Social Media And Legal Risk: Making the Web Work Well

Jay Ward Brown Managing Partner at Levine Sullivan Koch & Schulz, LLP
Pat Lieske - Axis, Vice President - Media
Christi Deardorff - Hiscox USA, Senior Vice President - Media/Entertainment
8 Key Social Media Legal Risks

1. Defamation and Section 230 of the CDA
2. Copyright, Fair Use, Public Domain and DMCA
3. Trademark
4. Trade Secrets and Confidential Information
5. Control of Social Media Accounts
6. Marketing on Social Media
7. Contests and Sweepstakes on Social Media
8. Insurance Coverage for Social Media Exposures
1. Defamation and Section 230 of the CDA
Section 230 of the federal Communications Decency Act generally provides immunity for hosting third party content online:

• “No provider or user of an Interactive Computer Service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1).
• “No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” 47 U.S.C. § 230(d)(3).

Section 230 comes into play when a user posts content on another’s website.
The CDA Protects You if the Content Is the Work of “Another”

- The CDA’s protection from suit applies only if the content is posted by “another” Information Content Provider.
- So, if a company or its employees or agents is the “creator or developer” of the content, in whole or even “in part,” then the CDA will NOT protect the company.
The CDA does NOT protect website from Intellectual Property claims:

- Copyright infringement
- Trademark infringement
- Misappropriation of the Right of Publicity (in some jurisdictions)
• Section 230 generally provides immunity for links to and retweets of third party content.

• This is because the content at issue – the linked website or the original tweet – is “information provided by another information content provider.”

• HOWEVER: There could be risk if the forwarder appears to have *adopted or endorsed* the content.
2. Copyright, Fair Use, Public Domain and DMCA
Key Concern: The Internet

- The Internet is not a copyright-free zone!
- It’s not automatically legal to use materials posted on:
Copyright

An original work of authorship, generally artistic or scholarly, in a fixed medium such as written down on paper or recorded digitally. Ideas are not protected, but the unique, tangible expressions of them are.

Copyrights, unlike Trademarks, do not need to be formally registered, but to bring an infringement lawsuit, or to receive statutory damages, the majority of US courts require registration or at least an application for registration.

Duration: Individual – life of the author plus 70 years. Corporate – lesser of 120 years after creation or 95 years after publication.
“For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with us. This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.”
Fair Use

A limitation and exception to the exclusive rights granted by copyright law. US doctrine that permits limited use of copyrighted material without acquiring permission from the rights holders for purposes such as criticism, comment, news reporting, teaching, scholarship or research. Four factor analysis to determine fair use.

1. The purpose and character of the use; including whether such use is of a commercial nature or is for nonprofit educational purposes;
   – To justify the use as fair, one must demonstrate how it either advances knowledge or the progress of arts through something new. Is the new work transformative or derivative?

2. The nature of the copyrighted work
   – The social usefulness of freely available information is weighed against the appropriateness of private ownership. [Zapruder film]
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole
   – In general, the less that is used in relation to the whole makes it more likely the sample will be considered fair use.
     • A political magazine lost a case where their 400 word excerpt of President Ford’s memoir was deemed to represent “the heart of the book”, and was thus substantial.

4. The effect of the use upon the potential market for or value of the copyrighted work
   – Does the work act as a direct market substitute?
     • A company made unauthorized movie trailers to distribute to video retailers and were in violation against the official trailers.
Works that are unavailable for private ownership: Intellectual property rights have expired; been forfeited; or are inapplicable.

Examples:
Works of Shakespeare and Beethoven, Newtonian physics formulas. The Bible is in the public domain, but there is a perpetual UK copyright on the King James version. Copyright is viable in new formulations of work or translations.
Enacted in 1998, the DMCA exempts internet service providers and other intermediaries from direct and indirect liability for copyright infringement by their users. [Viacom v. YouTube]

Online service providers must adhere to and qualify for certain prescribed safe harbor guidelines and promptly block access to alleged infringing material (or remove such material from their systems) when they receive notification of an infringement claim from a copyright holder or their agent. DMCA also offers a counter-notification provision that provides safe harbor from liability for users when they claim that the material in question is not infringing.
Hyperlinks & Copyright

• Linking generally does not raise copyright concerns unless linking to infringing materials (i.e., contributory copyright infringement).

• However, consider possible “terms of use” restrictions on deep links.

