

Cloud Media Lockers ...and Security

Vic Winkler
CTO

Covata USA, Inc
Reston, Virginia

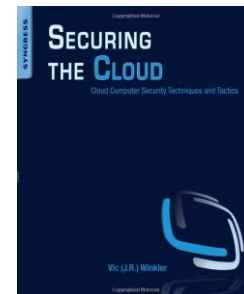
Covata
The product suite of
Cocoon Data Holdings Limited

COVATA

mini-bio

- Author

“Securing the Cloud: Cloud Computer Security Techniques and Tactics” May 2011 (Elsevier/Syngress)



- CTO

“Self-Defending Data” www.Covata.COM

Reston, VA | Sydney, Australia

COVATA™

- Published Researcher

Secure Operating System Design, Network Security Monitoring, Intrusion Detection, Information Warfare (PRC Inc., Northrup)

PRC, Inc.

- Security Design & Engineering

Sun Grid Compute Utility, Network.Com, The Sun Public Cloud (Sun Microsystems)

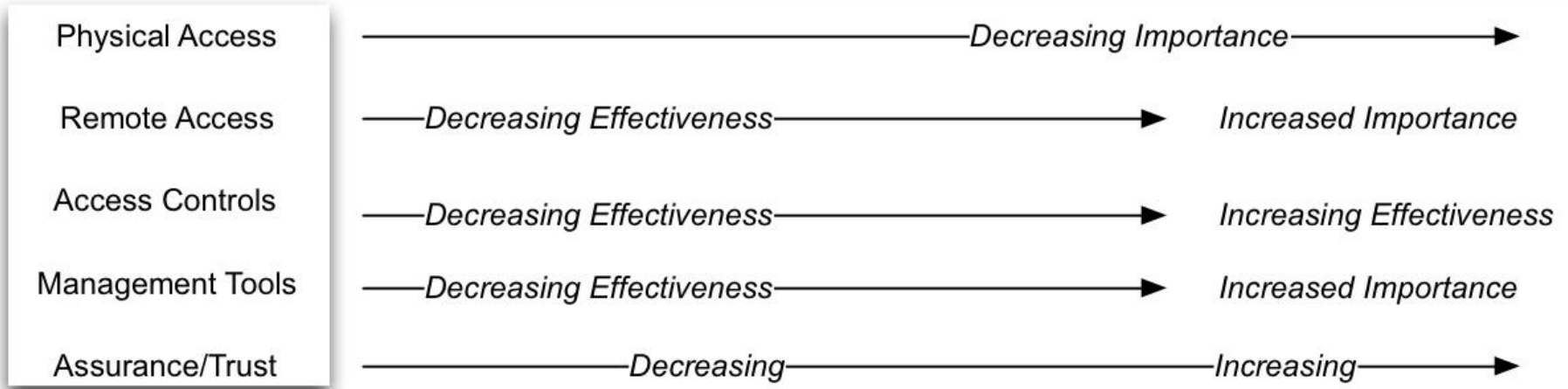
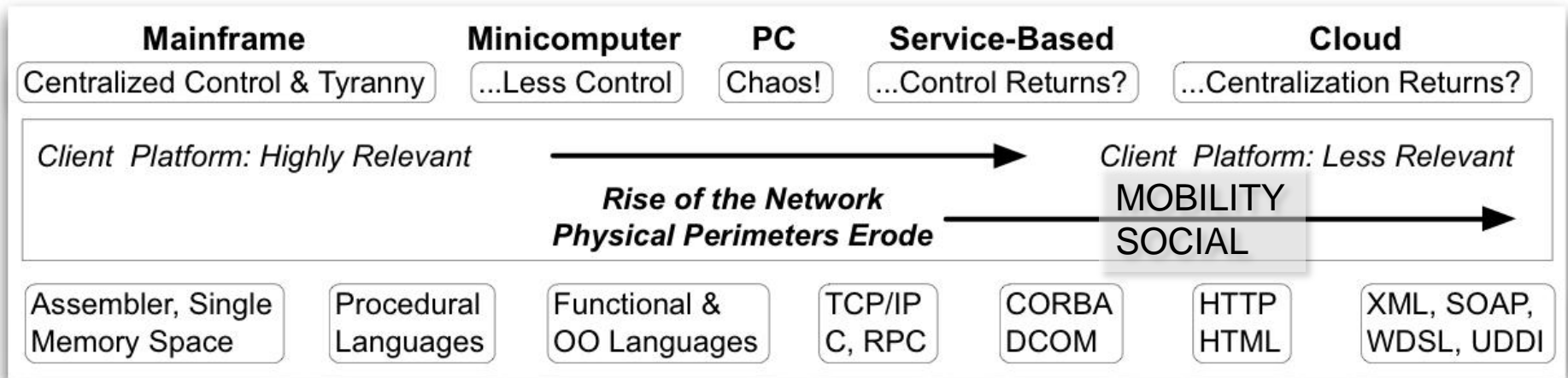


