What is Private and Public in Social Networking?

[and who wants it to be that way?]

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

For Privacy Reform and Compliance Forum
13 June 2012

Based on:

✦ Workshop for NSW Privacy Commissioner last year

✦ Judicial Commission of Victoria on the conflict between court powers to suppress identity and the culture of exposure online

✦ Meetings with Facebook's global privacy director, Google, direct and online marketing industry bodies

✦ Research into Communications Privacy Complaints handling, online Codes of Conduct, Data sovereignty & the cloud (3 reports)

✦ Experience as consumer and privacy advocate, and litigator

✦ Late night calls from women regretting 'provocative' photos…

What is Private and Public in Social Networking?

✦ This discussion is to encourage you to re-think and perhaps reject, the temptation to think that, because Social Media have lured some users into a culture of thoughtless, disrespectful over-sharing, this represents a licence harvest and feed the Big Data juggernauts straining at the leash to get at this loot.

✦ Social Networking is in the process of imploding, with the basis of trust it relies being undermined by: excessive advertising; irresponsible exposure to risk of teenagers, children, infants and babies; a proliferation of new modes of abuse; and jolly old Uncle Sam now turning up at the party to tell us to carry on while what would have been the KGB's dream is strapped on.

✦ If Golden Goose is to survive, privacy must come back, not die.
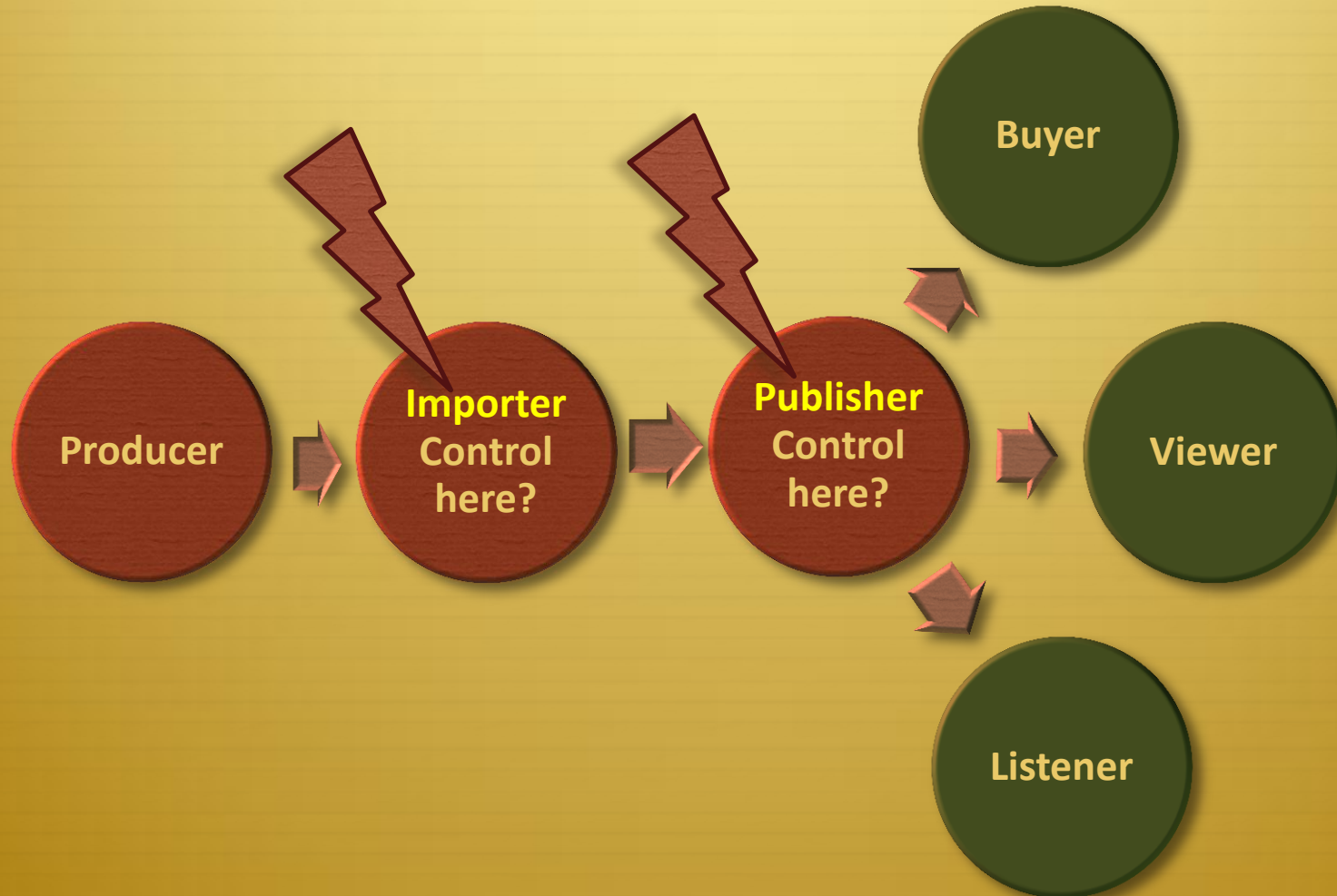
Online and social media impacts
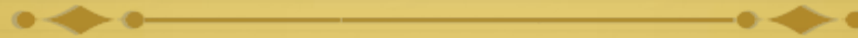
Tech changes
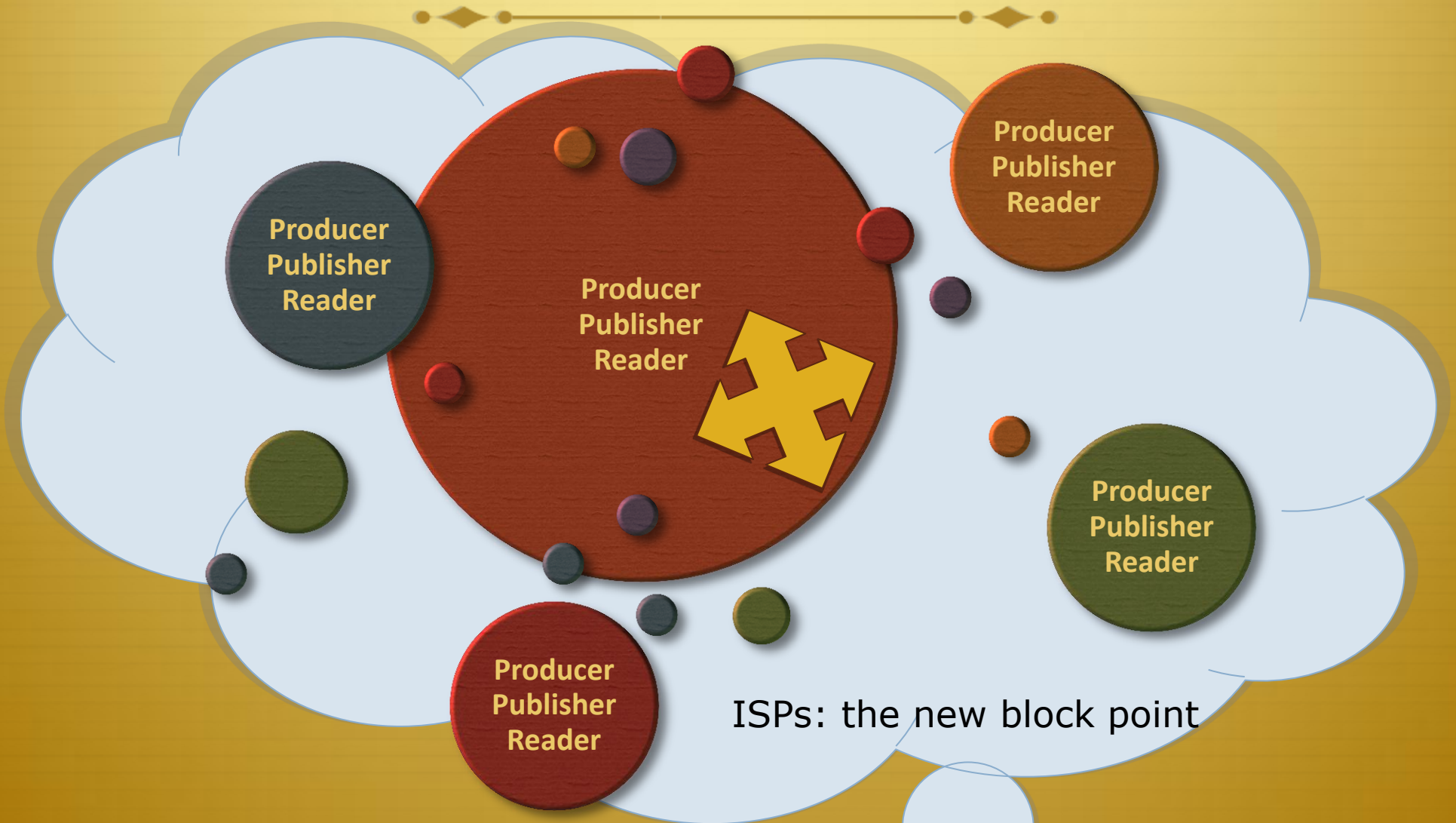Cultural changes
Legal changes

Technological changes underlying

- Offline world was nice and simple, for regulators.

