

2001/9/3 Digigoods Outline

1 Meta

1.1 About this Document

The document is an excerpt from my book in progress, *Digital Needs*. This book has three major aspects: 1) It's a requirements document from the general consumer to the vendors of digital technologies. 2) It's an implementation document – it prescribes technical, commercial and legal components and infrastructures designed to satisfy the stated requirements. 3) It's a roadmap of how to build the stated solution, taking into account the economic and political desires of the various interest groups.

This document is a rough draft, in outline form, of the chapter focussing on digital goods. The three aspects of *Digital Needs* are evident here (4 +Requirements, 5 +Implementation and 6 Transition).

This is a rough draft – so don't be surprised by typos and editing errors. These will be corrected in a later version. My apologies for any confusion that editing errors may cause.

Be sure to read the Terminology, Status and Marks notes immediately below – they will help to clarify this document.

Note that of this date (10/3/2001), I am looking for funding for continued work on the book – please contact me at gratton@pobox.com if you are interested.

Pat Gratton, 10/3/2001

1.1.1 Terminology

- If you choose to skim, be sure to read 3.1 +Terminology first – crucial terms are defined here.

1.1.2 Status

- You can judge the progress of the document by checking the Pass Tasks for 'x' marks preceding tasks.
- As of this writing, Medium Completion is partially finished: Introduction, Requirements and Generalization have all been rewritten to the level required by that pass.
 - Note in particular that:
 - Many editing errors still exist in the cleared sections – these will be corrected in a later pass.
 - Transition and Summary are still in rough draft (with many redundancies and missing pieces).

1.1.3 Marks

- 'x' in front of a task in the Pass Tasks section indicates that task has been completed.
- '+' in front of a section in the document means that section has been rewritten to level required by the current pass.
 - These marks are cleared at the beginning of each pass.
 - Note that due to way references are handled, the '+' marks also show up in reference links. (E.g. "See 4.2.1 +Access Purchase.")
- '??' marks indicate missing text.

1.2 Daily Tasks

- Reindex
- Save version.
- Backup
- ? Print out
 - Switch off online mode and reindex.
 - Print

1.3 Pass Tasks

1.3.1 Global Corrections

@ Goals

- Define and use a standard language for introducing new implementation aspects. (Something like: "already mentioned... in addition...", or maybe [NEW] or [ADD])

1.3.2 Medium Completion

@ Goals

- Structure should be 98% fixed.
- Discover and fill in major gaps in thinking
- Eliminate all ?? markers.
- All points should be present
- Most supporting and elaborating statements should be present.

x High Level Changes

- x Define references, then change text to use defined references.
 - x Use "See Chapter ?? Bob" for chapter references
- x Rationalize cognigood, cognifact, digigood, digifact usage.
- x Add Generalization section
- x Add cogniprop, digiprop, copygood terminology
- x Redefine references to include text, then use adjusted references
- x Add version information to page footers.
- x Notes for Reviewers

x Introduction

- x Terminology
- x Blocking the Digital Revolution
- x This Chapter

x Requirements

- x Fundamentals
- x Access Rights
- x Library Access
- x Distribution
- x Availability
- x Coexistence

- x Protection
- x Consumer Representation
- x Implementation
 - x Commercial Infrastructure
 - x Technical Components
 - x Legal Infrastructure
 - x Fundamental Requirements
 - x Access Rights
 - x Library Access
 - x Distribution
 - x Availability
 - x Coexistence
 - x Protection
 - x Consumer Representation
- Transition
 - Infrastructure Issues
 - Technical Issues
 - Legal Issues
 - Stakeholder Issues
- x Generalization
 - Summary

1.3.3 Research Inclusion

- @ Goal: Include previous research
- Compare against IT News notes.
- Compare against old papers.
 - x Old journal entries.
 - Digital Needs notes and papers
 - ! Note: I've already done one pass of this.
 - Fixstreams and varstreams.

