



Technology facilitated domestic violence against women

Alex Davis

Solicitor, Women's Legal Services NSW



Disclaimer

- All care has been taken in the presentation of information in this workshop.
- This workshop is not intended to take the place of legal advice given by a qualified legal practitioner.
- No responsibility is taken for any loss suffered as a result of the information given at this workshop.
- Copyright WLS 2015. Reproduction without the express written permission of WLS is prohibited.



What we will cover today

1. What is technology-assisted domestic violence?
2. ReCharge Project
3. Legal implications
4. Revenge Porn
5. Surveillance Devices



What is technology-assisted domestic violence?

The use of technology, such as the internet, social media, mobile phones, computers, & surveillance devices, to stalk, harass, intimidate or humiliate a partner or ex-partner





Technology-assisted DV

- **98%** of Australian DV workers had clients who had experienced technology-facilitated stalking & abuse

DVRCV/Delanie Woodlock, *SmartSafe Survey for Australian Support Workers*, 2015

- Reported to have unique impacts, some more & some less harmful than in-person behaviours

Stonard, K.E., Bowen, E., Walker, K., & Price, S.A. (2015). "They'll always find a way to get to you": Technology use in adolescent romantic relationships & its role in dating violence and abuse. *Journal of Interpersonal Violence*



Common behaviours

- Demanding passwords
- Unauthorised access of accounts
- Checking call logs, messages or accounts without permission
- Deliberate deleting or unfriending on social media
- Making false accounts
- Using technology to spread rumours
- Threats or intimidation through messages
- Large volumes of unwanted communications
- Constantly checking up on a person through technology or tracking through location settings
- Demanding, threatening to share or actually sharing private photos or videos without consent
- Hidden cameras or GPS



Recharge: Women's Technology Safety

- Joint project by WLS NSW, DVRCV, WESNET & ACCAN
- Australia-specific and Australia-wide online resource
- Legal guides for all States and Territories
- Technology-safety toolkits, how-to videos, advice and tip sheets
- www.smartsafe.org.au





Criminal Law Implications

Commonwealth

- Criminal Code 1995
- Telecommunications (Interception and Access) Act 1979
- Telecommunications Act 1997
- Copyright Act 1968

NSW

- Crimes Act 1900
- Crimes (Personal & Domestic Violence) Act 2007
- Surveillance Devices Act 2007





Civil Law Implications

- AVOs
- *Copyright Act 1968* (Cth)
- Minors: new complaints mechanism
- Victims Support
- Equitable action for breach of confidence
- Tort of intentional infliction of harm
- Tort of malicious or injurious falsehood
- Tort of intimidation or extortion
- Defamation
- ALRC inquiry serious invasions of privacy







Practical first steps

- Contact police / ACORN (www.acorn.gov.au)
- Contact Facebook or webmaster of website to take down
 - **whois.domaintools.com** for international websites
 - **whois.auregistry.net.au** for Australian sites
- Contact search engines such as Google, **support.google.com/websearch**
- Google image search/alerts
- Facebook – notify, change settings & download data

Whois response for **asklois.org.au**:

Domain Name	asklois.org.au
Last Modified	18-Mar-2014 23:59:20 UTC
Registrar ID	WAR
Registrar Name	Web Address Registration
Status	ok
Registrant	WOMEN'S LEGAL RESOURCES LTD
Registrant ID	ABN 88002387699
Eligibility Type	Company
Registrant Contact ID	R-005119401-SN
Registrant Contact Name	Helen Campbell
Registrant Contact Email	helen.campbell@wlsnsw.org.au
Tech Contact ID	C-002441781-SN
Tech Contact Name	Helen Campbell
Tech Contact Email	helen.campbell@wlsnsw.org.au
Name Server	ns1.sgp6.siteground.asia
Name Server	ns2.sgp6.siteground.asia