- Web 1.0: global publication, old media/publish models.

- Web 2.0: social networking, user generated content.

  - Convergence of producer and consumer, + distributor.

- Web 3.0?: mass personalisation, semantic web

  - 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 filter tables on parents, slash.

  - Facebook does not enforce own rule of at least 13 yrs old

Ye Olde Worlde (–2006)

New fangled (SNS/UGC)

Producer Publisher Reader

Producer Publisher Reader

Producer Publisher Reader

Producer Publisher Reader

Producer Publisher Reader

ISPs: the new block point

And then there was 2.0

- 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.

- Every device is an endless movie source: deluge of data.

- No editorial brain involved (both users and ISPs)? No selection?

- ISP replaces Publisher as censor point – very significant? *iiNet*

Legal disconnects:
'Info just wants to be free'?

✦ 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?

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: talk privacy but no rights. No *1st* or *4th Amdt.*

✦ Failure to pass legal right to privacy undermines social use of new technologies, as old law assumes only business and government

The battle over the nature of privacy

✦ More than about 'secrecy': right to be left alone, to be free of impact of constant, deliberate spying trying to get inside your head.

✦ China: never know/Panopticon: no-one home, but you self-censor

✦ Definition of 'Personal': US much weaker than EU, AU – metadata.

✦ Aggressive attacks from the jack-boot brigade demanding: "If you've got nothing to hide, you've got nothing to fear" [PINs please]

✦ Aggressive attacks from Murdoch press insisting that no sensible person would advocate for a legally enforceable right to privacy.

✦ Aggressive attacks from Online Behavioural Marketers, insisting uber-veillance & psycho-graphic profiling must be the price of entry to world they colonised, but was made for free by others.

The Four Horsemen...

Are we (almost) all part of the problem?

The Four Horsemen of the PI Apocalypse

- ✦ I start from User/ Citizen/ Consumer/ Voter/ Customer perspective, so not take other stakeholders at face value.

- ✦ Risk driven development, 'User centred design' is the only way to make safe software that works. Risks for users first & main thing.

- ✦ (Backed up by consumer protection experience; Codes often fail)

- ✦ Other participants, stakeholders, interests in online social media often claim to be, like Kevin, 'here to help'.

- ✦ But most have potential conflict of interest, so use spin to deny.

- ✦ Necessary to recognise that, rather than there being a bunch of bad guys, tame consumers and nice helpers, many are complicit …

Four Horsemen of the [online privacy/security] Apocalypse

- Over-zealous

- Over-opportunist

GOV'T

BUSINESS

YOU

CRIMINALs

- and Your 'Friends'

- Hacking

Why do the Four Horsemen matter?

- Presumption by many that government and industry are 'here to help', rather than both being part of the problems.

- Much cybersafety and cybersecurity 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.

- Also conveniently avoids focusing attention on governance and public policy failures which create those institutional risks.
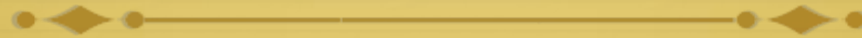
The Four Horsemen and social media

- Global online **Business** models: some built on users being data-hamsters ('you are the product') not customers. CONFLICT?

- **Government** concern about abuses, but tempted by access to wantonly exposed data (retention, data mining). CONFLICT?

- **Bad guys** adapting fast to the active promotion of gullible self indulgence, harvesting for anti-police face recognition efforts.

- Some **Individuals** disrespectful of their own and other people's personal information security and privacy. Ignorance, youth: key