Government & Defense Customers (Booz Allen Hamilton, Sun Microsystems, PRC)

Booz | Allen | Hamilton

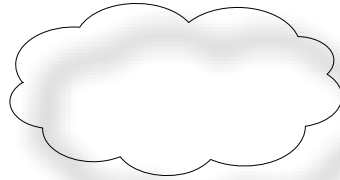
- email: Vic.Winkler@Covata.Com -or- Vic@VicWinkler.COM

A “Not-so” Accurate History of Things



3 Mega Trends

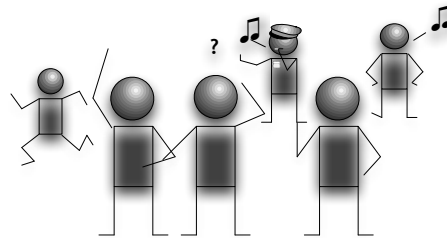
- Cloud



- Mobility



- Social



The Rise of the Cloud Media Locker

- Two major shifts in the consumption of digital media
 - Storage is moving from a local-only environment to a hosted one
 - Proliferation of network-connected devices has brought multiplatform access

Any discussion about Cloud Media Lockers would be incomplete without discussing the *Ultraviolet* standard:

Basically if you buy something on *Vudu*, it will be available on *VDIO* or other services.

That way the consumer is not locked into a single service, and always has access to purchased media. The UV license is now sometimes sold with DVD's.

(probing my extended network)

Vic

Cloud will shrink to the lowest cost/service denominator ultimately integrated with ISP backed services in exchange for one monthly annuity including bandwidth billed to your ISP. That means a slow but eventual consolidation for services like Dropbox that essentially replaced the old Napster/Kazaa P2P regime. In any event users don't really care where there media is located as long as its available.

Most piracy shifted to Cloud media lockers after the demise of P2P networks, but the improvement in monthly pay services like Rdio has made it increasingly more attractive for users to step up and pay.

The shift to cloud for any media is still governed by bandwidth reliability and availability. Countries, states or corporations rolling out fiber will change the game forever shifting media to the cloud and reducing the need for storage laden devices a death knell for the PC.

That makes personal and file security an increasingly important subject because cloud is being and will be hacked, its only a matter of time before a serious incident robs people of access to their valuable data. Events like these will bring people back to the days of DRM, but with significant improvements to browser security, products like Cocoon/Covata will be a different breed altogether, providing much improved control over asset distribution and tracking. This is important in the ever dangerous world of the unintended social network broadcast public persona - just look at SnapChat...

Hope this helps...