1.3.4 Brainstorming

- @ Goal: Final attempt to see if I've missed anything substantial.
 - Print out one topic per page and brainstorm.
 - List ideas and questions for each topic
- Introduction
- Requirements
- Implementation
- Transition
- Summary

1.3.5 Fine Completion

- @ Goals

- Fine check and completion after incorporating research and brainstorming
- Structure should be 99% fixed.
- All points should be present
- All supporting and elaborating statements should be present.
- Introduction
- Requirements
- Implementation
- Transition
- Summary

1.3.6 Paragraph Formation

@ Goal: Reorganize outline into paragraphs

- Mark paragraphs
- Mark supporting statements
- Introduction
- Requirements
- Implementation
- Transition
- Summary

1.3.7 Paragraph Checking

@ Check paragraph arrangement, flow

- Print new page with each topic and check:
 - Does paragraph to paragraph argument make sense?
 - Do paragraphs flow well?
- Introduction
- Requirements
- Implementation
- Transition
- Summary

1.3.8 Statement Checking

@ Check internal paragraph flow

- Print new page with each topic and check:
 - Internal argument and flow of each paragraph.
- Introduction
- Requirements
- Implementation
- Transition
- Summary

1.3.9 Outline Conversion

@ Goal: Convert outline to text.

- Save as new file and begin conversion
- Introduction
- Requirements
- Implementation
- Transition
- Summary

2 Contents

1 Meta.....1

1.1 About this Document.....1

 1.1.1 Terminology.....1

 1.1.2 Status.....1

 1.1.3 Marks.....1

1.2 Daily Tasks.....2

1.3 Pass Tasks.....2

 1.3.1 Global Corrections.....2

 1.3.2 Medium Completion.....2

 1.3.3 Research Inclusion.....3

 1.3.4 Brainstorming.....3

 1.3.5 Fine Completion.....3

 1.3.6 Paragraph Formation.....4

 1.3.7 Paragraph Checking.....4

 1.3.8 Statement Checking.....4

 1.3.9 Outline Conversion.....4

2 Contents.....6

3 +Introduction.....11

3.1 +Terminology.....11

3.2 +Blocking the Digital Revolution.....11

 3.2.1 +Digital Promise.....11

 3.2.2 +Inapplicability of Copyright.....11

 3.2.3 +Complexity.....12

 3.2.4 +Revolution is Required.....12

 3.2.5 +Companies Resist Revolution.....12

 3.2.6 +Legal System Resists Evolution.....13

 3.2.7 +Government Resists Revolution.....13

 3.2.8 +Consumers are Missing from Bargaining Table.....13

3.3 +This Chapter.....13

4 +Requirements.....15

4.1 +Fundamentals.....15

 4.1.1 +Benefit to Public.....15

 4.1.2 +Advantages of Digital World.....15

 4.1.3 +Simplicity.....15

 4.1.4 +Durability.....16

 4.1.5 +Progress.....16

4.2 +Access Rights.....16

 4.2.1 +Access Purchase.....16

 4.2.2 +Access Rental.....17

 4.2.3 +Simuluse Rights.....17

 4.2.4 +Limited Editions.....18

4.2.5 +Group Access.....	18
4.2.6 +Transfer.....	19
4.2.7 +Machine Associated Access.....	20
4.2.8 +Preview.....	20
4.2.9 +Printing.....	20
4.2.10 +Public Use Rights.....	21
4.2.11 +Dis-aggregation.....	21
4.2.12 +Derivation.....	22
4.2.13 +Annotation.....	22
4.2.14 +Composition by Reference.....	22
4.3 +Library Access.....	23
4.3.1 +Library Access.....	23
4.3.2 +Advertising Supported Access.....	24
4.4 +Distribution.....	25
4.4.1 +Distribution.....	25
4.4.2 +Portability.....	25
4.4.3 +Disconnected Functioning.....	26
4.4.4 +Caching Efficiency.....	26
4.4.5 +Reduced Cost of Entry for Creators.....	26
4.5 +Availability.....	26
4.5.1 +Publication.....	26
4.5.2 +Term Limits.....	27
4.5.3 +Deposit.....	27
4.5.4 +Permanence.....	27
4.5.5 +Updates.....	27
4.5.6 +Platform Emulation.....	28
4.5.7 +Free Access Digifacts.....	28
4.5.8 +Indexing and Searching.....	28
4.5.9 +Research.....	29
4.6 +Coexistence.....	29
4.6.1 +Copygood Conversion.....	29
4.6.2 +Digigood Printout.....	30
4.7 +Protection.....	30
4.7.1 +Access Control.....	30
4.7.2 +Infrastructure Protection.....	30
4.7.3 +Privacy Protection.....	31
4.8 +Consumer Representation.....	31
4.8.1 +Consumer Representation.....	31
5 +Implementation.....	32
5.1 +Commercial Infrastructure.....	32
5.1.1 +Access Vendors and Digifact Distributors.....	32
5.1.2 +AVDS Roles.....	32
5.1.3 +Typical Transactions.....	33

