

Outline



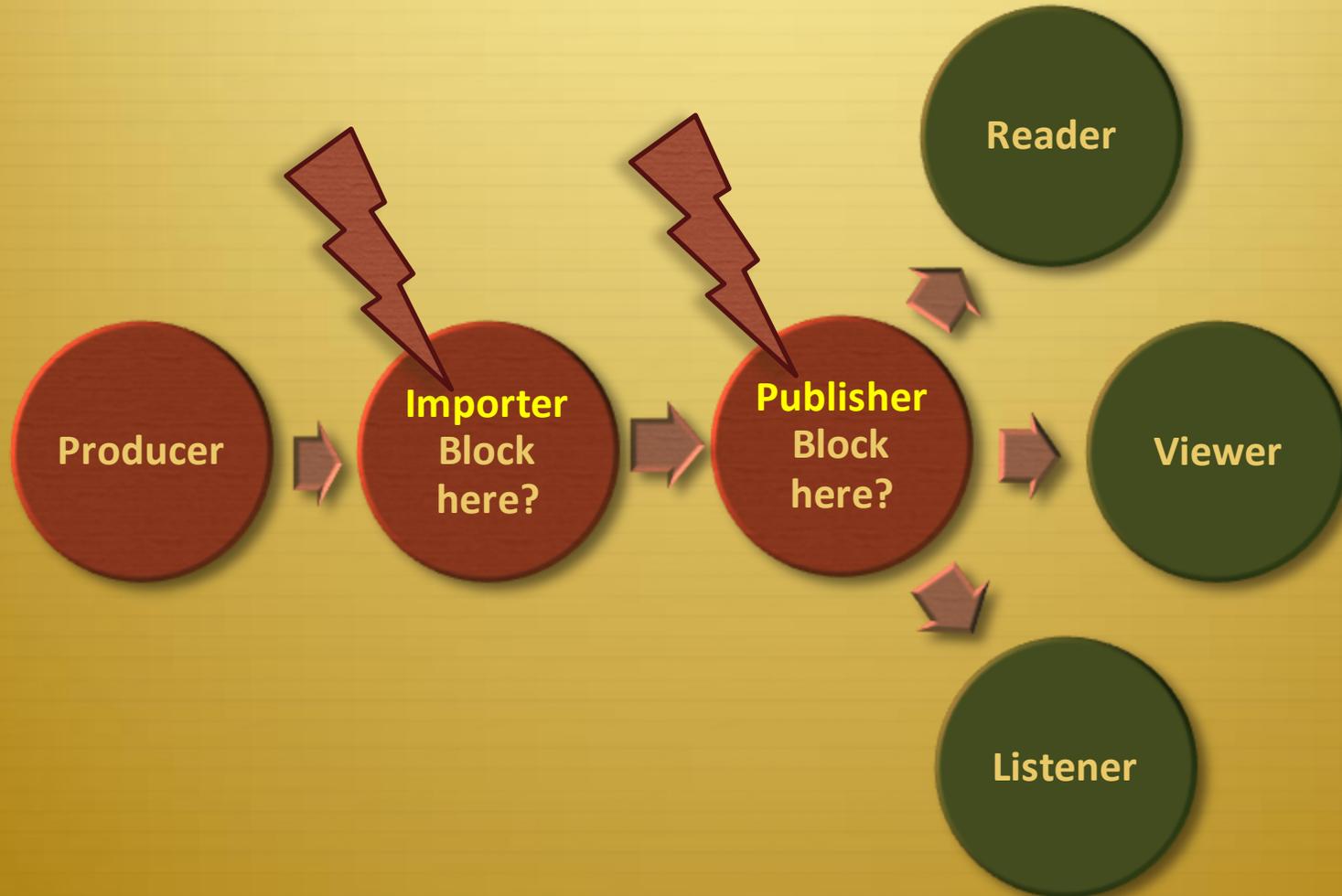
The new environment

- ✦ New fangled things
- ✦ Technological changes
- ✦ Legal disconnects
- ✦ Struggle for regulators to keep up
- ✦ Perimeter security fail
- ✦ IT security broken?
- ✦ Research for CI
- ✦ Challenges for customers