All the best

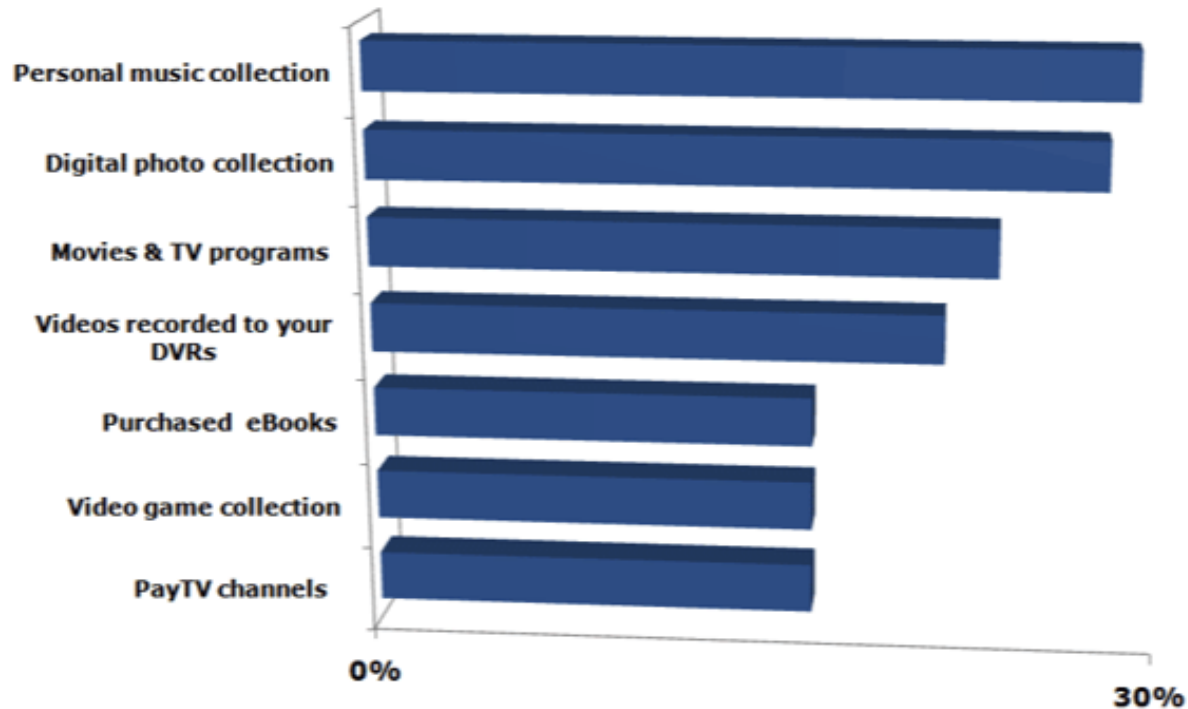
Kevin

Why Cloud Media Lockers ?

- **Cloud will shrink to the lowest cost/service denominator**
 - Integrated with ISP services
 - Single monthly annuity
 - One Bill
 - Piracy (P2P) → Pay !
- **From NAPSTER/Kazaa to a fully mainstream service**
 - User? Is my media available ?
- **Key ?**
 - Bandwidth & Availability





What do you Keep in a Cloud Media Locker?

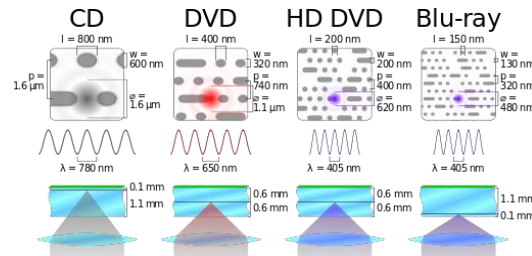
Appeal of Digital Locker
(U.S. Broadband Households)



Source: *Digital Media Evolution II*
© 2011 Parks Associates


136 Years of Content

<p>1951 IBM Punch Cards</p>  	<p>1960's Magnetic tape.</p> <p>(Ten reels of magnetic tape could contain as much data as a million punch cards)</p>	<p>1983 IBM PC/XT</p> <p>(Hard drive standard)</p> 	<p>2010's You no longer have to own and store copies of media when you purchase a license and stream the digital content</p> 
--	---	---	---



<p>1974 CD Up to 700 MB</p>  <p>1970's BETA VHS (up to 600 minutes)</p> 	<p>2000 Blu-ray</p> 
--	--

