An unruly new realm of personal information distribution: Social media and the law - developments

David Vaile
Executive Director
Cyberspace Law and Policy Centre
Faculty of Law, University of NSW
http://cyberlawcentre.org/
Outline

Regulation

- Lessig and Code
- Online and Social media impacts
- Technological changes
- Legal disconnects
- Struggle for regulators to keep up

Special Features of the online social environment
- A ‘wicked problem’?

- Infinitely Long and Short
- Australian v International material
- IT security: Perimeter must fail
- Four horsemen of the personal info security apocalypse
- Challenges for regulation
- Recent Prosecutions
- Where are we left?
Lawrence Lessig’s *Code*

Lessig identifies possible sources of regulation *(Code and other laws of cyberspace – 2.0)*

http://codev2.cc/

- **Law** (black letter, *cf.* actually enforced? Privacy?)
- **Technology** itself, a.k.a. *'Code’* (functions/limits)
- **Social norms** (netiquette, social practices?)
- **Business practice** (new social host business models, where the user is product, not customer?)
Online and social media impacts

Tech changes
Cultural changes
Legal changes
Technological changes underlying

- Offline world was nice and simple, for regulators and courts
- Web 1.0: global publication, old media publish models: AustLII
- Web 2.0: social networking, user generated content: Facebook 1
  - Convergence of producer and consumer, + distributor
- Web 3.0?: mass personalisation, semantic web, wearable tech.
  - It’s not just your friends who know you and what you mean
- Attack of the killer toddlers – we are so old!
  - Hackers retire at 15, kids turning tech. tables on parents, ‘slash’
  - Facebook does not enforce own entry test of ‘at least 13 yrs old’
Ye Olde Worlde (–2006)
New fangled (SNS/UGC)

ISPs: the new block point
And then there was ‘2.0’: Features

- Social networking, user generated content, degenerate narcissism
- Blurs boundary: Publishing *cf.* Personal Communications
- From centralised one-to-many topology to distributed network
- Everyone is both consumer and producer (‘prosumer’)
- Everyone is a permanent global publisher; can be intermediary
- Every device is an endless movie source: deluge of data
- No editorial brain involved (both users and ISPs)? No selection?
- ISP replaces Publisher as key point – very significant? *iiNet*
Cyberlibertarian fantasies still delude and excite (Decl. of Indep. ‘96)

Reality: Jurisdiction out of control, hyper liability (for you)
  Intensification, not escape, from jurisdiction (revenge of the States)

Or: no care, and no responsibility? (for the Cloud)
  Your data and business go offshore, but not legal protection?

The rise of the sub-human: minors at the frontier
  Deficit in ‘consequences’ cognitive development: paternalism?
  ‘Under the age of 18 or appears to be under 18’: kids make porn?

The fall of the ‘common carrier’: ISPs reluctantly change masters?
  Agents of a foreign power, or a hostile litigant interest? CoE CC
  Enforced discipline of their customers, on pain of sharing liability?

‘Info just wants to be free’?
The struggle for regulators to keep up

- Offline: centralised distribution, choke points: edit/publish
- Web 1.0: more distributors, easier importation
- Web 2.0: everyone is a creator, (re)-publisher, exporter
- Web 3.0: the Cloud knows what you like, and makes it?
- Encryption and roll-your-own protocols already in use
- The long cyber-war: endless arms race between the straiteners and those seeking to avoid the blocks? Enlivened by real armies.
- When is publication not publication?
- Confused discussion: Surely it is censorship? No First Amdt.
- Chinese solution: you never know: the Panopticon: (no-one home, but you self censor)
Special Features of the Online Social Environment

- Lifespan
- Cultural changes
- Legal changes
Why online media control might be a ‘wicked problem’

- Rapid constant evolution of technology, cultures and practices
- Scope is unmanageable? A billion FB users, a trillion items
- Classification model unviable? Urge to ‘filter’ - terminology
- Design philosophy of the net – under attack? Or net resists all?
- Supposed beneficiaries of protection also main perpetrators?
- Moral panic: ‘The Panic Button’ as solution? Overcriminalised?
- Real targets are parents? Wishful thinking? Or real victims?
- Temptations of ‘policy-based evidence’? Filter, safety, retention…
## Infinitely long and short lifespans

<table>
<thead>
<tr>
<th>‘The Document that Never Dies’</th>
<th>‘Document that Hardly Ever Lived’</th>
</tr>
</thead>
<tbody>
<tr>
<td>✬ Google Cache: days [next]</td>
<td>✬ Instant messaging, text: Arab Spring 2.0 demonstrates they are not really transient, but used as if... ?</td>
</tr>
<tr>
<td>✬ Internet Archive/ Wayback Machine: years [next]</td>
<td>✬ Snapchat: <a href="http://www.snapchat.com">www.snapchat.com</a> A smartphone app shares photos and videos that self-destruct after viewed once for up to 10 seconds; warns if recipients attempt to capture screen? [Next]</td>
</tr>
<tr>
<td>✬ Legitimate personal copies</td>
<td>✬ Fast Flux injection: malware staple</td>
</tr>
<tr>
<td>✬ Illicit personal copies</td>
<td>✬ Roll your own protocols and tools!</td>
</tr>
<tr>
<td>✬ Facebook’s ‘inactive’ accounts: creature from the black lagoon?</td>
<td>✬ DFAT, former ASIO, chief declines to commit to writing (Zygier case)</td>
</tr>
</tbody>
</table>
Welcome to the website of the Judicial College of Victoria

