Cyberstalking, Spam & Defamation

CJ341 – Cyberlaw & Cybercrime
Lecture #8

M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

Topics

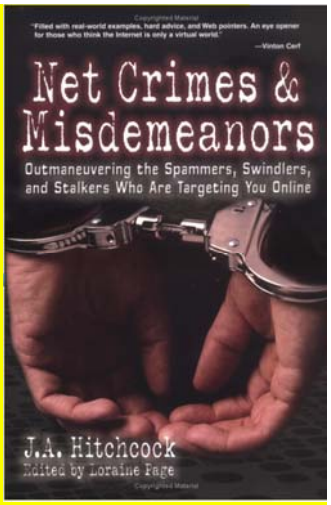
- Cyberstalking
  - Jane Hitchcock
  - Choosing Victims
  - Targeting Victims
  - Cyberstalkers
  - Law Enforcement Response
  - Applicable Law
- Spam and the CAN-SPAM Act
- Defamation
  - Cubby vs CompuServe (1991)
  - Stratton Oakmont vs Prodigy (1995)
  - Blumenthal v. Drudge & AOL (1998)
- Libel and Freedom of Speech
- Defenses

Cyberstalking

- "Cyberstalking"
  - Relatively new term – since early 90s
  - Refers to *harassment* or *physical threatening* of a victim through *electronic* or *digital* means (Clifford)
  - Term sometimes used interchangeably with online harassment or online abuse
  - No uniform definition
- Emerging crime
  - Originally considered harmless
  - CA first state to criminalize "stalking" behavior – after high profile events

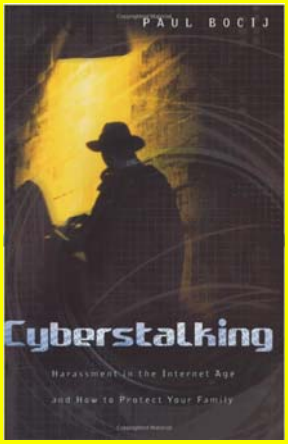
Jane Hitchcock

- Literary agent & author
- Victimized by mail-bombing (flooding) attack of her e-mail account
- Targeted because of commentary she posted on a message board
- After changing her e-mail address, harassment continued
- Personal information posted on site
  - Listed as a sexual deviant
  - Looking to act out rape fantasies
- Feared for her life



Cyberstalking

- Continuous process
- Not just one activity
- Activities may cross into physical world
- ***"Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighborhood or in your home."***
  - Vice President Al Gore
  - http://tinyurl.com/3sue7kl



Choosing Victims

- Accessibility
  - Cyberstalkers may not have to look far to locate personal / electronic contact information
  - Business cards
  - Personal Web sites
  - Google search
  - Myspace, Facebook
- Easy to communicate electronically

Targeting Victims

- Cyberstalkers Target Victims
  - E-mail
  - Online forums
  - Bulletin boards
  - Chat rooms
  - Spyware
  - Spam
- Examples
  - Chat harassment /"flaming"
  - Unsolicited/unwanted e-mail
  - Tracing Internet activity
  - Sending viruses,
  - Sending obscene images

Tracking Down Cyberstalkers

- Criminals take advantage of anonymity
  - E-mail forgery, spoofing, anonymous remailers
  - Fake registration information
- But difficult to remain completely anonymous
  - Methods may delay identification
  - Cooperation of ISPs can help trace traffic using IP headers
  - Wiretaps can collect evidence if suspect identified
  - Forensic evidence lies on computer systems

Law Enforcement Response

- Enactment of state statutes
  - Many states have added cyberstalking-specific legislation
  - Or amended pre-existing laws to address stalking via technology
- Finite Resources of LEOs
  - $$
  - Time
- Coordination / cooperation needed
  - Tracking across state lines
    - ✓Jurisdictional issues
    - ✓Search warrants, court orders

Applicable Law

- No federal statute specifically directed at cyberstalkers
  - Statutes do exist to prosecute sending of obscene, abusive or harassing communications [46 USC § 223(a) – see next slide]
- Patchwork application of state and/or federal law
  - State law varies from jurisdiction to jurisdiction
  - Some states have cyberstalking-specific statutes

Obscene, Abusive or Harassing Communications 46 USC § 223(a)

- See Clifford pp 30-31
- An offense to use a telecommunications device in interstate or foreign communications to:
  1. make, create, solicit, and initiate transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene, or child pornography, with intent to annoy, abuse, threaten, or harass
  2. make, create, solicit, and initiate transmission of any comment, request, suggestion, proposal, image or other communication which is obscene or child pornography knowing recipient is under age 18, regardless of whether the maker initiated the communication

Obscene, Abusive or Harassing Communications (cont'd)

3. make telephone call or utilize telecommunications device, whether or not conversation or communication ensues, without disclosing identity and with intent to annoy, abuse, threaten, or harass;
4. make or cause the telephone of another repeatedly or continuously to ring, with intent to harass;
5. make repeated calls or initiate communication with a telecommunication device, solely to harass;
6. knowingly permit any telecommunications facility under his or her control to be used to commit any of the above activities