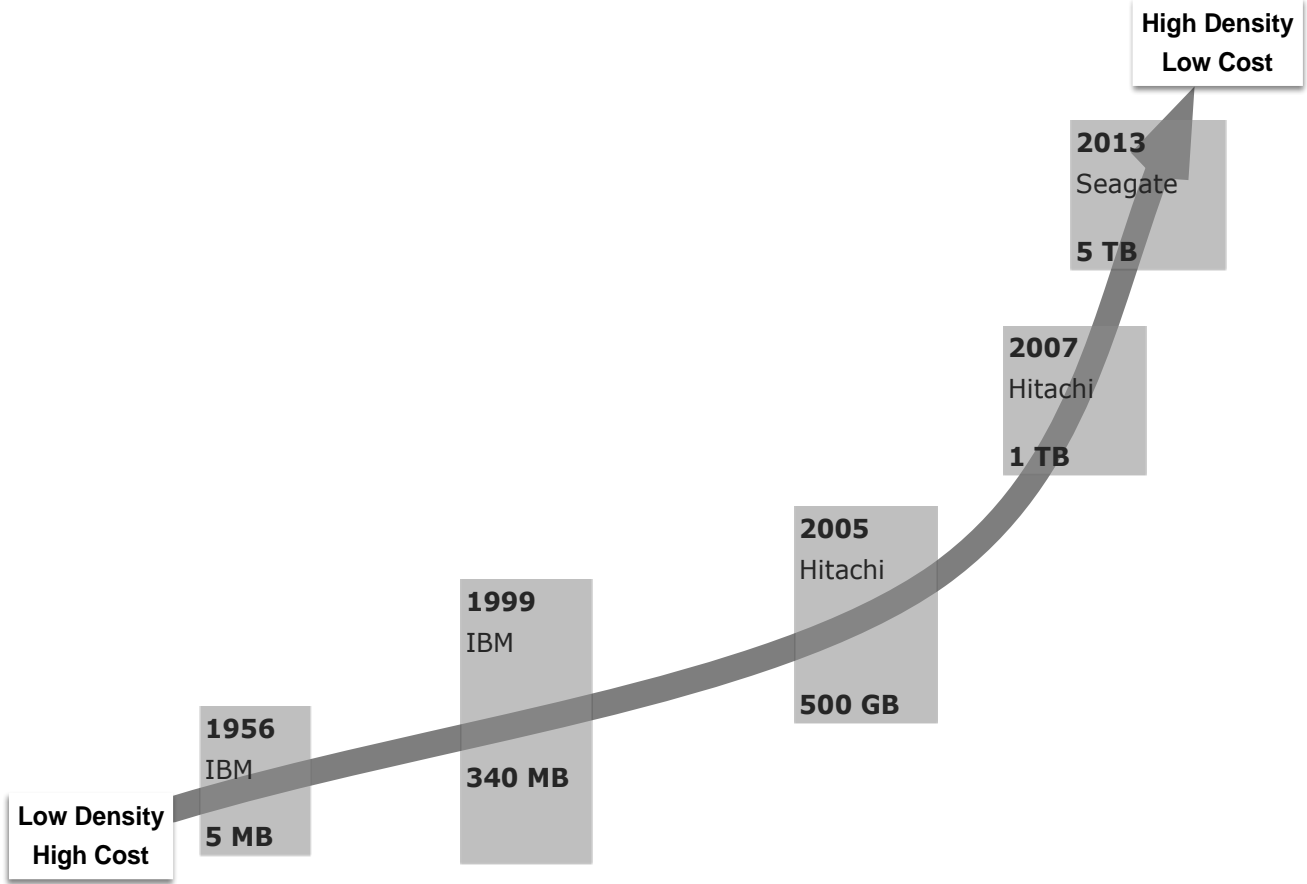
	
<p>Recording Devices Phonograph (1877 Edison) Motion Picture (1888 De Prince)</p>	


<p>1932: Kodak 8mm movie</p>

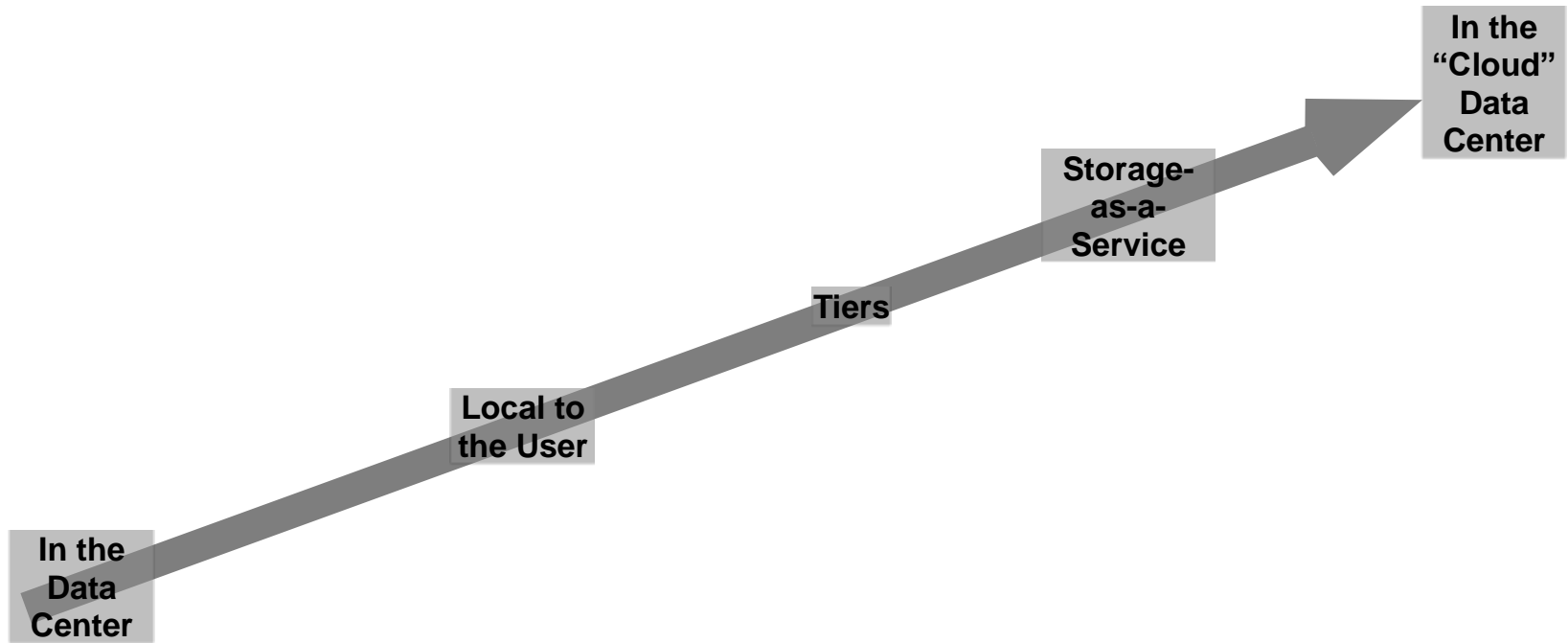

<p>1948: Kodak Special 16mm movie</p>

	
<p>1998 HDCAM "Digital Cinematography" 1980's Sony "Electronic Cinematography"</p>	