• Emerging consensus is that “in-line links” or “embeds” similarly are not infringing.
This is an in-line linked photo!

Take a look at this photo. The photo looks like it is on this blog. It really isn’t. The photo is stored at the website photobucket.com. This site merely contains an in-line link to the photo. That means that the photo does not reside on the same server as this blog. When your browser views this blog page, it reads the in-line link, which then directs your computer to that other server. Thus, the photo of Big Brown, the 2008 Kentucky Derby winner resides on the photobucket site.
3. Trademark Basics ® ™

A recognizable sign, design or expression which identifies products or services of a particular source from those of others. The trademark owner can be an individual, business, organization or any legal entity.

Trademarks can be owned or licensed. Trademark infringement can only occur if a trademark is registered with the Trademark Office.

Both copyright and trademark are considered forms of Property under the law.
• Infringement
  – Use of a mark in a manner likely to cause confusion, deception or mistake as to the source of goods or services
  – Can include confusion about endorsement or sponsorship

• Dilution / tarnishment
  – Use of famous mark in ways that undermine or disparage the mark
4. Trade Secrets and Confidential Information
“Ding dong the deal is dead! Turns out I won’t have to work all week…. My vacation is saved!”
• How a Facebook post violated a settlement agreement:

  "Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT."

Read more:
5. Who owns what: control of social media accounts
“On duty” Employee Speech

When tweeting, blogging, posting, …
• what employees do ON THE JOB is company’s business – and responsibility.
• What employees do OFF DUTY may still be company’s responsibility IF it is not clear whether the employee is speaking for the company or only personally.
6. Social media marketing
Key Marketing Risk Areas

– Use and protection of consumer data (internal privacy policies, and evolving US data privacy standards)

– Regulation of channels of marketing communications (i.e., Can-Spam Act)
The CAN-SPAM Act of 2003

Requires that “commercial” messages:

1. Include an “opt-out” mechanism
2. Identify the sender
3. Provide “clear and conspicuous” identification that the message is an ad or solicitation
7. Contests and sweepstakes on social media
Legal Sweepstakes

- Prize
- Winner determined by chance (i.e., random drawing)
- Eliminate consideration: Free to enter
- Where unsure, include “alternate free method of entry"
Legal Contest

- Prize
- Payment or consideration to enter
- Eliminate Chance: *Winner determined by skill*
  - Photo or essay contest
  - Properly structured trivia contest (not too hard or easy)
- Entries must be judged by consistent application of criteria
8. Insurance Coverage for Social Media Exposures

- Defamation, disparagement or harm to character, reputation or feelings including libel, slander, product disparagement

- Invasion, infringement or interference with rights of privacy, including false light, public disclosure of private facts, commercial appropriation of name or likeness

- Trademark infringement

- Copyright infringement
Questions?
What is K&R Insurance?

Dwight Kartchner – Response Consultant, Control Risks

Nephertiti Plunkett – Underwriter, Hiscox USA
Kidnapping: Worldwide Epidemic

- Over 55,000 reported kidnaps annually
- Over 85% of kidnaps not reported
- Incidents in every corner of the world including the United States.
- Annual value of ransoms over $500,000,000
- New types of crimes every year
K&R Coverage – Who Can It Cover?

- Corporations – small, medium, and large
- Government contractors
- Non-Governmental Organizations (NGOs), Relief Organizations, Non-Profits
- Religious Organizations, Houses of Worship
- Hospitals
- Universities and related higher education
- High Net Worth Families
## K&R Coverage - What Does It Cover?

<table>
<thead>
<tr>
<th>Standard Coverage:</th>
<th>Overlooked Coverage:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Kidnap</td>
<td>• Extortion</td>
</tr>
<tr>
<td>• Ransom</td>
<td>• Computer Virus</td>
</tr>
<tr>
<td>• Hijack</td>
<td>• Loss of Earnings (BI)</td>
</tr>
<tr>
<td>• Wrongful Detention</td>
<td>• Salaries</td>
</tr>
<tr>
<td>• Consultant Expenses</td>
<td>• Rest &amp; Rehabilitation</td>
</tr>
<tr>
<td>• Legal Liability</td>
<td>• Informants</td>
</tr>
<tr>
<td></td>
<td>• Recording Equipment &amp; Translators</td>
</tr>
<tr>
<td></td>
<td>• Interest Costs</td>
</tr>
<tr>
<td></td>
<td>• Extra Security</td>
</tr>
<tr>
<td></td>
<td>• Travel Costs</td>
</tr>
<tr>
<td></td>
<td>• Job Retraining</td>
</tr>
</tbody>
</table>
Types of incidents

- Product extortion
- Product contamination
- Threat extortion/blackmail/stalking
- Kidnap
- Political hostage-taking and wrongful detention
- International problem solving
Definitions

Kidnap-for-ransom
• The abduction of a person or persons with the intent of their detention in an *unknown* location until a demand is met.

