

The Security of DRM and Alternative Compensation Systems

Peter Eckersley

Computer Science &

Intellectual Property Research Institute of Australia

University of Melbourne

pde@cs.mu.oz.au

Talk Outline

- An analysis of digital copyright as it exists today, and alternative policies
- Focused on “non functional” copyright material for private consumption (books, films, music, web sites); software is a separate, harder, problem
- Will try to emphasise technical aspects of policy more than economic, legal and other issues
- Extracts from thesis, “Digital Copyright & The Alternatives”

Economic basis for copyright

- Digital authorship produces *public goods*
 - Everyone can enjoy them without diminishing others' enjoyment
 - By their nature, once a few people have them, everyone gets them
- Public goods are great but businesses do not get a concomitant return for producing them
- This is called the *free rider problem*

Part of a Larger Analysis

- Comparison of four characteristic policy “regimes” for digital copyright/alternatives
- Firstly, set out the regimes: what defines them, how do they operate?
 1. The status quo: pragmatism and inconsistency
 2. Information anarchy: no enforceable copyright
 3. Information feudalism: strong DRM enforcement
 4. Virtual markets: sophisticated public funding
- Then, compare the regimes: for what reasons might we prefer one to another? How much?

1. The *Status Quo*

- Copyright and anti-circumvention laws are very strict
- Supported by “information pragmatists” who are optimistic about marketplace solutions
- Enforcement is patchy: mostly non-existent but sometimes draconian; DRM gets cracked
- 30-40% of Australians infringe music copyrights
- 10% regularly download music from P2P sources
- Risk of “war on copying” like the “war on drugs”

2. Information Anarchy

- Information anarchy is a state of unregulated copying
- It may be a policy choice, or it may result from the enforceability of existing laws
- Anarchy may be present in some industries but not in others; it may be limited to private, non-commercial copying (or not)
- Artists and information producers are limited to whatever ad-hoc means they can find to raise funds (tip jars, street performer protocol, playing live, selling t-shirts, doing ads)

3. Strong DRM

- Has been labelled “lockdown” or “information feudalism”
- Reproduction (especially digital) made very difficult by ubiquitous strong DRM systems
- Piracy (especially P2P) driven underground; most people just buy their media files
- Enforcement can focus on professional pirates and “subversive” geeks

4. Public funding

- A few proposals for “alternative compensation systems” have been discussed in the recent legal and economic literature
- Property-like copyright is replaced with a system of taxation-funded remuneration for artists and publishers
- I've developed the most technically detailed proposal, for a “virtual market” which distributes public funding based on a combination of usage measurement and voting
- Some limited precedents in existing © systems

4 (cont.) Virtual Markets

- Collect taxes from blank media / connectivity / general revenue sources; set tax rates by extrapolation
- Measure each person's usage of © works in order to generate preference ratings; allow users to change those ratings if they wish (ie, vote)
- Add up everyone's normalised ratings in order to determine how much of the pie goes to the creators (owners?) of each work

Flagging Some (semi)technical Issues

- Strong DRM
 - Can the bar be set high enough for obtaining an unencrypted digital copy of your song/film/ebook?
 - Can anything be done about analogue to digital conversion?
 - Can P2P channels be closed?
- Virtual Markets
 - Can data be collected reliably and confidentially?
 - Can methods of “gaming the system” be controlled?
 - What hardware support is necessary?

Diversion: “Trusted” Computing

- Originally, an idea for hardware to facilitate DRM copyright enforcement
- Has caused a great deal of fear in the computer security and free/open source software communities (RMS: call it “treacherous” computing)
- Surprisingly, turns out to have useful applications in *alternatives* to copyright

Key features of Trusted Computing

- a embedded system known as a “tusted platform module” (TPM) is included on the motherboard
- able to collect “integrity” measures (IMs), eg:
 - hashes of kernel and executable code images
 - sanity checks on stacks, working memory & libraries
 - configuration files, register values, clock settings
 - anything else someone thinks of
- Is able to *remotely attest* these measures using an embedded private key
- Can establish cryptographic sessions with remote systems during which these IMs are preserved

Trusted Computing (continued)

- Parties can refuse to execute a protocol unless the other party is running a setup they approve of
- TPM can store data (crypto keys) for trusted application use only
- The task of would-be hackers is much harder: they must avoid tripping on any IMs
- As soon as a flaw or attack is discovered, users can be forced to upgrade before they are re-admitted to the network
- These powers can be used for good or evil!