- Penalties include fines, imprisonment up to 2 years or both

Corporate Cyberstalking

- Corporate Cyberstalking: incidents that involve organizations – companies, government
- 46 USC § 223(b)
  - Federal crime to make an obscene or indecent communication for commercial purposes or to allow a telephone facility to be used for this purpose
  - Federal crime to use telephone to make an indecent communication for commercial purposes which is available to anyone under the age of 18 or to allow a telephone facility to be used for this purpose

Threats: 18 USC § 875

- Federal crime to transmit in interstate or foreign commerce a communication:
  - Demanding a ransom for the release of a person;
  - Intending to extort money;
  - Threatening to injure a person;
  - Threatening to damage to property
- Requires a *threat* (so may not always apply to cyberstalking)

Threats (cont'd)

- Examples – Clifford pp 32-34
- *U.S. v. Kammersell*: 10th Circuit Court held that defendant who allegedly sent threatening communication from his computer to another could be prosecuted under the statute even though the defendant and the recipient were located in the same state because the jurisdictional element (Interstate commerce) was satisfied – finding message was transmitted over interstate telephone lines and traveled through a server located outside the state
- *U.S. v. Alkhabaz:* Defendant, Uof Mich. Student, used e-mail to communicated with a friend, much about descriptions of fantasized sexual violence against a female classmate; he was prosecuted for sending "threats" via interstate commerce. District court dismissed finding the e-mail message was not a "true threat" and was protected by the First Amendment; 6th Circuit Court affirmed the decision as it did not rise to the level of a threat

Stalking: 18 USC § 2261A

- Federal crime to
  - Travel in interstate or foreign commerce with intent to kill, injure, harass, or intimidate another, placing that person in reasonable fear of death or serious bodily injury to themselves or to a family member; or
  - Use mail or any facility of interstate or foreign commerce to engage in a course of conduct that places a person in reasonable fear of death or serious bodily injury to themselves or to a family member
- Key: Person must be placed in *reasonable fear of death or bodily injury*

Spam (not SPAM™)

- Can CAN-SPAM Can Spam?
- Spam Statistics
- Responding to Spam

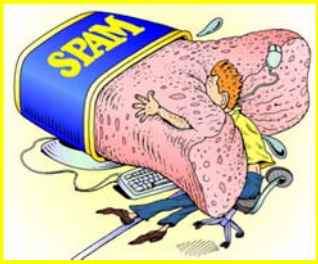


Image from URL below. Permission for re-use currently being sought but original author unknown.
http://marketingreview.web-log.nl/photos/uncategorized/spam_fun.jpg

Can CAN-SPAM Can Spam?

- CAN-SPAM* Act: "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" - Took effect Jan. 1, 2004
- Does not outlaw spam
- Requires spammers:
  - To identify themselves clearly,
  - Use no fraudulent headers
  - *Must honor consumer requests to cease sending mail*

**SPAM* in all-uppercase is a trademark of Hormel Foods. *Spam* or *spam* are acceptable jargon terms for unsolicited commercial e-mail.*

CAN-SPAM (cont'd)

- CAN-SPAM Act added provisions to US Code, including to Title 18, making it a federal crime to
  - Access a protected computer without authorization and intent to transmit multiple commercial electronic messages
  - Use a protected computer to replay or retransmit multiple commercial electronic messages with intent to deceive or mislead recipients
  - Falsify header information in multiple commercial messages
  - Register using false identity for 5 or more electronic mail accounts or 2 or more domains and intentionally initiate transmissions from such accounts or domains
  - Falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more IP addresses and initiate messages from such addresses

CAN-SPAM (cont'd)

- *Multiple* defined as >100 messages during 24-hr period
- Punishment: fines and/or imprisonment
- Also possibility of criminal forfeiture:
  - Any property traceable to the proceeds obtained from the offense *and/or*
  - Any equipment, software, or technology used to commit the offense

Spam Statistics

- Spamcop
  - Day, week, month, year statistics
  - http://www.spamcop.net/spamstats.shtml
- Spamhaus
  - Worst ISP offenders
  - http://www.spamhaus.org/statistics/networks.lasso
- Ciphertrust
  - Phishing botnets & corporate targets
  - http://www.ciphertrust.com/resources/statistics/
- CAUCE: Coalition Against Unsolicited Commercial Email
  - Politics, reports, history
  - http://www.cauce.org/

Responding to Spam

- *Don't* respond directly to spam
  - Giving away fact that address is valid
  - Will be added to lists sold to victims
- *Don't* send abusive responses to REPLY-TO address:
  - Could be false
  - Intended to spark wave of abuse at innocent victim
- *Do* use antispam tools
  - E.g., Cloudmark < http://www.cloudmark.com >
  - Report to abuse@<isp> only if message is very new to you (minutes)