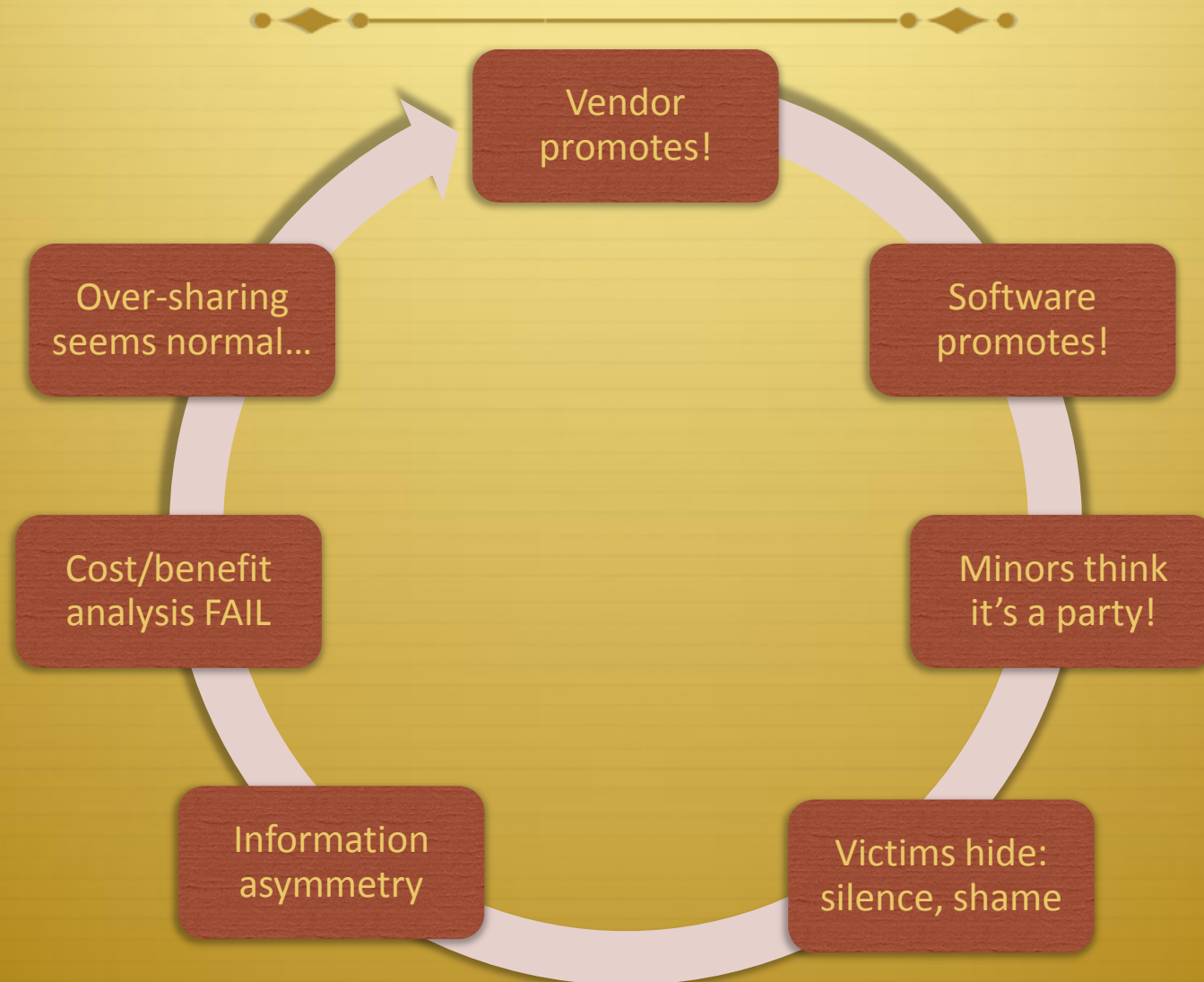- These four nasties should not lower the bar.

Private ➜ Public [➜ Private]

* One goal of the Horsemen is to capture personal information by a process of luring it out into the open.

* Claiming a bit of info about you is 'public' is not for some enhanced communal social space, the normal idea of 'public'.

* though encouraging people to be public seems harmless ...

* But it is often with the ulterior motive of re-capturing the PI and appropriating it back into different private hands, grabbing it for private uses often hostile to the original owner:

* Psycho-graphic profiling for marketing; Mass surveillance by secret foreign spy services; setting up a scam by fraudsters.

Social Media and the Push for Over Sharing

All the information and incentive goes one way…

Social media and PI: Over-Sharing FAIL

Vendor promotes!

Software promotes!

Minors think it's a party!

Victims hide: silence, shame

Information asymmetry

Cost/benefit analysis FAIL

Over-sharing seems normal…

Personal Information Security and social media

✦ It's permanent global publication; but without the editor, lawyer, publisher or shredder.

✦ All very new, rules change daily, no base of social experience to build a new 'common sense', no shared history of known Fails.

✦ Failure to appreciate consequences are not here, now, visible.

✦ Kids cognitive deficit – special vulnerability – need protection from everyone, including themselves (they are NOT adults!)

✦ Teenagers: consequence has to be right here and now to matter Children: even right here and now can be denied. [ACCAN eg.]

