . .

- USSC: *In case you didn't hear me the first time . . .*
 - Issued summary orders in various post-*Concepcion* petitions for certiorari
 - *Missouri Title Loans v. Brewer*
 - *Sonic-Calbasas, Inc. v. Moreno*
 - *Branch Banking and Trust v. Gordon*
 - Signaled some expansion of *Concepcion*
 - *CompuCredit Corp. v. Greenwood*, 565 U.S. __ (Jan. 10, 2012)
 - *Marmet Health Care Center, Inc. v. Brown*, 565 U.S. __ (Feb. 21, 2012)

How do I draft an arbitration agreement after *Concepcion*?

- Make the requirement of arbitration provision prominent in the contract
- Include a class action waiver (individual arbitration only)
- Reference that the FAA, and not state law, governs the arbitration clause (make choice of law provision consistent)
- Include both common law and statutory claims within the scope of arbitration clause
- Disclose that arbitration means no trial by jury
- Business to pay costs of arbitration (or make affordable)

How do I draft an arbitration agreement after *Concepcion*?

- Mutuality: Both parties agree to arbitrate claims
- Do not limit legal remedies
- Provide for a reasonably convenient location
- Select an appropriate arbitration provider (AAA or JAMS), identify applicable rules and advise where rules can be located
- Check provider rules on minimum standards for arbitration clauses
- Do not require confidentiality

Questions?



Lauri A. Mazzuchetti

PARTNER
Litigation
(973) 503-5910
lmazzuchetti@kelleydrye.com



Keri E. Campbell

PARTNER
Litigation
Entertainment and Media
(310) 712-6145
kcampbell@kelleydrye.com

KELLEY

DRYE

Insurance Coverage for Data Privacy Liability – Do You Already Have It, and if Not, Can You Buy It?

KELLEY

DRYE

Why Are We Here?



- Average Cost of Data Breach = **\$5.5 million**
 - Down from **\$7.2 million**
- Average Cost Per Record = **\$194**
 - Down from **\$214**
- First-Time Breach
 - Average Cost is **\$37 More Per Record**
- Highest Cost
 - **\$20,881,794**

Why Are We Here?



- Industry Segments

Financial	Industrial	Technology
Retail	Healthcare	Media
Hospitality	Public	Transportation
Services	Consumer	Communications
Education	Pharmaceutical	

Roadmap

- CGL Policies
 - Relevant Provisions
 - Leading Case Law
- Other Sources of Coverage
 - Property, E&O, Crime, Etc.
 - Specialty Policies
 - Common Provisions/Exclusions



Is Failure to Consider Potentially Applicable Insurance Coverage a Malpractice Trap?

- *Jordache Enterprises, Inc. v. Brobeck Phleger & Harrison*, 958 P.2d 1062 (Cal. 1998) (failure to provide notice to insurers potentially gives rise to malpractice, but “actual injury” occurs when client sustains loss, and therefore SOL had run on client’s claim)
- Solution: Address insurance coverage in law firm’s standard retention letter



Liability Insurance Claims Turn on Three Variables

- 1) Policy language
 - Many policies are written on Standard Insurance Services Office (“ISO”) forms.
 - Many insurers use their own forms
- 2) Allegations and proof in the underlying lawsuit
- 3) State law on insurance coverage issues

Comprehensive General Liability (CGL)

Is there CGL coverage
for data privacy suits?

YES!

(with some caveats)



Comprehensive General Liability (CGL)

COVERAGE B PERSONAL AND ADVERTISING INJURY LIABILITY

1. Insuring Agreement

- a. **We will pay those sums that the insured becomes legally obligated to pay as damages because of “personal and advertising injury” to which this insurance applies.** We will have the right and duty to defend the insured against any “suit” seeking those damages. However, we will have no duty to defend the insured against any “suit” seeking damages for “personal and advertising injury” to which this insurance does not apply. We may, at our discretion, investigate any offense and settle any claim or “suit” that may result.

