

TCB and DRM



Martin Häcker

“If we understood this
change, I believe we would
resist it.”

- Lawrence Lessig



“Free as in speech,
not free as in beer.”

- FSF



© 2005



What if DRM worked?

Some new business models?

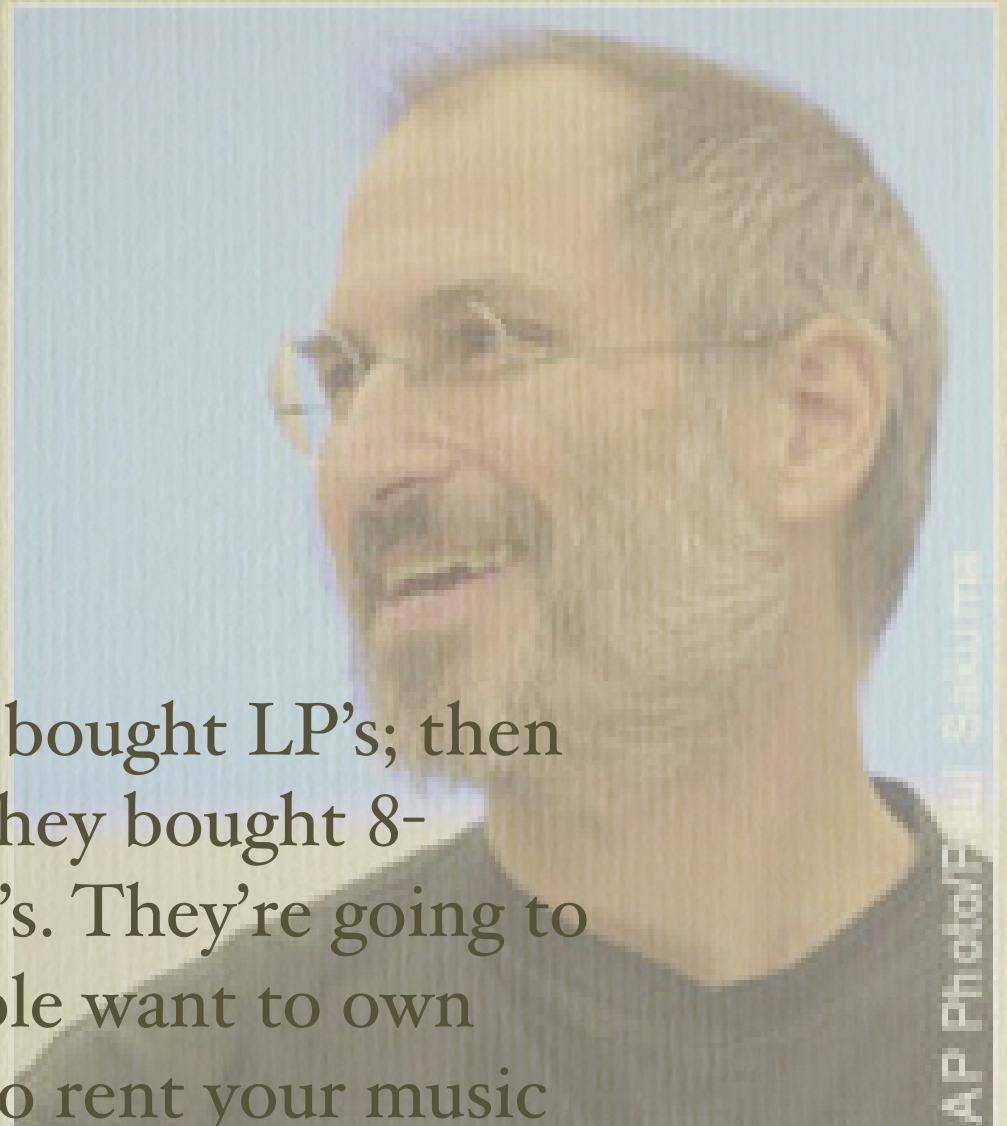
- Club /
Subscription
- Renting
Content
- Pay per view



but...