✦ Denial is part of the problem; must help kids grow out of it.

Personal Information Security
and social media *(cont.)*

 * Adults potentially deluded: by collusion of conflicted businesses with over-sharing choices, by friends, by info. asymmetry, secrecy.

 * Past 'common sense' about tech. eg photos no longer apply: permanent global publication, face recognition, tagging, invisible.

 * Eg: "Glassholes" backlash against Google Glass: a sign that novelty is no longer enough to befuddle? Desire to protect space

 * Aggressive appropriation of public space by those with new social surveillance tools is hostile to the interests of others.

 * Impact of Facebook on policing not widely admitted, but serious.

So, what is the blind spot of the smartest guys in the room?

✦ Online social networking giants are intensely creative software and advertising powerhouses, driven by hacker instincts, now massive.

✦ **'Move fast and break** [take?] **things', 'Ask forgiveness not permission'** are slogans from immature software developers raised to work with disposable throwaway prototypes, not compliance.

✦ Category error: human personal information, the stuff of lives, is **NOT disposable**. 'Oops, we'll fix it next version!' is not an answer when personal information abuse causes irrevocable harm. Their governance model, based on rapid prototyping, cannot cope.

✦ These models are now so profitable that there is now great commercial pressure to NOT adapt to this hard and real truth.

What are some risks of private information appropriated into the 'public'?

✦ Prospects for employment, insurance, housing, travel, security clearance, public office …

✦ Damage to personal relationships, trust, family, marriage, sex …

✦ Sexual or other harassment, smearing, shaming, vilification.

✦ ID theft, fraud, burglary, robbery, scams, framing.

✦ Profiling as national security, criminal or political risk; blackmail.

✦ Recruitment into inappropriate activities of all sorts by pressure.

✦ Personalised messaging designed to 'go under the radar', use personal preferences to avoid critical assessment of message.

Asymmetry: Bad news hides

- Social media is self advertising, and advertising for the self, but it only tells half the story, the bad news tends not to get out.

- Benefits are obvious, immediate, personal, and flogged to death. Risks and costs are remote in time, place or social space.

- Funsters advertise themselves and fun, but like most privacy disasters, privacy failure victims often hide, drop out, are socially excluded, go quite, self harm, even suicide.

- They do NOT say: 'Hey everyone, I was a real idiot, who knew there is a real world out there and not everyone is my friend? Don't be stupid, and learn from my mistakes!' So no feedback.

- Result: Users are unaware; unable to properly weigh cost cf. risk. So? 'Informed consent' re: sharing is undermined, unreliable.

The Four Horsemen are the enemy

✦ Government has powers of compulsion as well as persuasion, and can be tempted to exploit fears to act in secret. [PRISM] Regulators are subject to risk of 'capture' and taming.

✦ Businesses undermining a strong approach to respect for self and others' privacy have both a strong profit motive, and the best tools of persuasion and spin, as advertisers and marketers!

✦ 'Bad guys' are not going to be 'scare the horses' by being very visible in their exploitation of over sharing, but they're skilled.

✦ Individuals trampling the rights of themselves, friends or strangers tend to lower the bar, normalising risky behaviour.

✦ Are you with them, or with those working to regain the balance?

What next?
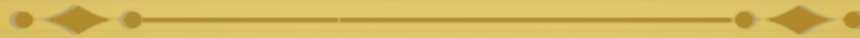
What to do?

- ✦ Revisit **assumptions** about the supposed conversion of personal information from the private to the public sphere.

- ✦ Acknowledge the potential **conflict of interest** that comes from the desire to appropriate and use this newly 'freed' information for your essentially private purposes.

- ✦ Be extra sensitive to the various **risks** of harm, and thus the potentials for conflict of interest between the beneficiary of this appropriation, and the often uninformed or immature original owner.

- ✦ Contemplate the importance of being **trustworthy** if you want trust. Treat people like customers and people, not the product.

Some helpful hints

- Encouraging **restraint**, not over-sharing, is a positive obligation.

- The debate on **PRISM** may change things – watch closely!

- If Cloud based social media based in US are untrustworthy, **data sovereignty** may become more of an issue. EU's day comes?

- **Trust** will become more of an issue, secrecy more suspicious.

- Old laws work: **s578C** NSW *Crimes Act* 'Publish indecent article' *Police v **Usmanov*** [2011] NSWLC 40.

- Tools like **Ghostery** open eyes to the 2,000-strong industry doing otherwise invisible commercial bugging, snooping and profiling.

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