5.1.4 +Digigood Owner.....	34
5.1.5 +Digigood Registrar.....	34
5.1.6 +Digigood Certifier.....	34
5.1.7 +Re-Use Vendor.....	35
5.1.8 +Access Registrar.....	35
5.1.9 +Access Vendor.....	36
5.1.10 +Library Access Vendor.....	36
5.1.11 +Digistore.....	36
5.1.12 +Consumer.....	37
5.2 +Technical Components.....	38
5.2.1 +Digifact References.....	38
5.2.2 +Encryption.....	39
5.2.3 +Watermarking.....	39
5.2.4 +Identification.....	39
5.2.5 +Trusted Platform.....	40
5.2.6 +Simuluse Manager.....	40
5.3 +Legal Infrastructure.....	40
5.3.1 +Superseding Copyright Law.....	40
5.3.2 +Standard Consumer Contracts.....	41
5.4 +Fundamentals.....	41
5.4.1 +Benefit to Public.....	41
5.4.2 +Advantages of the Digital World.....	41
5.4.3 +Simplicity.....	42
5.4.4 +Durability.....	42
5.4.5 +Progress.....	43
5.5 +Access Rights.....	43
5.5.1 +Access Purchase and Rental.....	43
5.5.2 +Simuluse Rights.....	43
5.5.3 +Limited Editions.....	43
5.5.4 +Group Access.....	44
5.5.5 +Transfer.....	45
5.5.6 +Machine Associated Access.....	45
5.5.7 +Preview.....	45
5.5.8 +Printing.....	46
5.5.9 +Public Use Rights.....	47
5.5.10 +Dis-aggregation.....	47
5.5.11 +Derivation.....	47
5.5.12 +Annotation.....	47
5.5.13 +Composition by Reference.....	47
5.6 +Library Access.....	48
5.6.1 +Library Access.....	48
5.6.2 +Advertising Supported Access.....	49
5.7 +Distribution.....	49

5.7.1 +Distribution.....	49
5.7.2 +Portability.....	50
5.7.3 +Disconnected Functioning.....	50
5.7.4 +Caching Efficiency.....	50
5.7.5 +Reduced Cost of Entry for Creators.....	50
5.8 +Availability.....	50
5.8.1 +Publication.....	50
5.8.2 +Term Limits.....	51
5.8.3 +Deposit.....	51
5.8.4 +Permanence.....	51
5.8.5 +Updates.....	52
5.8.6 +Platform Emulation.....	53
5.8.7 +Free Access Digifacts.....	54
5.8.8 +Indexing and Searching.....	55
5.8.9 +Research.....	55
5.9 +Coexistence.....	55
5.9.1 +Copygood Conversion.....	55
5.9.2 +Digigood Printout.....	58
5.10 +Protection.....	58
5.10.1 +Access Control.....	58
5.10.2 +Infrastructure Protection.....	60
5.10.3 +Privacy Protection.....	62
5.11 +Consumer Representation.....	65
5.11.1 +Consumer Representation.....	65
6 Transition.....	66
6.1 Infrastructure Issues.....	66
6.1.1 Digigood Registrar Service.....	66
6.1.2 Access Registrar Service.....	66
6.1.3 Access Vendor Service.....	66
6.1.4 Digistore Service.....	66
6.2 Technical Issues.....	66
6.2.1 Reference Format.....	66
6.2.2 Encryption.....	67
6.2.3 Encryption Schemes.....	68
6.2.4 Encryption Approaches.....	68
6.2.5 Identification and Public Key Infrastructure.....	69
6.2.6 Trusted Platforms.....	69
6.2.7 Consumer Software.....	71
6.3 Legal Issues.....	71
6.3.1 Copyright Law.....	71
6.3.2 Publication.....	71
6.3.3 Moral Rights.....	72
6.3.4 Other.....	72