“They bought 45’s; then they bought LP’s; then they bought cassettes; then they bought 8-tracks; then they bought CD’s. They’re going to want to buy downloads. People want to own their music. You don’t want to rent your music -- and then, one day, if you stop paying, all your music goes away.”

- Steve Jobs, Rolling Stone interview



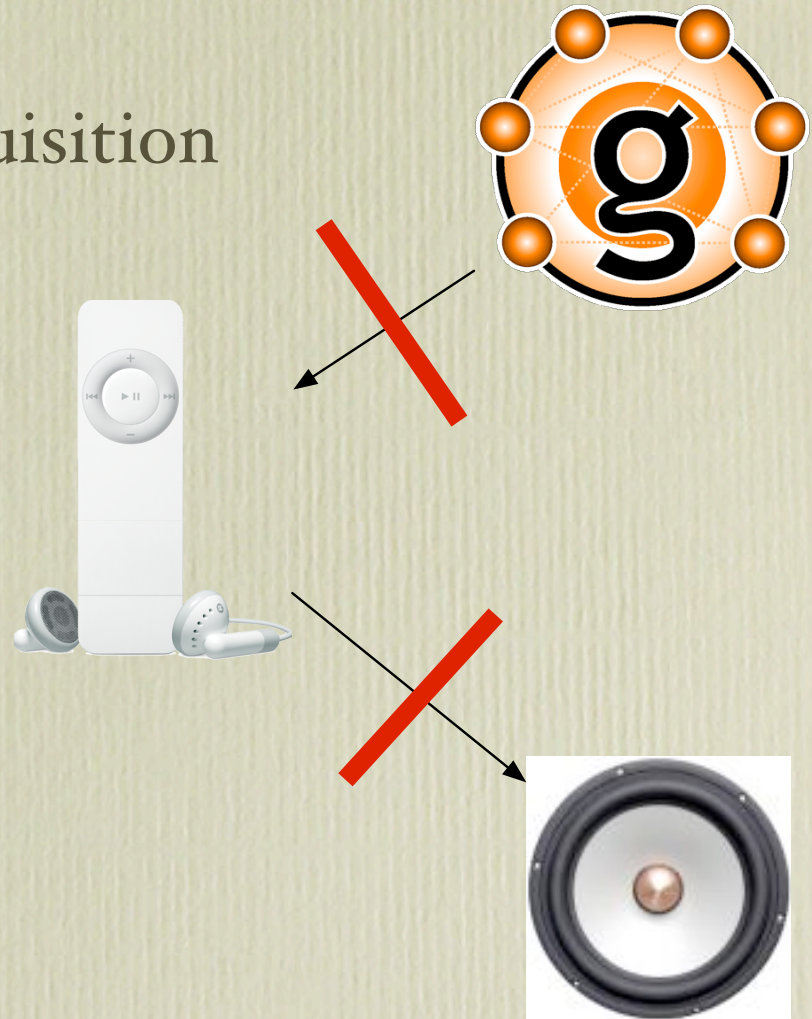
DRM though enables ...

- to control who creates
- to control markets



How does DRM work?

- Unauthorized use and acquisition
- Three approaches
 - Watermarking
 - Fuzzy hashing
 - Secure containers



Watermarking

- “Embedded” signal
- Protects against:
 - Unauthorized use
 - Unauthorized acquisition (somewhat)

Fuzzy Hashing

- The content becomes the hash
- Protects against:
 - Unauthorized use
 - Unauthorized acquisition (somewhat)

Hash Table(strings)	
0	(null)
1	(null)
2	(null)
3	"Steve"
4	(null)
5	(null)
6	(null)
7	(null)
8	(null)
9	(null)
10	(null)
11	(null)

Secure Containers

- Encrypting the content
- Protects against:
 - Unauthorized use only



“We claim [...] this would
have little effect on piracy.”

- S. Haber, B. Horne, J. Pato, T. Sander, R. E. Tarjan

managed vs. unmanaged
content

A green dragon with yellow horns and wings is breathing fire. A hot air balloon with a purple and white striped balloon and a white basket is floating in the sky. The background is a dark, stormy sky with a full moon and a large fire on the right side.