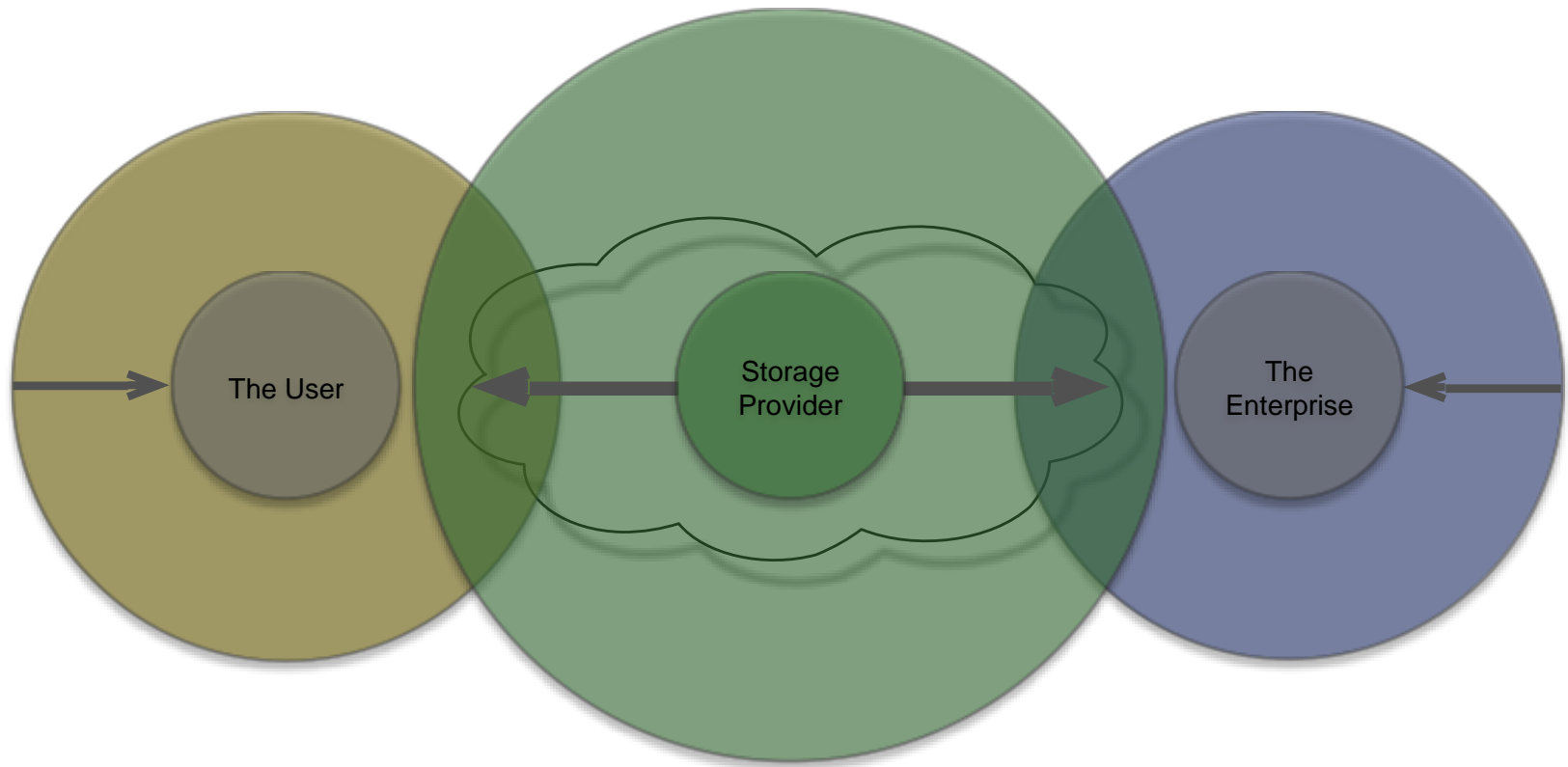
Units of Storage: The Disk Drive



“The Power of 2”: Storage Capacity & Network Bandwidth



Cloud-Based Storage ...is Where my Stuff is



Even “Desktop” Microsoft is Playing (everyone is headed here)