Hostage Extortion
• The abduction of a person or persons with the intent of their detention in a *known* location until a demand is met.

Threat Extortion
• A written or verbal contact is made, by any means of communication, threatening to harm or cause damage to a company, person or persons unless a demand is met.

Product Extortion
• An extortion incident in which a threat is made to do commercial damage to a company through the contamination of its products against a demand for cash or other concessions. This can also involve an initial contamination prior to receipt of a threat.
Value of a K&R policy is twofold:

1) Security protection—provides expert advice from a K&R consultant who is specifically trained with one objective in mind.

2) Financial protection—the insurance policy reimburses the client for costs they incur in an incident – costs which most clients cannot afford to absorb.

Crucial to vet the capabilities and experience of response firm attached to the K&R policy.
Control Risks has worked on **2,535** cases of kidnap, extortion and other crises in **127** countries.

**Breakdown by type:**

<table>
<thead>
<tr>
<th>Type</th>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kidnap</td>
<td>1,201</td>
</tr>
<tr>
<td>Product contamination/extortion</td>
<td>326</td>
</tr>
<tr>
<td>Threat extortion</td>
<td>777</td>
</tr>
<tr>
<td>Short-term hostage extortion</td>
<td>26</td>
</tr>
<tr>
<td>Bomb extortion</td>
<td>33</td>
</tr>
<tr>
<td>Other</td>
<td>172</td>
</tr>
</tbody>
</table>

Total case days for all incidents **46,436**

(This represents more than 127 years of accumulated experience)
Location of Response cases in 2013 and through 2014

Mexico 80
Nigeria 26
Colombia 15
China/Hong Kong 10
Venezuela 8
Syria, India 7
Egypt, Mozambique, Pakistan, Germany 4
South Africa, UK, USA, Canada, Honduras, 3
Iraq
Switzerland, Angola, Brazil, CAE, Indonesia, 2
Greece, Sudan, Kenya
Thailand, Togo, Algeria, Bangladesh, Cameroon, 1
Peru, Madagascar, Libya, Ukraine, Spain,
Slovenia, Russia, Netherlands, France, Yemen,
Australia, Belgium, Cyprus, El Salvador, Ecuador

Total of 206 Cases
Kidnaps worldwide, 2013 – durations of cases

- Less than a week: 74%
- Eight days to a month: 18%
- One to three months: 6%
- More than three months: 2%
Kidnaps worldwide, 2013 – victim outcomes

- Escaped: 75%
- Released or presumed released: 5%
- Rescued: 18%
- Killed or died: 2%
Matt Boynton **Director**

John Wade  
**Deputy Director,**  
Nick Hammond  
**Operations Manager**

Lara Symons  
**Business Manager**

19 Full-time Consultants

2 Team Administrators

4 Research Analysts
Four multi-lingual analysts.

Kidnap-for-ransom database of 38,993 kidnap cases and details of 79,787 victims.

Extortion database of 437 short-term hostage cases, 280 hijacks, 1096 threats, 129 bomb extortions and 76 illegal detentions.

Product database of 803 product extortions and 3,423 product contaminations
• All consultants only involved in Response work

• Response never sub-contracts

• Consultants of a ‘relevant background’

• Response Services are provided from a central pool of consultants who are located in Utah, Texas, Florida, Colombia, South Africa, and the Greater London area

• Trained hand-holders in international offices
Response Objectives

• The safe, timely and secure release of the victim

• The correct handling of the extortion in the interests of the client

• Safeguarding the continued operations of the client

• To act within the law
Sequence of Events during an Incident

- Receipt of notification of the event
- Fact-finding
- Immediate telephone advice/deployment of trained hand-holder
- Receipt of electronic “Backpack” from Research Analysts
- Deployment of consultant to area of problem
- Deployment, if required, of a Manager or Senior Consultant to Corporate Head Office
The Local Consultant