Defamation

- Issues
- Cubby v CompuServe
- Stratton Oakmont v Prodigy
- Blumenthal v Drudge & AOL
- Libel & Freedom of Speech
- Limitations on Lawsuits
- Defamation of a Business
- Suarez Corp v Brock Meeks
- Defenses Against Defamation Actions
- Rights of the Plaintiff

Defamation

- Defamation
  - Invasion of reputation and good name
  - *Making a statement to the public about another person that harms that person's reputation* (Burgunder p. 612)
- Basis for complaint
  - False statement
    - ✓Spoken = slander
    - ✓Written = libel
  - About another person
  - In the presence of others (public)
  - Harm to reputation
    - ✓Exposes victim to hatred, contempt, ridicule
    - ✓Tendency to injure person in work

Defamation - Issues

- Internet makes it easy to disseminate defamatory statements
  - Written
  - Oral (e.g., online audio clips)
- No or little skill required to post / disseminate
- Difficulty ascertaining person who made statement (anonymity, aliases)
- Liability
  - Person making statement may have no money for meaningful monetary recovery
  - Who should be held responsible for harmful comments? ISPs?
    - ?Question: Who is responsible for blog content? ISP?

Cubby v CompuServe (1991)

- One of 1st important cases to address responsibility of ISPs for transmitting defamatory comment
- CompuServe was one of largest ISPs at time
- Thousands of discussion *forums*
- Forums usually managed by *owners*
  - Independent individuals or corporations
  - E.g., Security forums were run by NCSA
- Journalism forum participant posted allegedly libelous text
  - Cubby Inc. filed libel suit against CompuServe
  - Court held CompuServe could not be held liable for such defamatory postings
  - Analogous to standards for library, bookstore, news-stand

http://epic.org/free_speech/cubby_v_compuserve.html

Stratton Oakmont v Prodigy (1995)

- Facts:
  - Allegedly libelous attack on company and president posted on Prodigy
  - Prodigy advertised its responsibility for running a *family-friendly* ISP
  - It promulgated "content guidelines" & used removal software
- Court ruled in favor of plaintiff's contention that Prodigy was more like *publisher* than *distributor*
- Thus *attempts* to censor/control content led to legal *responsibility* for content
- But in practice, moderators *cannot* control publication in most lists

http://www.issuesininternetlaw.com/cases/stratton.html

Blumenthal v Drudge & AOL (1998)

- Gossip columnist had agreement with AOL to create, edit, and update content of the Drudge Report; AOL could edit or remove content that it determined to violate AOL's terms of service.
- Drudge transmitted alleged defamatory statements about Blumenthal who was about to begin work as an assistant to the President
- Blumenthal sued Drudge *and AOL* for defamation

http://epic.org/free_speech/blumenthal_v_drudge.html

Blumenthal v Drudge & AOL (cont'd)

- Decision: AOL immune from suit
- Section 230 of Communication Decency Act of 1996 provides "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."
  - Immunizes providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others.
  - Congress decided not to treat providers of interactive computer services like other information providers (e.g., newspapers)

http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

Libel &Freedom of Speech

- Not all speech is protected by 1st Amendment
  - Free speech has its limitations
  - Does not permit the making of false or misleading statements (no "Defamation of Character")
- No inalienable right to disseminate defamation
- *Opinions* are usually not considered defamatory even if they do cause harm
- *Civil tort* as remedy for damage is not precluded by 1st Amendment

Limitations on Lawsuits

- Public officials are restricted in bringing defamation actions
  - Must prove "actual malice"
- Also applies to public figures
  - De facto standard of visibility
  - Includes people who don't necessarily want to be public figures

Defamation of a Business

- Can a business sue anyone for defamation?
- Current trends
  - <companyname>sucks.com
  - Many legal actions against such sites
    - ✓But many plaintiffs have *lost*
  - Sometimes employees bound by employment contracts restricting public comment

Suarez Corp v Brock Meeks (1994)

- Brock Meeks a journalist for online commentary via e-mail and Web
  - Suarez Corp accused Meeks of defamation
- Meeks raised issue of *meta-public figure*
  - Pointed out that public figures supposed by jurisprudence to have
    - ✓Public visibility
    - ✓Increased opportunity to rebut charges
  - Therefore plaintiffs qualified as equivalent to public figures
  - Case settled with $64 payment and promise of notification to plaintiff

Defenses Against Defamation Actions

- Truth
  - Not sufficient in all jurisdictions
  - May have to prove good motives
- Privilege
  - Publication in discharge of official duty
  - Legislative or judicial proceedings
  - Report in public journal about such proceedings
  - Charge or complaint to public official leading to a warrant

Rights of the Plaintiff

- Demand correction of published libel
  - If not demanded, plaintiff may lose rights for later complaint, recovery
  - Or will have to show stronger proof of loss, damage
    - ✓Loss of reputation
    - ✓Shame
    - ✓Mortification
    - ✓Hurt feeling

Now go and study