

THE LAW OFFICES OF



GIBBEL KRAYBILL & HESS ^{LLP}

ATTORNEYS & COUNSELORS AT LAW

“Virtually Terrified?”

Safely Operating Your Organization Online

Presented by GKH Corporate Practice Group

Wednesday, October 31, 2012
(Rescheduled for November 12, 2012)



WWW.GKH.COM

The Eerie Shadows: Doing Business in Other States

- Nexus test – what the state can do to you
 - File with department of state as foreign company
 - File and pay state income taxes
 - Collect sales taxes
- Minimum contacts test – what other people can do to you
 - Subject to litigation in foreign jurisdictions
 - *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*,
952 F. Supp. 1119 (W.D. Pa. 1997)

http://apps.americanbar.org/litigation/litigationnews/top_stories/docs/zippo.pdf



The Spider Webs

- Qualifying to do business
- Licensing for professional services
- State intellectual property right violation challenges vs. federal patent and trademark (discussed later by Peter)



The Booby Traps: Selling Online

- State consumer protection laws
- Vicarious liability
 - What your buyer does with your product
 - Tampering with your product and reselling
 - Faulty installation



Into the Cauldron: Sales or Use Tax For Online Sales

- A tax is due <http://smallbusiness.findlaw.com/business-taxes/do-you-have-to-pay-sales-tax-on-internet-purchases.html>
- Amazon as trendsetter www.npr.org/2012/09/14/161083090
- Legislative initiatives
 - Federal http://www.huffingtonpost.com/2012/08/10/online-shopping-tax-cost_n_1764287.html
 - PA <http://www.nolo.com/legal-encyclopedia/pennsylvania-internet-sales-tax.html>
 - Exemption for small retailers



Advertising Online

- Risk of suit in foreign jurisdictions
 - Jurisdictional challenge
 - Venue challenge



Collection

- Get paid before shipping
- Terms of Sale
 - Pennsylvania choice of law
 - Lancaster County choice of forum
- Foreign judgments
- Debt collection
 - Does not apply to commercial transactions
 - Consumer transactions
 - Federal law
 - State laws



Privacy Policies

3 Key Areas:

1. Setting your own “rules” for how you collect, store and use personally identifiable information (“PII”)
2. Complying with your own “rules”
3. Staying up to date on changes in state law

Privacy Policies

- ❖ Personally identifiable information has been defined by the US Government's **Office of Management and Budget** (OMB) as:

*"information about a person that contains some **unique identifier**, including but not limited to name or Social Security Number, from which the identity of the person can be determined ... [such as], education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, **social security number, date and place of birth, mother's maiden name**, biometric records, etc., including any other personal information which is linked or linkable to an individual."*

Privacy Policies

1. *Setting your own “rules” for how you collect, store and use PII*

- Work closely with an expert web-designer
- Ensure compliance with California Online Privacy Protection Act of 2003

Privacy Policies

2. *Complying with your own “rules” and updating as needed.*

- Regularly audit your site to ensure that your Privacy Policy accurately reflects what you collect and how you handle PII



Privacy Policies

3. *Staying up to date on changes in state law*

- State laws vary; new standards arise regularly
- No consistent Federal Standard for businesses storing and using PII
- Must comply with the most stringent requirements of each state where your website would be accessible
- *In PA, a failure to comply with your own Privacy Policy is a violation of consumer protection laws as deceptive business practices*

Privacy Policies Should Explain:

1. What types of personally identifiable information (“PII”) will be collected when the online user registers on your site
 - *name*
 - *social security number*
 - *date and place of birth*
 - *mother’s maiden name*



Privacy Policies Should Explain:

2. How you use collected PII

- “to better respond to the user’s needs”
- “to improve our website based on user feedback”
- “to process transactions”
- “to send periodic emails”

3. How you implement security to protect the user’s PII

- “We use 128-bit SSL encryption technology and allow access to your information only to those authorized individuals within our organization”

Privacy Policies Should Explain:

4. How you use cookies at your website to track or record activities of users at your website
 - “to compile aggregate data concerning site traffic to improve our site”
5. If you disclose any PII to outside parties, specifically state how this occurs
6. Mention any third-party links that you make on your website

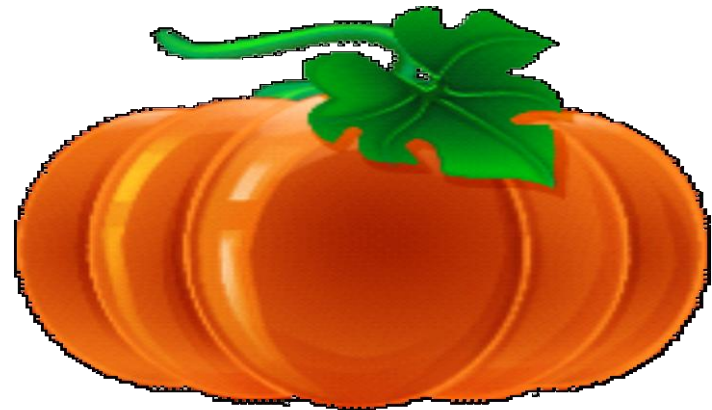
Privacy Policies Should Explain:

7. If your site is accessible to **Californians**, you need to state somewhere in your Privacy Policy how users may change their PII
 - *“As part of the California Online Privacy Protection Act, all users of our site may make any changes to their information at any time by logging into their account and going to the ‘Edit Profile’ page”*
 - This applies if your homepage is accessible by CA residents for the purchase of services for personal, family or household purposes

Privacy Policies

Customer Acceptance of Privacy Policies

1. *Use of the website is agreement*
2. *“Click the Box”*



Sample Privacy Policies

How do I get started?

- Can begin drafting your privacy policy from free templates available on-line + working with your web designer
- Then provide to GKH for final review before adding online
 - <http://www.freeprivacypolicy.com/>

Terms of Use

- Purpose: “Website Terms of Use” govern appropriate use of your website by users.
- Examples: The Website Terms of Use Policy would:
 - Forbid posting false or infringing information on your comments page.
 - Forbids use of your licensed materials including logo (your information can change without notice)
 - Provide notification that you can change the terms of use without prior notice.
 - Direct users to your Privacy Policy

Terms of Use

Free Terms of Use Template:

<http://www.inixmedia.com/2010/02/free-terms-of-use-template-for-website/>



Data Breaches

What is a data breach?

- A data breach is an event where sensitive, protected or confidential information has potentially been viewed, stolen or used by someone not authorized to do so.
- Data breaches may involve personal health information (PHI), personally identifiable information ([PII](#)), trade secrets or intellectual property.

Data Breaches

A number of industry guidelines and state compliance regulations require strict control over sensitive or personal information to avoid data breaches

- In the corporate environment, the Payment Card Industry Data Security Standard ([PCI DSS](#)) governs who may handle and use sensitive PII such as credit card numbers, PINs and bank account numbers in combination with names and addresses
- In the healthcare industry, the Health Insurance Portability and Accountability Act ([HIPAA](#)) regulates who may see and use PHI such as name, date of birth, Social Security number and health history information

Data Breaches

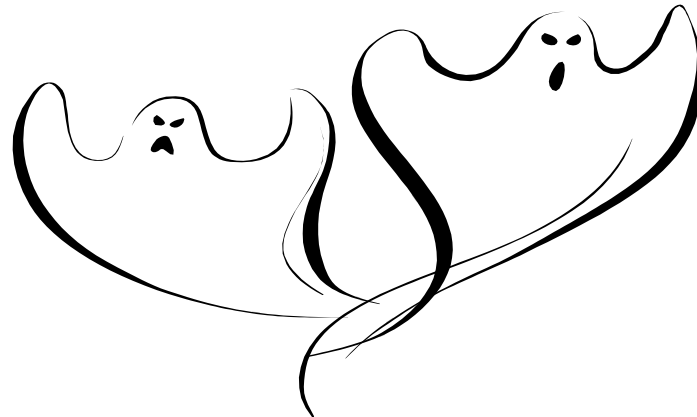
You've discovered a breach! Now what?