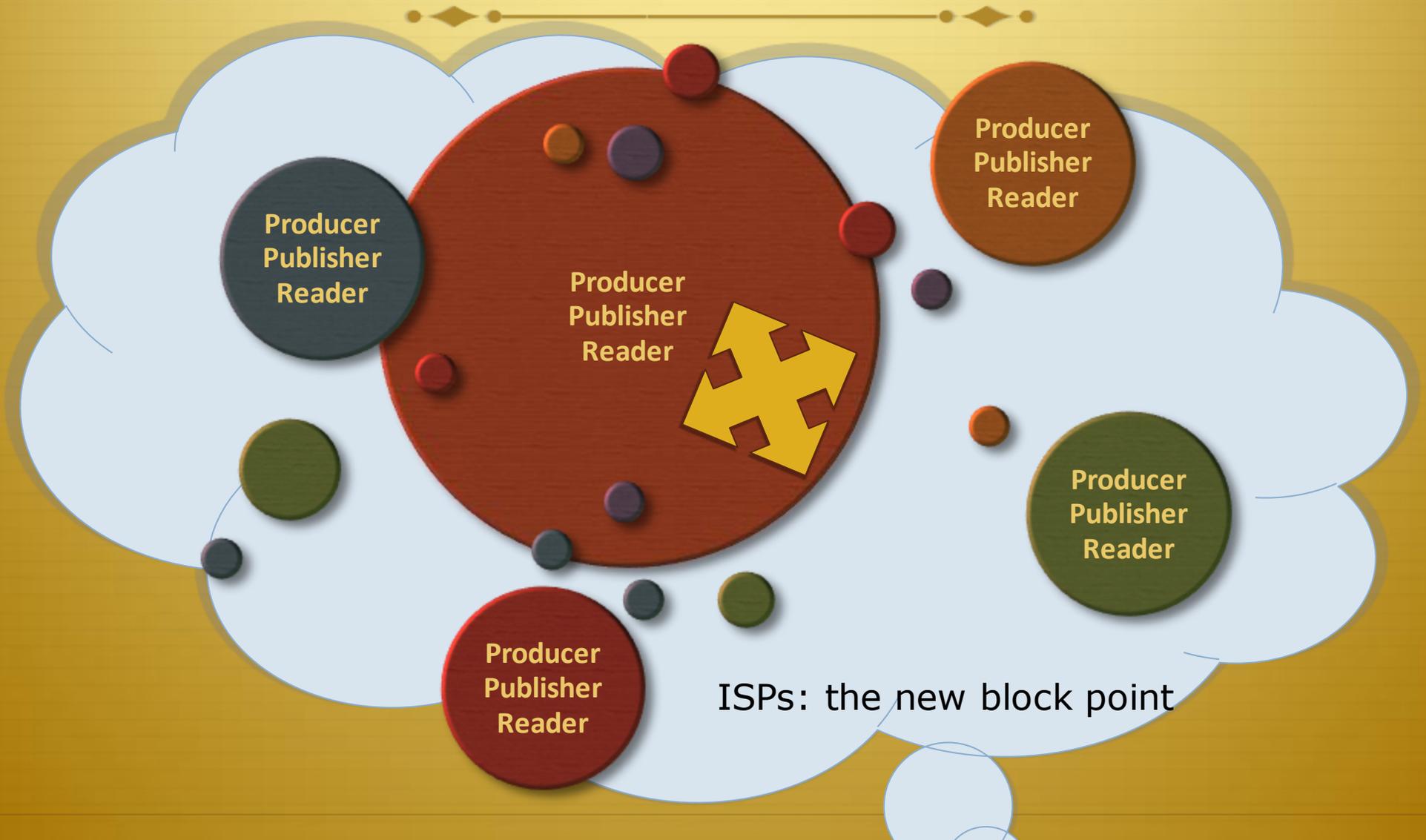
Special Features of online market for content

- ✦ A 'wicked problem'?
- ✦ Where does this leave us?