Comprehensive General Liability (CGL)

14. “Personal and advertising injury” means injury, including consequential “bodily injury”, arising out of one or more of the following offenses:
- a. False arrest, detention or imprisonment;
 - b. Malicious prosecution;
 - c. The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies, committed by or on behalf of its owner, landlord, or lessor;
 - d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person’s or organization’s goods, products or services;
 - e. **Oral or written publication, in any manner, of material that violates a person’s right of privacy;**
 - f. The use of another’s advertising idea in your “advertisement”; or
 - g. Infringing upon another’s copyright, trade dress or slogan in your “advertisement”.

Comprehensive General Liability (CGL)

- e. Oral or written publication, in any manner, of material that violates a person's right of privacy;

“Publication”

“Material”

“Right of Privacy”

Netscape vs. Federal

Netscape Communications Corp. vs. Federal Ins. Co., 2007 WL 2972924 (N.D. Cal.), aff'd in part, rev'd in part, 343 Fed. Appx. 271 (9th Cir. 2009)

- Netscape was accused of gathering personal data from internet users for targeted advertising
- Slight variation on ISO language: “Making known to any person or organization written or spoken material that violates a person's right to privacy”
- Allegation that Netscape “made known” information to itself was sufficient to trigger duty to defend

Netscape vs. Federal

Exclusion for “deliberately breaking the law” does **not** apply

District court held that an exclusion for “online activities” precluded coverage, BUT

Ninth Circuit affirmed the finding of “personal and advertising injury,” and reversed application of the “online activities” exclusion

Takeaway: Disclosing personal data of another satisfies the “right of privacy” prong of the definition of “personal and advertising injury”

Cases Interpreting “Right of Privacy”

American Family Mut. Ins. Co. v. C.M.A. Mortgage, Inc. 2008 WL 906230 (S.D. Ind.) (finding coverage for suit alleging unauthorized use by a mortgage company of an individual plaintiff’s credit report in a solicitation)

Zurich Am. Ins. Co. v. Fieldstone Mortgage Co., 2007 WL 3268460 (D. Md.) (same)

Pietras vs. Sentry Ins. Co., 2007 WL 715759 (N. D. Ill.) (same analysis applied to class action suit, and exclusions held inapplicable under “Illinois estoppel” rule)

Recall Total Management vs. Federal Ins. Co., 2012 WL 469988 (Conn. Super. Ct. January 17, 2012) (no coverage for transport vendor when a cart containing computer tapes of sensitive IBM employee data fell from a van, because no “publication,” and no actionable violation of the employee’s “right of privacy”).

Why So Few Cases?

- Policyholders want to avoid publicity?
- Insurers accept coverage and pay promptly and cheerfully?
- Insurers reject coverage and policy holders fail to pursue it?
- Cases have not yet reached the point of decision?

Zurich American Ins. Co. vs. Sony

April 16-19, 2011

Hackers gained access to two of Sony's networks which supports its PlayStation devices

- Gained access to personal and financial information of 77 million customers

June 3, 2011

Hackers gained access to a third Sony network, resulting in access to additional customers' private information

55 U.S. class action complaints, mostly in California, plus 3 Canadian class actions

- consolidated into an MDL
- motion to dismiss filed March 16, 2012

Potential Exposure: Very High



Zurich American Inc. Co. v. Sony



On July 20, 2011, Zurich sued 8 Sony entities and numerous other Sony insurers in New York State court for a declaration of no coverage.

- Zurich took no definitive coverage position until after suit was filed
- Sony filed a competing action shortly afterwards in California state court in San Diego
- Forum dispute (likely) was resolved by a March 2012 decision dismissing Sony's California case

Zurich vs. Sony (cont.)

- **Why Did Zurich Sue Sony Preemptively?**
 - Big dollar claim?
 - New and unexpected exposure?
 - Precedential effect?
 - Choice of law?
 - Publicity?



Zurich vs Sony (cont.)