- Determine the extent of the breach (type of information stolen, number of customers affected)
- Has the breach resulted in harm or likely harm to your customers?
- If a data breach results in ***identity theft*** and/or a ***violation of state or industry compliance requirements***, the organization could face fines or other civil or criminal prosecution.

Data Breaches – Financial Exposure

Financial Exposure in the Event of a Breach:

- Studies have revealed that the average cost of a data breach in 2010 was \$7.2 million.
- *Negligence* was found to be the leading cause of data breaches (41% of the data breach incidents).



Data Breaches – Financial Exposure

The following are expenses a company may incur when a data breach results in the loss or theft of PII:

- Forensic Examination – Determines the severity and scope of the breach
- Notification of Third Parties - Most state laws require companies to notify those individuals if PII is lost, stolen or compromised. Varies by state.
- Call Centers – If heavy call volume expected.
- Credit or Identity Monitoring - Not required by most state laws, but good for customer relations.

Data Breaches – Financial Exposure

- Public Relations – Engagement of PR firm in severe cases
- Legal Defense. Defend against claims of:
 1. Negligence
 2. Breach of Warranty
 3. False Advertising
 4. Unfair or deceptive trade practices
 5. Violations of various applicable state/federal laws
- Fines and Penalties from Regulatory Proceedings. Range from \$100 - \$1,000,000+

Data Breaches

Insurance Coverage Available

- Forensic Examination; Notification to 3rd parties; Call Centers (maybe); and direct costs of obtaining a PR firm
Coverage under many Network Risk policies
- Credit/Identity Monitoring – Coverage provided by a limited number of policies
- Legal Defense Costs – Coverage may be provided under certain Cyber Risk policies

Data Breaches

Recent Data Breach Case

- 2008 TJ Maxx Data Breach – Over 45 million credit and debit card numbers stolen

Non-compliance with Payment Card Industry Standards.

- Inadequate wireless network security
- Improper storage of customer data
- Failure to encrypt customer account data

Your Brand and Its “Goodwill”

Is your brand valuable online?

Is your brand federally registered?



Your Brand and Its “Goodwill”

Goodwill is the inherent value of trademark rights. A trademark is the exclusive right to use a brand in a certain business niche in a certain geographic area. You can exclude others who seek to use your brand in that niche. That’s the primary value of a **trademark**.

When to protect your “Goodwill”

Apply for a federal trademark before:

1) the value of your brand is more than you can afford to lose

2) investing marketing dollars to enhance your brand's recognition

Major Benefits of a Federal Trademark:

1. Exclusivity for the entire United States of America
2. Statutory damages of \$150,000 plus your attorney's fees for "willful infringement"
3. Any non-permitted use of your brand by someone else is infringement

Other Benefits of a Federal Trademark:

1. Evidences rights for the purposes of securitizing debt or sale of those rights
2. Superior status for website registration



ICANN Arbitration

- Domain name disputes via arbitration by the Internet Corporation Assigned Names and Numbers <http://www.icann.org/>
- WHOIS search results <http://www.internic.net/whois.html>
- Favors trademark registrant of active brand
- Resolution typically less than \$5,000
- Demolishes Cybersquatter Extortion Schemes

Takedown Notices Under DMCA

- Protects copyrights but gives safe-harbor to certain online service providers (OSPs)
See <http://www.chillingeffects.org/dmca512/>
- Does not generally apply to trademarks, and gives no safe harbor to OSPs for infringements
- Typically no court involvement
- Private party settlement/compliance
- To submit effective takedown notice: need to know Facebook policy and industry-specific website marketing policies of OSP

USPTO Federal Trademark Registration

- From “TM” to “®”
- First conduct mark clearance by research of availability (attorney involved)
- Make a single application for each word phrase, graphic, or combination of those (attorney involved)
- Additional fee for each class of goods/services
See www.uspto.gov/trademarks