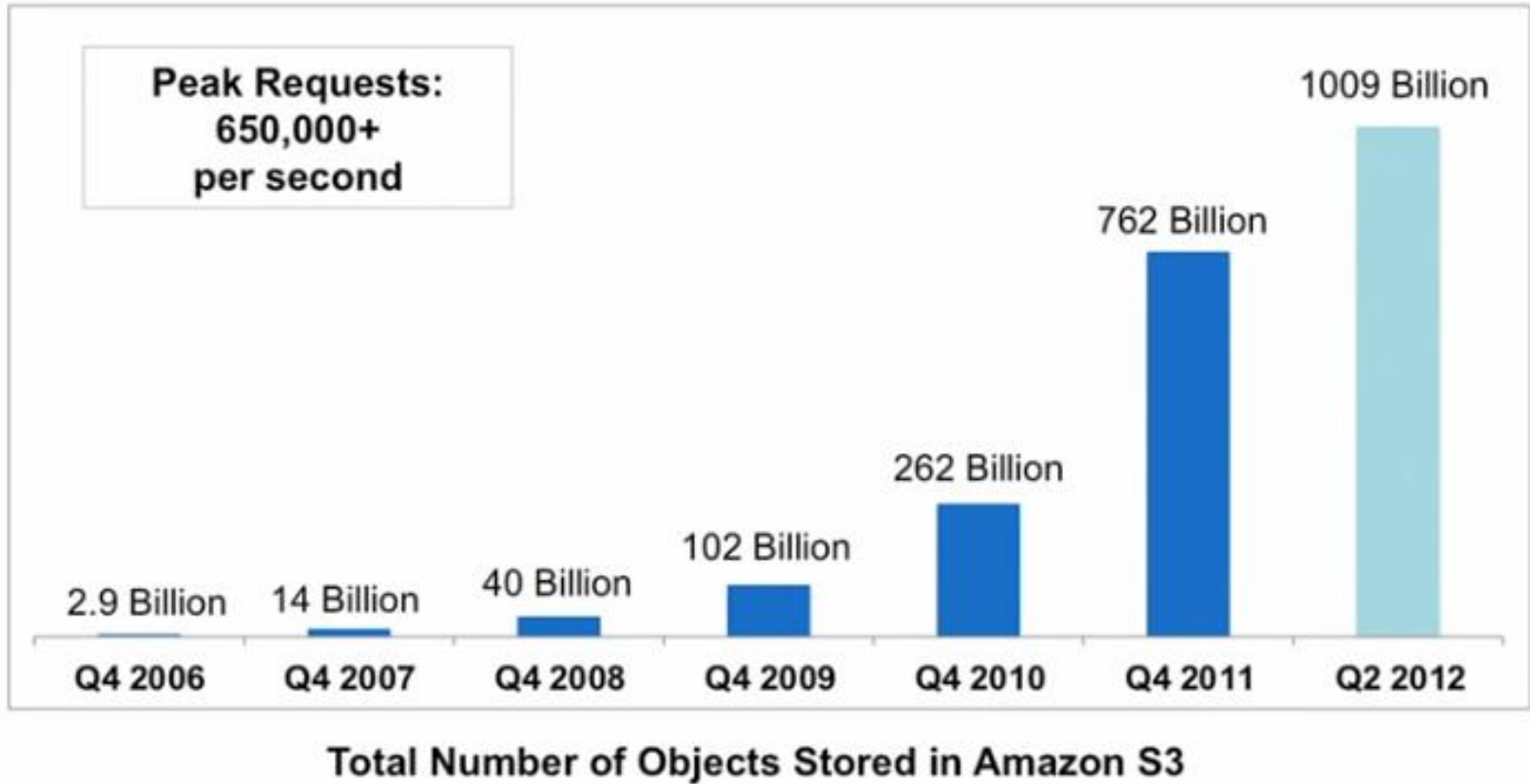
Storage, Backup, and Recovery

Gain peace of mind

Windows Azure provides scalable, durable cloud storage, backup, and recovery solutions for any data, big and small. It works with the infrastructure you already have to cost-effectively enhance your business continuity strategy as well as provide storage required by your cloud applications including unstructured text or binary data such as video, audio and images.