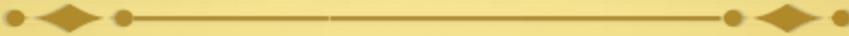
Ye Olde Worlde (-2006)



New fangled (SNS/UGC)



And then there was '2.0': Features

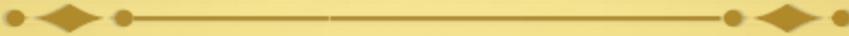


- ✦ Social networking, user generated content, degenerate narcissism
- ✦ Blurs boundary: Publishing *cf.* Personal Communications
- ✦ From centralised one-to-many topology to distributed network
- ✦ Everyone is both consumer and producer ('prosumer')
- ✦ Everyone is a permanent global publisher; can 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*

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 just do it
- ✦ 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: Surely it *is* censorship? No *First Amdt.*
- ✦ Chinese solution: you never know: the Panopticon:
(no-one home, but you self censor)

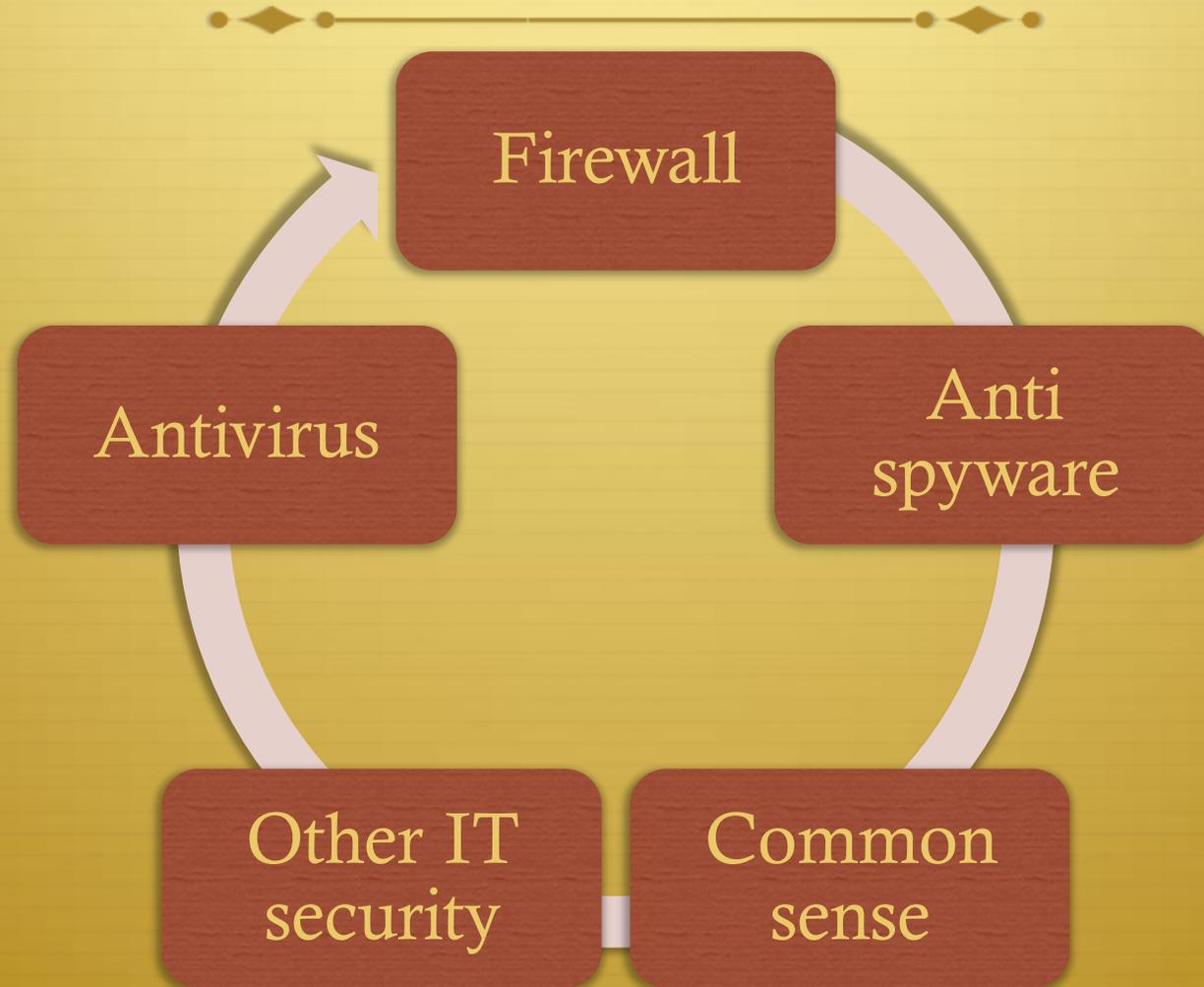
Special Features of the Online market for content