6.4 Stakeholder Issues.....	72
6.4.1 Consumers.....	72
6.4.2 Advertisers.....	72
6.4.3 Decline of Advertising?.....	72
6.4.4 Book Industry.....	73
6.4.5 Copyright Office and Library of Congress.....	74
6.4.6 Music Industry.....	74
6.4.7 Audio Broadcast.....	75
6.4.8 Advertising Supported Internet.....	76
6.4.9 Video.....	76
6.4.10 Video: Mixed Advertising and Digistore Model.....	77
6.4.11 Collection Agencies.....	78
6.4.12 Software Publishers.....	78
6.4.13 Libraries.....	78
6.4.14 Public Libraries.....	78
6.4.15 Corporate and Organizational Libraries.....	79
6.4.16 Free Access Digigood Providers.....	79
6.4.17 Privacy Advocates.....	79
6.4.18 Free Information Advocates.....	80
6.4.19 Lawyers.....	80
7 +Generalization.....	81
7.0.1 +Property Generalization.....	81
7.0.2 +Digifact Generalization.....	81
8 Summary.....	82
8.0.1 Requirements.....	82
8.0.2 Action.....	82

3 +Introduction

@ This chapter is concerned with technical, commercial and legal infrastructure for distribution of digital goods.

@ Digital technology as revolution in distribution of cognigoods.

3.1 +Terminology

@ Some new terminology is useful.

- Cognifact (cognitive artifact): an item of "information", e.g., book, picture, theory, phrase, etc.
- Cogniprop: an owned cognifact
- Cognigood: a cogniprop to which access may be sold
- Cognistriction: restriction on distribution or use of a cognifact

- Digifact (digital artifact): an digital item of information
- Digiprop: an owned digifact
- Digigood: a digiprop to which access may be sold
- Digistriction: restriction on distribution or use of a digifact

- Copygood: a physical representation of a cognigood, protected by copyright law

3.2 +Blocking the Digital Revolution

@ Digital technology promises greatly improved access to and use of cognigoods. However, because this revolution in capability requires a corresponding revolution in technical, commercial and legal infrastructure, and because this revolution in infrastructure has yet to happen, the promise is not being fulfilled.

3.2.1 +Digital Promise

@ Digital technology promises many improvements in distribution of cognigoods.

- Lower cost (Zero copying cost)
- Immediate distribution (e.g., customer wants, customer gets immediately over the network)
- Production on demand (vs. runs of X number of copies of books)
- Portability across devices
- Low bulk (which continues to decrease with improving technology)
- Searchability
- Hyperlinks and annotation
- Backup makes impervious to physical damage

3.2.2 +Inapplicability of Copyright

@ But Copyright law is poorly adapted to digigoods.

- Based on physical limitations of copygoods.
- Vs. computer world, where copying is fundamental to access.

3.2.3 +Complexity

@ And both copyright and cognigood contract law are so complex that they hinder the digigood market.

- Of copyright law.
 - Basic copyright: reproduction, distribution, etc.
 - Varies somewhat by categories
 - Collision of different types in digital world
 - First sale
 - Can't rent CDs (though you can resell them)
 - Can't rent software
 - Can't charge admittance for viewing of a videotape or DVD.
 - Fair use
 - Various special case provisions for libraries, dance halls, etc.
 - General public today is likely to be a copyright holder, so there is a need to remove complexity for authors as well as for consumers.
 - Both IP & NII and Digital Dilemma books recommend education.
- Of contract law.
 - Shrink-wrap licenses are complex and non-standard.
 - Terms vary from vendor to vendor, product to product.
 - Terms vary over time.
 - Terms include overly restrictive clauses.
 - Is not even read by consumer.

3.2.4 +Revolution is Required

@ A revolution in technical, commercial and legal cognigood infrastructure is required in order to deliver the advantages promised by digital technology.

- To handle radical change implied by radical, revolutionary technology.
 - To provide a single solution that applies across all forms of cognigoods (text, audio, video, software, etc.)
- To replace fundamental assumptions of "copyright"
- To implement a new, simple deal. (Simple for both consumers and creators.)

3.2.5 +Companies Resist Revolution

@ But current commercial infrastructure resists revolution.