- Defenses to date are cryptic
- Likely Issues:
 - Is there “personal and advertising injury”?
 - Exclusions

Zurich vs. Sony (cont.)

Knowing Violation Of Rights of Another

“Personal and advertising injury” caused by or at the direction of the insured with the knowledge that the act would violate the rights of another and would inflict “personal and advertising injury”.



Zurich vs. Sony (cont.)

Criminal Acts

“Personal and advertising injury” arising out of a criminal act committed by or at the direction of the insured.



Zurich vs. Sony (cont.)



Insureds in the Media and Internet Type Businesses

“Personal and advertising injury” committed by an insured whose business is:

- (1) Advertising, broadcasting, publishing or telecasting;
- (2) Designing or determining content of websites for others;
- (3) An Internet search, access, content or service provider.

Zurich vs. Sony (cont.)



Distribution Of Material In Violation Of Statutes

“Personal and advertising injury” arising directly or indirectly out of any action or omission that violates or is alleged to violate:

- (1) The Telephone Consumer Protection Act (TCPA), including any amendment of or addition to such law; or
- (2) The CAN-SPAM Act of 2003, including any amendment of or addition to such law; or
- (3) Any statute, ordinance or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating or distribution of material or information.

Comprehensive General Liability – Notice

- The importance of giving prompt notice
- CGL policies have a two-tiered notice requirement

Comprehensive General Liability - Notice

Duties In The Event of Occurrence, Offense, Claim or Suit

a. You must see to it that we are notified as soon as practicable of an “occurrence” or an offense which may result in a claim. To the extent possible, notice should include:

- (1) How, when and where the “occurrence” or offense took place
- (2) The names and addresses of any insured persons and witnesses; and
- (3) The nature and location of any injury or damage arising out of the “occurrence” of offense.

Comprehensive General Liability - Notice

b. If a claim is made or “suit” is brought against any insured, you must:

- (1) Immediately record the specifics of the claim or “suit” and the date received; and
- (2) Notify us as soon as practicable.

You must see to it that we receive written notice of the claim or “suit” as soon as practicable.

Coverage for FTC or other Agency Proceedings

“Suit” means a **civil proceeding** in which **damages** because of “bodily injury,” “property damage” or “personal and advertising injury” to which this insurance applies are alleged.

Will likely turn on the remedy sought and how it can be characterized.

Money Damages – YES

Fines, penalties, disgorgement of profits, injunctive relief – less likely

Only one potentially covered component is needed for duty to defend.

Comprehensive General Liability - Exclusions

- Insurers are beginning to add “Breach of Security Excursions”
- Offers compelling argument in favor of coverage for policies without exclusions
- Will likely be phased in over time

Property Insurance Coverage



- Issue
 - Does damage to electronic information constitute “direct physical damage”?
- *NMS Servs. Inc. v. The Hartford*, 62 F. App'x 511 (4th Cir. 2003)
 - Hacking event
 - Exclusion for acts by persons entrusted with property
 - District court granted summary judgment
 - Fourth Circuit reversed

Property Insurance Coverage



- Issue
 - Does damage to electronic information constitute “direct physical damage”?
- *Landmark Amer. Ins. Co. v. Gulf Coast Analytical Labs., Inc., No.*, 10-809, 2012 U.S. Dist LEXIS 45184 (M.D. La. Mar. 30, 2012)
 - Data corrupted when system failed
 - Hartford argued data was intangible
 - District court disagreed
 - Data was intangible *but still physical*

Property Insurance Coverage



- Issue
 - Does physical damage include loss of use?
- *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000)
 - Power outage
 - No physical damage
 - “Physical damage” is not restricted to physical destruction
 - Criminal statutes relevant to analysis

Property Insurance Coverage



- Issue
 - Does loss of use constitute “loss” of property?
- *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, No. 11-6187, 2012 U.S. Dist. LEXIS 44401 (D. N.J. Mar. 29, 2012)
 - Hackers took over servers
 - Hartford argued neither a “transfer” nor a “loss” of property
 - District court held
 - policy was ambiguous
 - loss of use qualifies as “loss” of property