Applications of Trusted Computing

- Files (.wma, .avi, .pdf, .doc, email) can be sent with access limited to approved applications
- P2P & anonymising networks can refuse to communicate with unofficial clients (“darknets”)
- You can *really* check for rootkits on your box
- Internet voting can be made reasonably secure
- Virtual markets can collect reliable usage/voting data on the popularity of copyright works
- EFF: would be better if there was an *owner override* option (preventing the first two uses)

Feasibility of Strong DRM

- Trusted computing is a good first step: fewer software leaks, and they can be closed (ADC still possible; books are a problem too)
- Hardware-based DRM systems (particularly in consoles) have a record of being rapidly circumvented by physical modification of hardware
- True robustness requires defences against that modification
- Watermarks + traitor tracing provide some reinforcement (but this is limited)

Tamper Resistance

- Need to consider:
 - physical interference (files, drills, solvents, etc)
 - low voltages, power surges, arbitrary clock signals
 - rapidly changing and extreme temperatures
 - radiation
- IBM 4756 / 4764 implements countermeasures for all of these on a PCI card
- Costs \$1000s; IC variant possible for \$US 20-30?



Feasibility of Virtual Markets

- A secure platform for measurement / voting is very important... but we want to use... the PC
- Could be obtained in several ways:
 - Controlled sampling with vigorous oversight
 - Separate, hardware “dongles” (simple, trustworthy *but* tradable & only good for download counting)
 - Trusted computing!
- The last two should be coupled with the use of minimalist honeypots to detect attacks in the wild (TC is nicest for cleaning these up)

Virtual Market Feasibility (cont)

- Need to count the votes reliably and anonymously
 - Could try to use some elaborate, offline process to create a trustworthy electoral commission (this is hard)
 - Or use a mix net
- To reduce incentives to cheat:
 - make votes hard to verify; let users overwrite them; minimum thresholds & quantisation for remuneration
 - remind users of the benefits they get from the system
 - law enforcement

Normative comparison of © regimes

Regime

Aspect of Comparison

	<i>Status Quo</i>	<i>Anarchy</i>	<i>Strong DRM</i>	<i>Virtual Market</i>
<i>Artificial scarcity</i>	=			
<i>Incentives for production</i>	=			
<i>Infrastructure, computer security + enforcement</i>	=			
<i>Transaction costs</i>	=			
<i>Taxation overheads</i>	=			
Conclusion relative to status quo	=			

Comparative Security Costs

- Strong DRM turns out to be much more expensive
 - Many, many weak points: US \$20-\$30 per device for tamper resistant ICs (or \$100-\$150 for miniaturised 4758-style assemblies). Australians buy 7 million devices a year.
 - Digital leaks can be very, very disruptive (a hacked gadget or someone walking out of Sony with a hard disk or someone cracking a large digital music store)
 - Unlike a virtual market, there is no rollback

Normative comparison of © regimes

Regime

Aspect of Comparison

	<i>Status Quo</i>	<i>Anarchy</i>	<i>Strong DRM</i>	<i>Virtual Market</i>
<i>Artificial scarcity</i>	=	++\$3 billion/year (unlimited copying)	-- \$1 billion/year (piracy abolished)	++\$3 billion/year (unlimited copying)
<i>Incentives for production</i>	=	- -/--- (if you believe in cultural markets)	+\$10s of millions investment in cultural production /year	+ better than a naïve market
<i>Infrastructure + enforcement costs</i>	=	+ avoids “war on copying”	- up to a few \$100s of millions/year	+ avoids “war on copying”
<i>Transaction costs</i>	=	- (fundraising awkward)	+ strong DRM may facilitate some rights clearance	++ transaction costs minimised
<i>Taxation overheads</i>	=	=	=	-- up to \$200 million / year
Conclusion relative to status quo X	=	probably negative but depends on philosophy	negative in the \$100 millions/yr range	positive in the \$billions/year range

(Dollars in .au as a loose proxy for some more credible ethical measurement)

Conclusions

- There is a substantial case for at least experimenting with alternative compensation systems (*vive la France!*)
- Politically, this may require continued compromise of DRM systems and persistence of P2P networks
- However strong the case may be for music, it will only get stronger as digital books become more widespread

SONY

© 2003

SONY

LIBRIÉ

e-Book Reader
EBR-1000EP



BBEB

©2003 Sony Corporation

29
7/2

1 2 3 4 5 6 7 8 9 0
Q W E R T Y U I O P

A S D F G H J K L ; ' [] \ /

Z X C V B N M , . - _ = + * /

ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10

© 2003

LIBRIÉ