- IP companies are doing business as usual. (Bring a product out and see if public goes for it.) But digigoods require a fundamental re-negotiation of deal with consumers. This re-negotiation should be explicit, public and well advertised. Consumers need to feel that they're part of the process.
 - Don't make sufficient mention of basic plans, long term deals.
 - In particular, there doesn't seem to be something equivalent to purchase once, use forever.
 - Don't take sufficient advantage of digital domain – tend to try to turn digigoods into copygoods.
 - Lack of consumer confidence in them (here today, gone tomorrow).
- Vested business models – change is expensive and uncertain.
- Moreover, change generally results in decreased income for businesses.
- Digital change threatens to dis-empower existing middlemen (book and music publishers). These

interests are likely to fight to maintain their market dominance.

- Vested interests hold libraries of products which they can leverage to gain benefits in the digital age.
- Current cognigood industry is built around the practicalities of distribution of copygoods. Thus we can expect the desires of the industries behind this to be leery of digigoods.

3.2.6 +Legal System Resists Evolution

@ And the cognigood related legal system resists revolution.

- Common law is innately ill-suited to handling revolutionary technologies.
- Legislative process for modification to copyright law has essentially only had to deal with extensions of copyright law – e.g., copyright applied to movies, to recorded music performances (records), to broadcast, etc.
- But digital technology isn't just an extending technology, but rather a revolutionary technology – one that promises/threatens to completely change or replace all existing channels of distributing cognigoods.
- Likewise, much of copyright law is tied around notion of control of copygoods. Thus, it too will stand in the way of radical revision.

3.2.7 +Government Resists Revolution

@ The government resists changes required in order to implement digigood technology.

- Will require high quality encryption – that will require approval of government. And if key escrow is to be used, that will require approval by consumers.

3.2.8 +Consumers are Missing from Bargaining Table

@ And even consumers, through their absence from the bargaining table, are blocking the digigood revolution.

- Negotiation will be required, but there isn't a good representative for consumers to sit at the bargaining table.
 - Note that change will most likely proceed through contract law (more flexible than copyright law), but is also vastly more subject to the leverage of existing power holders. Until consumers are able to aggregate their buying power into an organization capable of sitting at the negotiating table, they will not be able to exert the leverage that they need to exert – especially over digigood contracts.
- Without representation, consumers will be wary and resentful of radical new changes.
 - Some infrastructure changes will threaten privacy – such changes will require the presence of consumers at the negotiating table.
- Consumer wariness of new technology will decrease sales, and thus delay rollout of those technologies.

3.3 +This Chapter

@ Requirements, Implementation, Issues, Summary.

- Requirements takes the problems and opportunities stated above, restates them in more detail and expands on them a lot. It attempts to state consumer requirements at fair length, while keeping implications and limitations of digital domain in mind as well as the countering demands of cognigood

- producers.
- Implementation describes an implementation designed to meet the requirements. When necessary, it describes how it meets the requirements.
 - Technical, Legal, and Stakeholder Issue sections consider implications, concerns and likely reactions to the implementation.
 - Summary revisits the high points of chapter, especially the requirements and the actions required to achieve the implementation.

4 +Requirements

@ Handling digigoods requires a new technical, commercial and legal infrastructure. Here's what we, as consumers, should demand of that infrastructure.

4.1 +Fundamentals

@ Here are the fundamental (abstract) requirements for the digigood infrastructure.

- Fundamental, in sense that they're not met by specific features of the solution, but by overall nature of it.
- Fundamental, in sense that they drive other, more specific, requirements.

@ Implementation is presented in 5.4 +Fundamentals.

4.1.1 +Benefit to Public

@ [Constitution quote] This states goals quite well.

- Basically, guarantee of financial remuneration is provided to motivate authors to create cognigoods for public.
- Encourage wide distribution of cognigoods:
 - Release to general public for a reasonable fee in the near term
 - First sale allows storage in libraries where cognigood may be obtained by loan.
 - Eventual full and free release to the public.

4.1.2 +Advantages of Digital World

@ Advantages of digital world should be present in digigood infrastructure.

- As stated above:
 - Lower cost (Zero copying cost)
 - Immediate distribution (e.g., customer wants, customer gets immediately over the network)
 - Production on demand (vs. runs of X number of copies of books)
 - Portability across devices
 - Low bulk (which continues to decrease with improving technology)
 - Searchability
 - Hyperlinks and annotation
 - Backup makes impervious to physical damage

4.1.3 +Simplicity

@ Digigood deal and infrastructure should be easy to understand.