- Establish communications
- Establish a management organisation
- Identification of, and liason with, government and local law enforcement agencies
- Strategy and tactical options
- Anticipation
- Select/train communicator or intermediary
- Media handling
- Family liason
• Recommend a management organisation and decision-making authority

• Analysis and briefing on the problem

• Identify strategic decisions

• Liaison with external third parties

• Family liaison

• Media management

• Legal liabilities and responsibilities
Response Does Not

- Participate in face-to-face meetings with kidnappers
- Act as communicator on behalf of client
- Carry or pay ransom
- Break the law
- Compete with law enforcement
- Publish client names
- Mount rescue missions
Questions?

Contact Details:
Dwight.Kartchner@controlrisks.com
• Presented by:
• Viggo Boserup, Esq. CEDS
• Certified Electronic Discovery Specialist
Practical Guide to E-Discovery

Viggo Boserup, Esq. CEDS - JAMS
Introduction

• Difference between Paper and Electronic Data
  – Paper’s physically visible
    • We know how much we have
    • We know where it is
    • We know who has it
    • We know how to preserve it
    • We know how to retrieve it
    • We know how to review it
    • We know how to produce it
    • When we ran out of space, we got rid of it
      (Darwinian document retention)
• Electronic data not visible

  – We know it is there, but we can’t see it to find, review, or produce without technology

  – It is located not in filing cabinets but in employee files, department/group files, enterprise databases, and backup media
• Now it can be anywhere and held by anyone

  – In the last 25 years or so, all documents stored on electronic media

  – The following have added further complexity to e-discovery

    • Smartphones
    • Tablets
    • BYOD
    • Cloud storage
• Here are the major rules under FRCP as well as some of the California counterparts:
  – FRCP 26 (a) (1) - Initial disclosures
  – FRCP 26 (f) - Meet and confer
    • Cal Rules of Court 3.724 requires CMC 120 days after service of complaint with meeting of counsel 30 days before that re discovery and 8 items re ESI
  – FRCP 26 (b) (2) (B) - Not reasonably accessible
    • CCP 2031.210 (d)
  – FRCP 26 (b) (2) (C) - Cost shifting and proportionality
    • CCP 2031.280 (e) “translate to usable”

  – Continued on next slide
Here are the major rules under FRCP as well as some of the California counterparts:

- FRCP 30 (b) (6) - Discovery about discovery
- FRCP 34 - Form of production-usual or reasonably usable
  - CCP 2031.030 (a)(2) requesting party can specify format
- FRCP 37 - Safe Harbor—major change in the works-Rules Committee at Portland Meeting April, 2014
  - CCP 2031.060 (i)(1) CCP 2031.300 (d)(1)
- FRCP 45 - Non-party subpoenas
- Federal Rules of Evidence Rule 502 regarding privilege and work product and inadvertent disclosures
  - CCP 2031.285
• FRCP 37 (e) Safe Harbor under review by Rules Committee
  – Look for new language incorporating “Curative Measures” in lieu of “Sanctions”

• Very deliberative process
  – Met in Portland 4/10 and 4/11/14 then goes to standing committee in May, then Judicial Conference, Supreme Court, then Congress which has 6 months to do anything or nothing, so earliest is December 2015.
INFORMATION MANAGEMENT AND LITIGATION READINESS

BE READY FOR IT BEFORE IT HAPPENS

• Records management policy outlining retention and destruction practices to support business needs

• Should be in anticipation of relevant, reasonably anticipated, or actual litigation

• Must have companion policy for legal holds.
Cal. State Bar Standing Comm. on Prof’l Responsibility & Conduct, Proposed Formal Op. 11-0004. Lists 9 activities attys handling ediscovery should be able to do:

1. Assessing ediscovery needs
2. Implementing appropriate preservation procedures
3. Analyzing and understanding client’s ESI systems and storage
4. Identifying custodians of relevant ESI
5. Performing appropriate searches
6. Collecting responsive ESI in a manner that preserves its integrity
7. Advising clients on available options for collection and preservation of ESI
8. Engaging in a “competent and meaningful” meet-and-confer to address e-discovery plan
9. Producing responsive ESI in an appropriate manner
FIVE STAGES OF E-DISCOVERY