TM Application Support

- In Use vs. Intent to Use (in commerce)
- Specimens
- Choosing Class and Drafting Description



TM Application Prosecution

- Examiner review after 3 months
- Disclaimers
- Publication for Opposition
- Opposition period of 30 days
- Registration within 3 months

TM Maintenance

- Affidavit of Use and Noncontestability (6th year)
- Renewal Filings (every 10 years)
- Consistency in marking things with your trademark
- Consistency in using your registered mark
- Care in altering mark and filing for additional marks
- Making Licensing Agreements

Other Ways to Protect Your Brand

- Domain name registrations(!) - .com .net .org .biz
- Use your brand in commerce and enhance your Common Law Trademark rights
- Corporation entity registration at PA Dept of State
<https://www.corporations.state.pa.us/corp/soskb/csearch.asp>
- Fictitious Name (d/b/a) filing at PA Dept of State
- PA Trademark (not advised)



Suggested TM Strategy

- Register Company and any fictitious names with PA Dept of State
- Register with USPTO your primary brand and any additional marks that gain goodwill
- Consistently use your mark(s)
- Use grassroots information and internet searches to find and prosecute infringers
- Make written licensing agreements for any permitted uses by others . . . and send C&D letters for non-permitted uses

Cease-and-Desist Letter Example

Re: Infringements of STAR TREK Copyrights and Trademarks

...Paramount owns all of the rights to ... the "STAR TREK Properties". These rights are protected by numerous copyrights and trademarks.... We have recently learned that you have posted various elements of the STAR TREK Properties on your site at [www.\[website\].com](http://www.[website].com). For example, we refer to your posting entitled "Synopsis of "Star Trek: First Contact" (the "Synopsis"), as well as various photographs of STAR TREK elements. Your posting of these items is an infringement of Paramount's rights in the STAR TREK Properties. Based upon the foregoing, we hereby demand that ...: (i) you [remove] all infringing materials from your site, ...; and (ii) you will refrain from posting any similar infringing material on the Internet or any other on-line service in the future. ...

See e.g. <http://www.chillingeffects.org/fanfic/notice.cgi?NoticeID=7>

Cease-and-Desist Letter Recipients

- Consider: Who has prior use, who is registered, is registration class & description similar?
- Negotiation
 - reasonable license fee?
 - infringement damages?
- Litigation

See e.g. <http://www.chillingeffects.org/fanfic/notice.cgi?NoticeID=7>

Cease-and-Desist Letter Recipients

- No written permission to use the work/mark?

= likely infringement
- Only use others' images or brands when you have written permission
- Only post what you want the world to see



Employee Internet Activity

- What an employee does online can effect employment
 - Blogging, Facebook, Twitter, etc.
 - What you don't know can hurt you, *i.e.* disparaging comments, leaking of confidential information, criminal activity
 - What you do know can hurt you, *i.e.* legally protected activity, disability information

Employee Internet Activity

- Have a policy regarding work and non-work electronic communications
 - No expectation of privacy
 - Employer's right to monitor and inspect
 - Out of work electronic communications

NLRB and Electronic Communication

- Employees can discuss the conditions of their employment with co-workers
 - This includes critical comments about the terms and conditions of employment
 - Regardless of whether it is at the water cooler or on Facebook



Social Media

- Can an employer require an employee to provide passwords to social media?
 - In PA, generally yes
 - Information obtained through employees' social media may create employer obligations
 - Disciplinary actions must be uniformly and consistently applied

Protecting Confidential Information

- Define what is your company's confidential information/trade secrets
- Establish policies and protocol
 - Limit employees' access
 - Limit what is posted online
 - Making it available to the public voids the information's confidentiality

THE LAW OFFICES OF



GIBBEL KRAYBILL & HESS ^{LLP}

ATTORNEYS & COUNSELORS AT LAW

QUESTIONS & ANSWERS