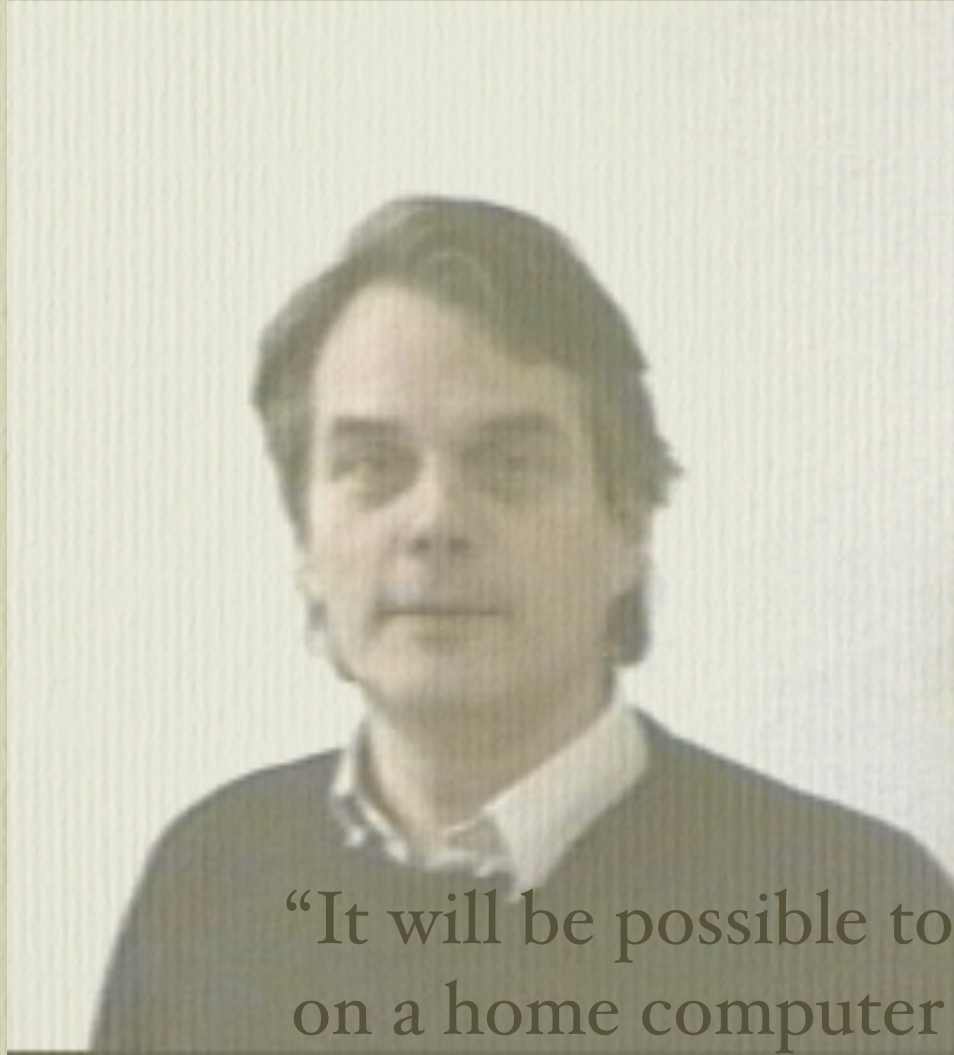
Draconian DRM to the rescue...

Some Problems

- New devices
- License authority
- Public content
- Private content

TOP
SECRET

XXX?