Why online content control might be a 'wicked problem'

- ✦ Rapid evolution of technology, cultures: Are we keeping up?
- ✦ Design philosophy of the net – under attack? Or net resists all?
- ✦ Scope is unmanageable? A billion FB users, a trillion items
- ✦ Moral panic: 'piracy' as model? Overcriminalised?
- ✦ Customers also main perpetrators?
- ✦ Real protection is for pre-digital and earthly territorial models ?
- ✦ Temptations of 'policy-based evidence'? Stats and Stats
- ✦ Story of the researcher who secretly understood 'piracy'

Perimeter security: FAIL



Why IT perimeter security must fail



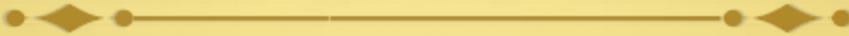
- ✦ Needs to be 100% effective
- ✦ For a connected device, 99.9% means that 0.1% loophole will be found, in seconds or weeks.
- ✦ No IT security tools is even 99.9% effective.
- ✦ The other side are in a constant arms race with the IT security providers and other vendors trying to keep them out.
- ✦ 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% v 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.

Research for CI



- ✦ 2006 Copyright Act changes, legalised ipods, TiVo
 - ✦ Sample of 1500, late 2010
 - ✦ Few noticed they were law breakers before, or change.
- ✦ Of the minority who noticed,
 - ✦ Illegal ipod and TiVo seen as unfair
 - ✦ Increasing fairness linked to increasing reluctance to cheat
- ✦ No basis for 'give them an inch, they take a mile' fear
- ✦ Supports adapting law to expectations to increase compliance

Challenges for customers



- ✦ Many are happy to pay, but on good terms
 - ✦ Actually offer for sale: full catalogue
 - ✦ On time
 - ✦ Fair price, durable, many outlets
 - ✦ High quality, fast, no threats
 - ✦ No compatibility or DRM problems
 - ✦ \$\$ goes to artist, not only middlemen
- ✦ Existing online offerings often fail...
- ✦ Unauthorised downloads offer some benefits
- ✦ Potential for adaptive business model?

Where does this leave us?



- ✦ Movie industry seeking to hold on to sinking model?
- ✦ Do prosecutions make any difference? Or annoy customers
- ✦ Is the customer right? What if we gave them what they want?
- ✦ Will we ever have a proper discussion of needs of young pp?
- ✦ Failure of local and US regulators to push rights holders to “meet the market”, share the digital dividend, and sell on good terms?
- ✦ Excessive legal protection as a barrier to innovation?

Questions?



David Vaile

Cyberspace Law and Policy Community

Faculty of Law, University of NSW

<http://www.cyberlawcentre.org/>

d.vaile@unsw.edu.au

0414 731 249