E&O Liability Coverage



- Issue
 - Is the damage “accidental”?
- *Eyebalster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010)
 - Third party coverage
 - Allegations were of intentional acts
 - District court rejects claims
 - Eighth Circuit reverses
 - Act must be “intentionally wrongful”

Crime & Fidelity Policies



- *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, Case No. 06-443 (S.D. Ohio Mar. 30, 2009)
 - Hacking event
 - \$6 million in losses
- *Scottrade, Inc. v. The St. Paul Mercury Ins. Co.*, No. 4:09-cv-01855-SNLJ (E.D. Mo. Nov. 12, 2009)
 - Hacking events (over two years)
 - \$13.8 million in losses

Specialty Policies

ACE	Admiral	Allied World
Arch	AXIS	Beazley
Brit	CFC	Chartis
Chubb	CNA	Crum & Forster
Digital Risk	Essex	Euclid
General Star	The Hartford	HCC
Hiscox	Ironshore	Liberty International
Markel	NAS	Navigators
OneBeacon	Philadelphia	RLI
Safeonline	ThinkRisk	Travelers
XL	Zurich	

Specialty Policies

ACE	Admiral	Allied World
Arch	AXIS	Beazley
Brit	CFC	Chartis
Chubb	CNA	Crum & Forster
Digital Risk	Essex	Euclid
General Star	The Hartford	HCC
Hiscox	Ironshore	Liberty International
Markel	NAS	Navigators
OneBeacon	Philadelphia	RLI
Safeonline	ThinkRisk	Travelers
XL	Zurich	

Policies



- Security and Privacy Protection
- Cyber Security Liability
- Network Security and Privacy Liability
- Electronic Data Processing Coverage
- Internet Liability & Network Protection
- Network Risk Insurance
- Breach Response
- Etc.

Common Coverage Provisions



- Digital Asset Loss
 - Corruption or destruction of data due to security failure
 - First party
 - Third party
 - Devil is in the definitions
 - Inability to prevent unauthorized access or use of computer system and/or introduction of malicious code resulting in
 - Corruption or destruction
 - Interruption

Common Coverage Provisions

- Cyber Extortion Coverage
 - Credible threat to . . .
 - Release information
 - Introduce malicious code
 - Corrupt, damage, or destroy
 - Restrict or hinder access
 - Rewards



Common Coverage Provisions

- Breach Response
 - aka Crisis Management
 - aka Security Failure Notification Loss
- Can Include
 - Compliance with privacy laws
 - Legal expenses
 - Forensic consultants
 - Public relations



Common Coverage Provisions



- Security and Privacy Liability
 - Typical third-party coverage
 - Actual or alleged negligent act, error or omission
- Employee Privacy Liability
 - Third-party liability to employees
 - HIPAA, COPPA, FCRA, etc.
- Electronic Media Liability Coverage

Common Coverage Provisions



- Business Interruption Loss
- Contingent Business Interruption Loss

Less Common Coverage Provisions

- *Regulatory Proceedings & Fines*
- *Breach Preparedness Support*
- *E-Vandalism Expenses Support*

Typical Exclusions



- Losses resulting from acts of insured, directors, trustees, officers, risk managers, managers, etc.
- Power outages, utility failures, etc.
- Seizures under governmental authority
- Design failures
- Inadequate maintenance or security measures
- Spyware, unsolicited fax, e-mail, telephone calls, etc. by the insured.
- “[A]ny self propagating Malicious Code or other distributed attacks, including viruses, worms and malware.”

Questions?



Edward E. Weiman

PARTNER

Litigation

Insurance Recovery

(310) 712-6177

eweiman@kelleydrye.com



Richard D. Milone

PARTNER

Litigation

Insurance Recovery

(202) 342-8425

rmilone@kelleydrye.com