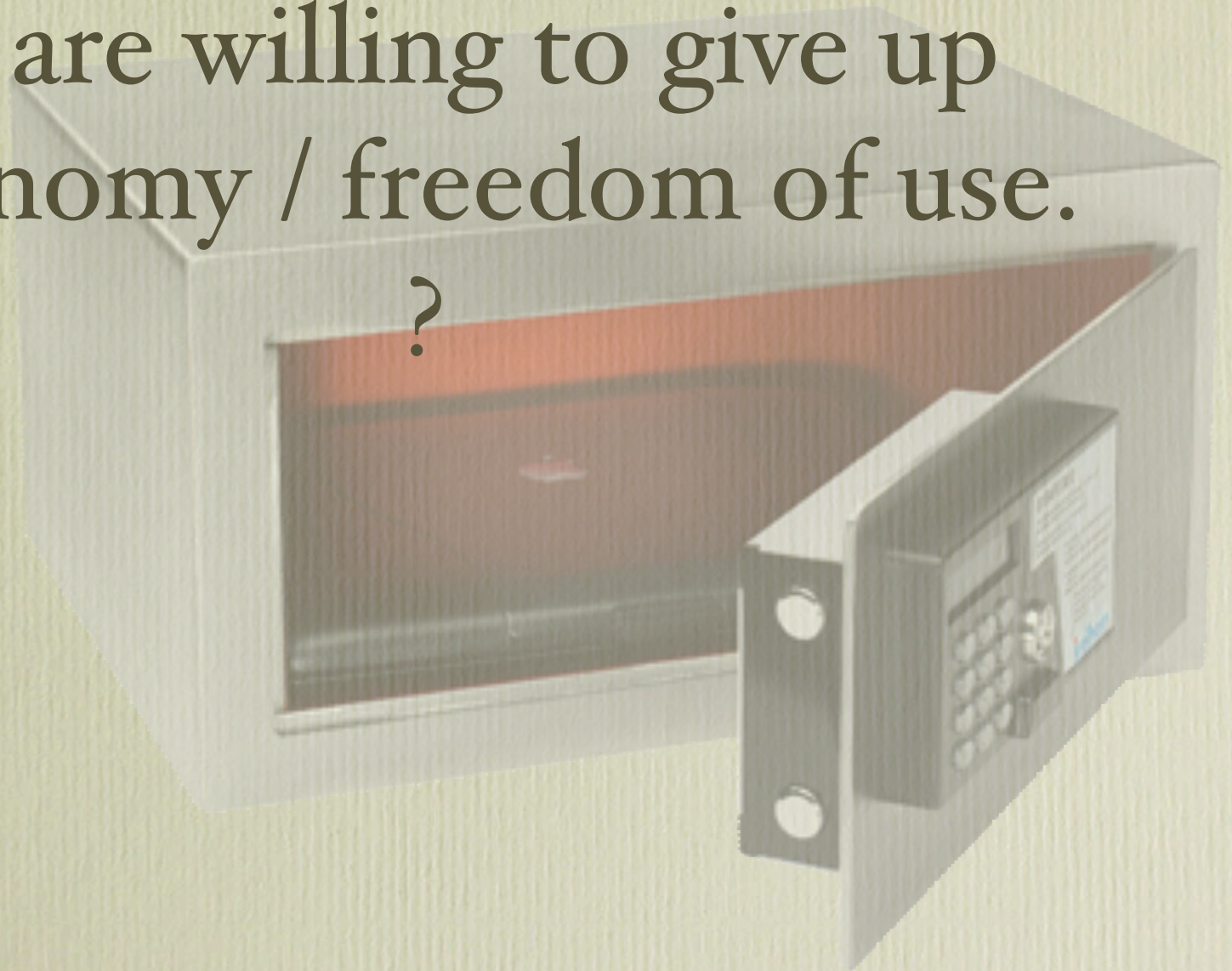


“It will be possible to compute arbitrary collisions on a home computer in one evening.”

- Prof. Dr. Ernst-Günther Giessmann (HU-Berlin)

Piracy could be managed if
we are willing to give up
autonomy / freedom of use.

?



Not Feasible:

- Technically
- Economically
- Socially





“... we would resist it!”
- Lessig

What could we do then?

Is competing possible?

- 40% of all software is pirated
- Solarium vs. self tanner vs. sunbathing
- Water bottlers vs. city waterworks



Here's how!

- Content management
- Content delivery
- Business models



Quelle: nbconsulting.de Int.



Quelle: perry-rhodan.net