[Benefits](#) [Scenarios](#) [Get Started](#)

The 900 lb Gorilla



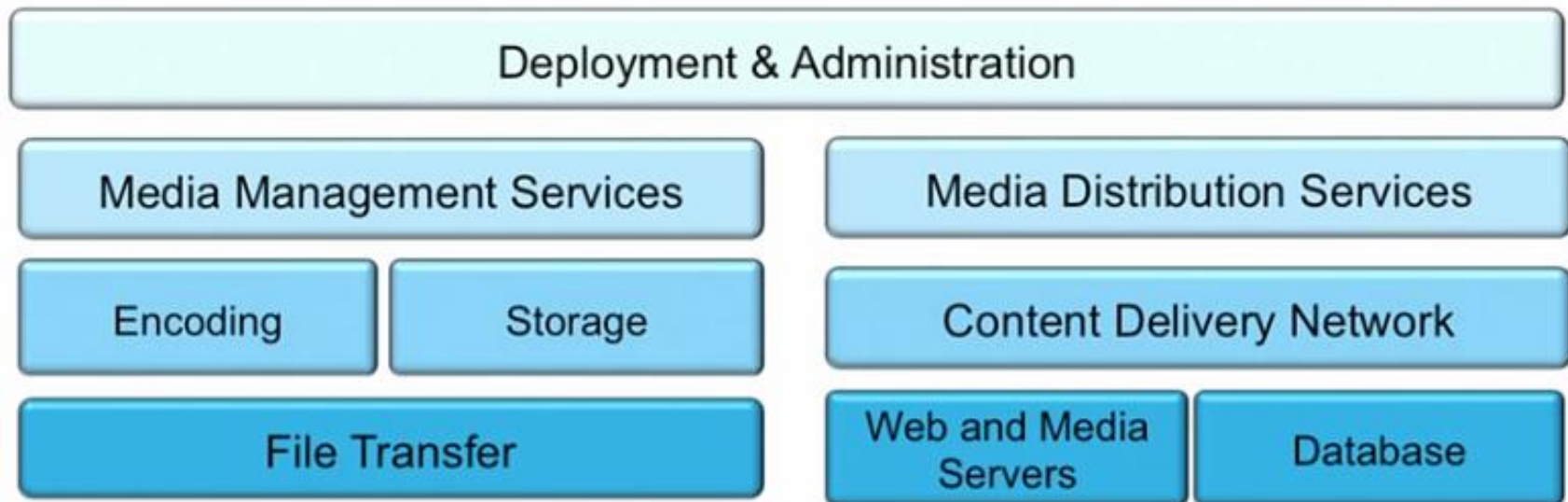
Amazon's Platform



AWS Media Platform Overview

Digital Asset Management

Media Distribution



Motivation for Data-Level Protection

- Devices and networks “hackable”

Meaning: You need to trust EVERYTHING in the data path!

- My Backup is on Your Email Server

Meaning: There are more copies of your data than you think!

- Full Disk Encryption vs. Data Level

Meaning: If I can hack your computer – I HAVE the key to your disk encryption

Question: Do You ACTUALLY Have Control Over Your Data?

- No access *without your permission*
- You specify *under what circumstances*
- Each attempted access is *audited*
- You can *revoke access anytime*
- ...*All copies act the same way*



How Can You Achieve That?



No. 9.

- Either:
 - Embed “self-defending” functionality into data (good luck), ...or
 - Add Information Rights Management (IRM)

- In brief, adding a form of IRM:
 - Extends traditional access controls with “*persistent controls*”
 - You “*shape*” them to meet your needs

- We can call this “*Originator Control*” (or ORCON)

Policy Enforcement & Caveats

Server-Side Enforcement

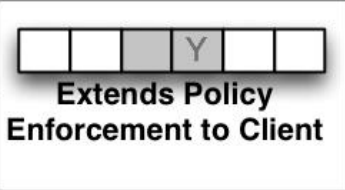
"ORCON Key-Granting Controls" extend identity-based access control mechanisms with additional rules that define specific conditions that must be met before a key is granted.



Examples: Geo-presence, time-constraints, device characteristics, etc.

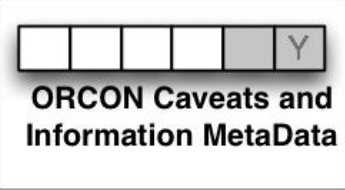
Client-Side Enforcement

"ORCON Usage Controls" serve to define specific usage modes that a client must be able to enforce.



These persist with data and enforce interaction limits (copy, edit,...) by a client.