1. Preservation
   - Legal hold steps
     - Identify sources of ESI
     - Written notice to custodians
     - Distribution - only to select group most likely to have the data being requested
     - Response - confirm receipt, understanding, and willingness to comply through a method that can be tracked
     - Interview key personnel to confirm understanding
     - Periodic follow through (monthly/quarterly)
     - Release notice-avoid overwhelming custodians and losing seriousness of project
     - Tracking-all holds across all matters for a corp entity
• 1. Preservation: Essentials of Documentation (cont’d)
  – Legal Hold Documentation
    • What steps were taken to identify the location of relevant information?
    • Legal hold communication itself
    • Evidence of its distribution
    • List of recipients
    • Confirmations
    • Follow-up communications
    • Update these documents
    • Track the timing of later decisions and communications
  – For an almost amusing example of a woefully weak legal hold procedure, see *Procaps S.A. v. Pantheon Inc.* 2-28-14
2. Collection

- Forensically-sound collection assures no alteration of the content or quality of data as it existed prior to collection

- Validating Collection

- “Not Reasonably Accessible” - FRCP 26 (b) (2) (B)
3. Processing

- Establish well-defined workflow with software that provides logs of what was accomplished and what failed during processing

- Data De-Duplication

- Culling

- Date Ranges

- Search terms

- De-Duplication Again-eliminate identical hash value documents
• 4. Review for relevance and privilege
  – Relevance - create data sets through search terms if not already done in collection method using Boolean logic, proximity connectors, stemming, wildcards, stop words etc.
  – Privilege-review team must be trained in law of privilege
  – Review team should have samples of responsive documents
  – Team should have protocol for reviewing documents showing types of analytical decisions to be made and marked properly
  – Quality control here is important and should be done concurrently with review to identify and correct immediately any anomalies
  – Training the review team
5. Production

- Native format - no conversion from its original form.
- Imaged Format - static
- Hosted Environment - more common now where the parties have joint access to the production (eg Relativity)
- Due to wide variety of formats, parties often agree to more than a single format
- Metadata
- Federal Rules of Evidence, Rule 502: Clawback Agreements provide for the return of documents inadvertently produced provided the request is made reasonably soon after its discovery. Often set forth in a protective order.
TECHNOLOGY ASSISTED REVIEW (TAR) AKA PREDICTIVE CODING

• Automated document review
  – Senior attorneys intimately familiar with case train software to make coding decisions
    • Proprietary algorithm to create model that generates prediction score for every document based on how counsel codes a small number of documents or “seed” documents. Counsel then makes judgment re accuracy of prediction, fine tuning results by adding more documents to the seed set. Then counsel reviews and codes seed sets through iterative process until desired accuracy is reached.
  – Then counsel decides which to produce, eg those documents with threshold score of 70% or better shall be produced
TECHNOLOGY ASSISTED REVIEW (TAR) AKA PREDICTIVE CODING

• Representative cases:
  
  – *DaSilva Moore* - January 2012-approved use of TAR
  
  – *EORHB v. HOA Holdings* - October 2012-ordered TAR
• Visual analytics - charts and clusters to represent computer analysis
• Automated Legal Hold software - locking down data preventing modification, moving, deletion, copying etc.
• Social Media Discovery tools - bots crawling social media sites for responsive material
• Information Governance - application of advanced analytics (Predictive analysis) to manage, clean, and dispose of enterprise data
Senior attorneys typically supervise and train less-seasoned colleagues.

Senior attorneys, however, are often least equipped to understand the complexities of technology and may have little experience in social media.

This has not escaped the notice of the bench.
ADVERSARIES OR NOT, COLLABORATION IS CRITICAL

• Due to the cost of being second-guessed, one side cannot afford to go it alone.
• Early collaboration is critical before parties’ positions harden and/or disputes have arisen
ADVERSARIES OR NOT, COLLABORATION IS CRITICAL

• From the moment of the meet-and-confer, it is critical that parties get on the same page
  – Prepare and share agenda for the meet-and-confer
  – Bring to the meet-and-confer a draft discovery plan including all issues to be discussed:
    • Initial disclosures—timing, form, or requirements
    • Subjects on which discovery is needed
    • Privilege and work product issues including clawbacks and protective orders
    • Agreement to vary FRCP limitations, e.g. fewer or more depositions or interrogatories
    • Agree on methodologies for discovery
QUESTIONS?