We ensure judicial officers are provided with opportunities to enhance their skills, knowledge and abilities
Australian cf. international material

- Extraterritoriality, foreign jurisdiction limits, ‘data sovereignty’
- Difficulties for censorship, suppression, takedown, prosecution
- Onshore: Notices (Content Takedown, Link deletion, Stream cessation) for items hosted in Australia from ACMA, Courts
  - Directed not at author or owner, but ICH, intermediary
  - No motive to resist? Or seek actual classification, review?
  - No obligation online to classify, check, edit (cf film, game, publ.)
  - ‘Prohibited’ or ‘Potentially prohibited’: RC, X18+, some R18+, MA15+
- Potential to use Council of Europe Cybercrime Convention by, and in, USA and EU to streamline criminal prosecution: 1/3/13!
Perimeter security: FAIL

- Firewall
- Antivirus
- Anti-spyware
- Other IT security
- Common sense
Why IT perimeter security must fail

- Needs to be 100% effective
- For a connected device, 99.9% means that 0.1% loophole will be found, in seconds or weeks.
- No IT security tools is even 99.9% effective.
- The other side are in a constant arms race with the IT security providers and other vendors trying to keep them out.
- They only need the tiniest crack – easy to achieve eventually
- Constant innovation by some of the smartest IT people on the planet, and legions of ‘script kiddies’ using auto-mutating tools
Is IT security broken?

- Unix IT security model (WinNT, Mac, *nix) doomed
  - Assumes informed user. But complicated, we’re all bozos.
- Perimeter defence model is doomed: 0.01% vs 99.99%
  - Hacktivists and crims can get into anything
  - Minutes/hours before any honeypot compromised?
- No basis for user decision to agree, click; false alarms.
- Zombies & malware industrialise rapidly, mass customise
- Implications: we definitely can’t keep them out, or info in.
Four Horsemen of the [online privacy/security] Apocalypse

- Overzealous
- Over-opportunistic
- Hacking
- Scams
- and Your ‘Friends’

GOV’T • BUSINESS

YOU • CRIMs
Why do these ‘Four Horsemen’ matter?

✧ Presumption by many that government and industry are ‘here to help’, rather than ‘part of the problem’.

✧ Much cyber-safety and cyber-security education material is distorted by this assumption.

✧ Good players in all four sectors, but serious risks from all too.

✧ Failing to see this may blind users to the worst risks for them in a given situation. Courts may look in the wrong place.

✧ Also conveniently avoids focusing attention on governance and public policy failures which create such institutional risks!
Challenges for regulation

- Impossible to treat online content same as offline mass media
  - Human classification, processing, review: orders too expensive
  - Machine classification, automation: intrinsically ineffective
  - Transparency and accountability (old) v. secrecy (new)?
- No ambition/hope to classify/control all – but what to say to parents, victims, or litigants?
- Complaints/reporting as a visible response... Then what?
- Problem of the social network giants: too big to care, too big to afford to deal with individuals? ‘Customers’ cf. ‘Products’?
- Potential of exemplary prosecutions? Shock of consequences?
Recent prosecutions

:NSW Dist Ct.: *Police v Ravshan USMANOV* [2011] NSWLC 40

 Publish Indecent Article, s578C of *Crimes Act* 1900 (NSW)

- Non-internet offence, old offence!
- Former partner, pictures posted, created during the relationship
- Intent to cause distress, a means of ‘getting back’ at former GF.
- Plea of guilty, failed bid to minimise sentence, 6 mo. suspended
- Poor legal advice, Dep CM unimpressed with ‘it was nothing’.
- No precedents, magistrate picks middle of range to start.
- Discount for plea (25%), then adds 25% for lack of contrition
- Dist Ct. approved 6 months result, agreed shd be suspended
Recent prosecutions (cont.)

- Vic Bendigo Mag. Ct: **Henderson** 2011, breach intervention order
  - Full admissions, said it was only harmless fun. No relationship.
  - “couldn’t understand how she had proof he posted the comment”
  - Illustrates lack of appreciation of both the harm and the evidence gathering capacity of online systems. Importance of data forensics!
- **McCrory and Turner**, Aug 2012, same town! **Revived** 2013!
  - ‘Root Raters’ – FaceBook’s original purpose?
  - ‘Use carriage service to offend’: **Criminal Code** (Cth) s474.17?
  - ‘publishing objectionable material online’: ??
  - Jail terms reduced to Community Corrections Orders on appeal
Where does this leave us?

- Ignorance of consequences a key driver
- Will prosecutions make any difference?
- The politics of gesture? Or just the shock needed?
- Will we ever have a proper discussion of needs of young pp?
- Failure of local and US regulators to hold giants to account creates culture of impunity – rewards ‘see if you can get away with it’ not compliance. Absence of auditing and protection for individuals’s data?
- Uncertainties in user requesting or court ordering takedowns.
Questions?

David Vaile
Cyberspace Law and Policy Centre
Faculty of Law, University of NSW
http://www.cyberlawcentre.org/
d.vaile@unsw.edu.au
0414 731 249