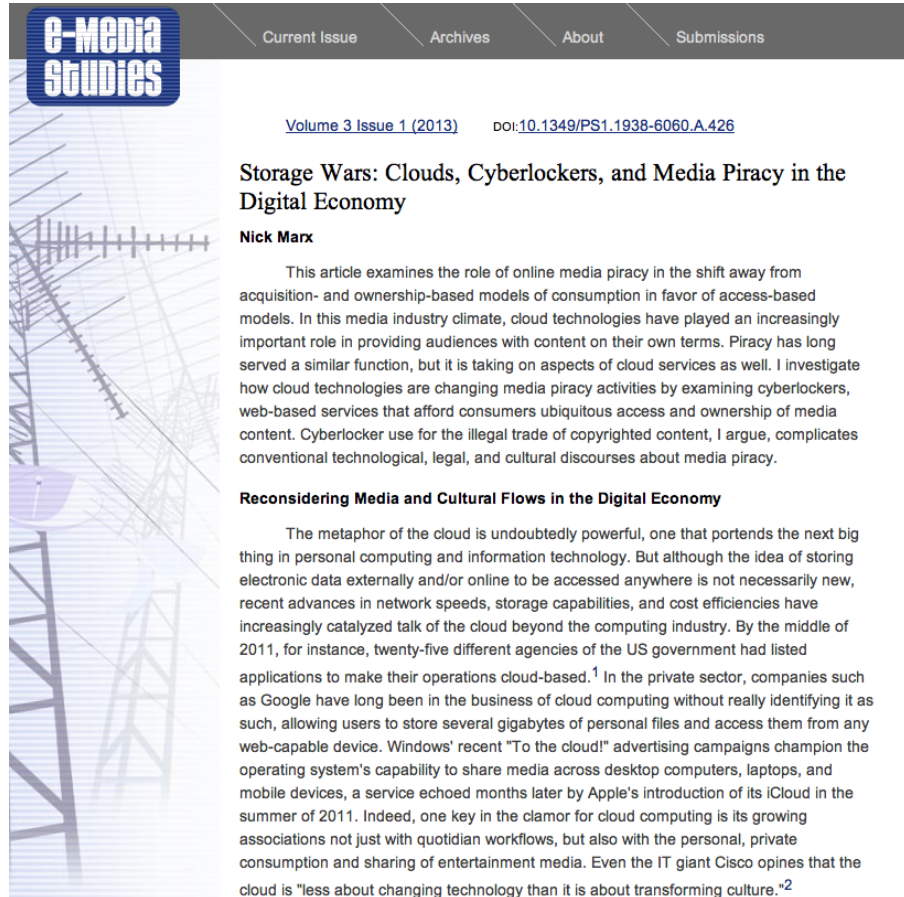
"ORCON MetaData" is used to visually mark information with caveats or labels that reflect its sensitivity and how it should be handled.



These can "emulate" "classification" metadata, or they can simply be sensitivity markings.

(why cloud media lockers?)

Why? You ask why? It's easy. Cost. Availability. Cool. I like cool. Evolution. Access ...I want it now. Privacy? Well, sure, but frankly I still want it now. You know, what happens in Vegas...



The screenshot shows the e-Media Studies journal website. The header includes the journal title and navigation links for Current Issue, Archives, About, and Submissions. The article information is as follows:

e-Media Studies
Current Issue Archives About Submissions

Volume 3 Issue 1 (2013) doi:10.1349/PS1.1938-6060.A.426

Storage Wars: Clouds, Cyberlockers, and Media Piracy in the Digital Economy

Nick Marx

This article examines the role of online media piracy in the shift away from acquisition- and ownership-based models of consumption in favor of access-based models. In this media industry climate, cloud technologies have played an increasingly important role in providing audiences with content on their own terms. Piracy has long served a similar function, but it is taking on aspects of cloud services as well. I investigate how cloud technologies are changing media piracy activities by examining cyberlockers, web-based services that afford consumers ubiquitous access and ownership of media content. Cyberlocker use for the illegal trade of copyrighted content, I argue, complicates conventional technological, legal, and cultural discourses about media piracy.

Reconsidering Media and Cultural Flows in the Digital Economy

The metaphor of the cloud is undoubtedly powerful, one that portends the next big thing in personal computing and information technology. But although the idea of storing electronic data externally and/or online to be accessed anywhere is not necessarily new, recent advances in network speeds, storage capabilities, and cost efficiencies have increasingly catalyzed talk of the cloud beyond the computing industry. By the middle of 2011, for instance, twenty-five different agencies of the US government had listed applications to make their operations cloud-based.¹ In the private sector, companies such as Google have long been in the business of cloud computing without really identifying it as such, allowing users to store several gigabytes of personal files and access them from any web-capable device. Windows' recent "To the cloud!" advertising campaigns champion the operating system's capability to share media across desktop computers, laptops, and mobile devices, a service echoed months later by Apple's introduction of its iCloud in the summer of 2011. Indeed, one key in the clamor for cloud computing is its growing associations not just with quotidian workflows, but also with the personal, private consumption and sharing of entertainment media. Even the IT giant Cisco opines that the cloud is "less about changing technology than it is about transforming culture."²

Thank You!

Vic.Winkler@Covata.Com

Vic@VicWinkler.com

On: Google+ & LinkedIn