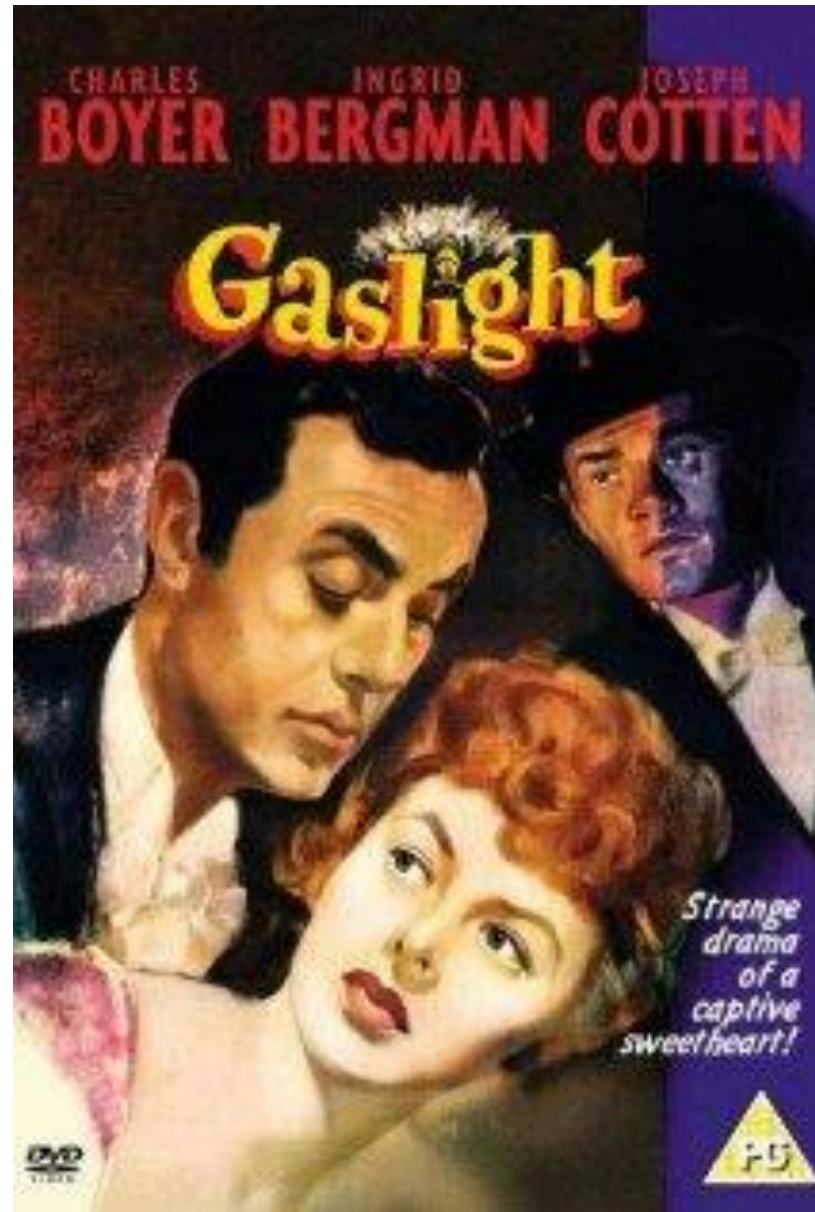
Revenge Porn

- E-Safety Commissioner for minors – takedown notices
- **AVO/ Stalking or intimidation; s 13 C(D&PV) Act 2007 (NSW)**
- **Using carriage service to menace, harass or cause offence:**
s 474.17 Criminal Code 1995 (Cth)
- **Voyeurism provisions: s 91J – 91M Crimes Act 1900 (NSW)**
- **Publishing an indecent article: s 578C Crimes Act 1900 (NSW), eg**
,Police v Ravshan Usmanov
- **Copyright infringement; s 115 Copyright Act 1968 (Cth)**
- **Defamation – eg, *Shepherd v Walsh & Ors***
- **Equitable action for breach of confidence; *Giller v Procopets*;**
Wilson v Ferguson
- **Tort of intentional infliction of harm; *Wilkinson v Downton***



Additional order suggested wording

The defendant is prohibited from directly or indirectly, publishing photographs or videos of the protected person engaging in sexual activities or in which the protected person appears naked or partially naked





Example spyware...

MSPY



Surveillance

- Google, Apple, email, social media accounts, the 'Cloud'
- Internet browsers that sync
- Be aware of children's devices, eg tablets or smartphones
- Be aware of location settings on apps such as Facebook messenger
- Be aware of passwords being saved in browsers and connected logins

Eg. Gmail, Google Search and Youtube (owned by Google); iMessage & synced laptops

- Check for spyware on mobile devices & computer
- Get client to change passwords so strong & secure
- Change security settings including location settings





Additional order suggested wording

*The defendant is prohibited from attempting to
locate, follow or keep the protected person
under surveillance*



Surveillance

- ***Surveillance Devices Act 2007 (NSW)***
 - Prohibition on installation, use and maintenance of listening devices (s 7)
 - Installation, use or maintenance of optical surveillance devices without consent (s 8)
 - Prohibition on installation, use and maintenance of tracking devices (s 9)
- ***Telecommunications (Interception and Access) Act 1979 (Cth)***
 - Telecommunications not to be intercepted (ss 7 & 105)
- **Admissibility of evidence**
 - Section 138 Evidence Act 1995 (NSW) – note discretion



Gathering evidence: what to tell clients

- Do not delete text messages, voicemail messages, photos
- Try and save them to a computer/USB flash drive
- Use screenshots with URL, date & time
- Use speakerphone wherever possible if with a support person
- Keep a diary or voice notes
- Give police permission to access phone, computer, Facebook, email account etc
- Be aware of ability to download Facebook data
- Do not engage in reactive responses with offender
- Remember improperly or illegally obtained evidence cannot be used in court unless the probative value outweighs how it was obtained



Further information

- SmartSafe
 - www.smartsafe.org.au
- Digital stalking: a guide to technology risks for victims
 - www.digital-stalking.com
- DVRC – technology safety planning
 - www.dvrcv.org.au/knowledge-centre/technology-safety
- Publication: Digital stalking: A guide to technology risks for victims (version 2, Nov 2012), Jennifer Perry
- Ask LOIS resources