Cyberstalking and what you can do about it

David Vaile, Executive Director

Cyberspace Law and Policy Centre
UNSW Law Faculty

March 2009

http://cyberlawcentre.org/2009/cyberstalking/

Outline

- Not a law lecture, sorry
- About cyber stalking
- Legal issues
- Online features
- Role of evidence

Cyberstalking contexts

- School, youth
- Relationship/family
- Communities
- Strangers?
- Work
- Politics/public life
- International scammers?
- ‘Erotomania’ - rare? Not intend harm?

Media: the ‘cyber’

- Email
- Old web (static) – rare? Inc images, cartoons
- Social networking web sites: Facebook, MySpace
- SMS or voice on mobile
- Camera on mobile
- Instant messaging
- Virtual worlds (avatars)
- Bulletin boards/discussion groups
- Wikis
- Twitter
- Computer hijacking/malware (cybercrime)

Means

- Threats (= assault?)
- Pestering
- Defamation
- Impersonation (US case), trickery
- Surveillance, monitoring, tracking
- Allegations and complaints
- Social shunning (exclusion)
- Images, still/video, capture/send
- Partial ID theft

What’s the same?

- Intimidation
- Disempowerment
- Isolation?
- Fear or oppression
- Perpetrator not ‘the full quid’, distorted motivation, mistake-prone
- Potentially criminal
- Attempt to conceal
- Risky engaging to get evidence?

What’s different

- Anonymity
- Pseudonymity
- Nature of evidence
- Remote/distance/jurisdiction
- Tools and their implications

Other On-line/Off-line Differences

• Uses recording device	• No recording device?
• Anywhere, anyone	• More local
• Perp. hard to ID?	• Perp easier to ID
• Leaves meta-data, logs	• Leaves little trace?
• Uses IT and networks	• May use basic/no tools
• Perp feel safe?	• Perp conscious of risk
• Prone to forensic data analysis	• Physical forensics?
• Abuse of controlled space (organisers)	• Not within controlled space

Prevention:
Don’t give yourself away

- Online privacy: easy to overlook
- Risks obscure, thrill obvious
- Personal information security
- Social networking sites
- Young people w. no experience base
- Older people unaware of tech realities
- Needs broad public awareness campaign
- Privacy policies and interface bad?

Treatment: Legal aspects

- Legislative provisions, offences etc.
  - General stalking, offline
  - Cyberstalking
  - Cybercrime (using computer for offence)
  - Child abuse material if U18?
  - Defamation?
- Jurisdiction: Fed/State/International
- Cases: *DPP v Sutcliffe*, cartoon, swing
- Complex and inadequate?

Cyberstalking laws: diff by jur.

- Qld S.395B Ch.33A *Qld Crim Code* add email, ph, tech - No need for specific intent
- SA s19AA SA *Crim Law Consolidation Act* 1935 specific intent, 2 occasions
- NSW S545 *Crimes Act* 1900 Stalking or intimidatn, intent cause fear physical/mental harm
- Cth *CyberCrime Act* and *Crim Code* no use?
- *Crimes Legn Amdt (Telecoms Offences & other Measures) Act* 2004 (No. 2) – cl 474 *Crim Code Act*
- See Urbas, *Internet Law Bulletin* 10:6 Sep 07 p.62

Don’t rely on law/conviction

- Will/motivation: compromised?
- Assistance: expensive or rare
- Police: various limitations
- Laws: not fit the behaviour?
- Evidence: essential, missing?
- Conviction: often fails
- Remedies: too late?

Self help: the role of evidence

- No evidence = no chance to convict
- Evidence = weapon, perp weakness
- Useful in many stages, not only court
- Trigger for assistance, credibility
- Trump card?
- Turn the tables, take control
- Become the hunter?
- Guess what: a computer is a data recorder!

Get the evidence

- Why? - to take control
- What? - whatever, authenticated
  - Transcripts, recordings, notes
  - Screen dumps
  - Copies, downloads
  - Names, dates, times, places…
- How? - built-in/extra tools, knowledge
- When? - live, after, retain it all

Train people to get evidence

- Web guide
- Booklet
- Schools
- Advice lines with tech help
- Self help groups/supporters
- Keep it simple but concrete
- Examples for each medium, OS
- Offer extra detail for keen beans

Not a panacea, but central

- Can be useful for everything from request to buzz off to prosecution brief/admissible evidence
- If it's serious need to emphasize provenance, reliability, credibility of source and process
- A useful exercise: to develop the supporting tools to encourage and enable active evidence gathering

Use it: Evidence at work

- Negotiations
- Insurance?
- Reporting to system owners
- Seeking help
- Reporting to police
- Basis for prosecution or AVO
- Permanent record in case escalation
- (Make sure you backup! duplicates)

What’s wrong with this picture?

- While generally safe to collect, certain uses may trigger further risks
- Some people not interested or able
- Authentication requires some thought (and perhaps training resources)
- Not a magic bullet
- Perp may be too cunning?
- Prosecution may not be able to exploit

David Vaile, Executive Director

Cyberspace Law and Policy Centre
UNSW Law Faculty

d.vaile@unsw.edu.au

02 9385 3589

http://cyberlawcentre.org/2009/cyberstalking/