- Should be possible to state the basic deal within one paragraph – and preferably one sentence.
- Contrary to earlier reports, the solution is not education, but simplicity.

@ Wide application. Same rules should apply to all digifacts (text, audio, video, resources, software).

@ Technical infrastructure should be transparent 99% of time, and extremely easy to use for the 1% of the time that it is visible.

@ Simplicity – agreement covering any digigood ought to be comprehensible through a few checkboxes, icons, etc.

- Small standard dialog box should indicate all relevant information about the license for any digifact.

- Underlying contract should be absolutely standardized.

4.1.4 +Durability

- @ Digigood infrastructure should be flexible to accommodate short term technical changes, and durable enough to withstand long-term use as digital distribution of data becomes the dominant (and possibly only) method of distribution of cognigoods.
- Expect digital distribution to be the norm in the future – thus the distribution system should be centered around it's assumptions rather than created as an extension to the copygood system. Before too long and for millennia after that, the notion of tying up IP in the assumptions of their physical embodiments will seem quaint and antique – just as the notion that success in trade depending on having good navigable waterways now seems quaint to us.
- Technical details and capabilities are likely to fluctuate for quite a while – we should have good general principles which would allow us to traverse these fluctuations without to too much difficulty.

4.1.5 +Progress

- @ Consumers should gain from deployment of digigood infrastructure.
- However, it's acknowledged that some losses may be necessary – specifically to first sale principle – see below.)
- Creators should benefit as well – this is expected to be a win-win situation for these two groups.
- However, companies built on the assumption of copygoods are likely to lose profit margins and market share.
- In particular, consumers should see reasonable pricing. Digital technology drastically reduces many of the costs associated with publishing. Those advantages should be passed along to the consumer.

4.2 +Access Rights

- @ This section begins by considering the purchase or rental of access rights by an individual, and then considers various extensions to this basic access transaction.
- @ Implementation is presented in 5.5 +Access Rights.

4.2.1 +Access Purchase

- @ Consumers should be able to buy permanent access rights to a digigood.
- This provides a direct comparison to the current situation, where most cognigoods are bought and (potentially at least) held permanently by the consumer.
- User can follow a simple rule, "If it's only myself accessing the digigood – then I have the right to do so."
- @ Versus other approaches
- vs. current system based on copy control
- copy control counter to fundamental nature of digital world, where access is copying.
- vs. machine specific access
- access rights would disappear with machine
- theft, damage or obsolescence of machine would result in loss of digital access rights associated with it.

- not portable – abandonment of one of great advantages of digital world, which is the independence of a digifact from any particular copy of it.
- This is an effort to force digital material into the characteristics of the physical world, where copygoods are limited in number.
- vs. Anonymous receipts
 - Loss of receipt means loss of material. Central registry is more secure for user. (E.g., house might burn down, but digigood receipts would survive in digigood registrar.)
 - Registrar based information offers protection against loss of privacy after compromise of user's secret key.
 - Registrars are more flexible across technological change. Because information is concentrated in relatively small number of tight managed commercial operations, changes can be made more rapidly than corresponding changes could be made to all consumer machines.
 - Development of successful attack on receipt technology would result in collapse of system, while central storage of access receipts would avoid this problem thanks to physical security of databases.
 - Even if databases were corrupted, backup copies of databases could be used.
 - Anonymous receipts are an attempt to technically secure privacy. Legal restraints (assisted by correct infrastructure) should provide adequate privacy, while allowing valid public safety investigations (see Chapter ?? Civic Digics).
 - See 4.7.3 +Privacy Protection.
- @ Access purchase price should be reasonable.
 - Access rights purchase should be substantially below current equivalent hardcopy price (since access purchase price is completely missing both physical and electronic distribution costs (electronic distribution should be priced separately and competitively – see 4.4.1 +Distribution), and also because access purchase is missing resale rights – see 4.2.6 +Transfer).
 - For single use digigoods, price shouldn't be much higher than single use rental. (Assuming that resale is not allowed – see 4.2.6 +Transfer.)
 - This depends on the typical “replay” value of the work.
 - Some digigoods, e.g., TV shows, entertainment books are typically “played” only once

4.2.2 +Access Rental

- @ Consumers should be able to rent access to a digigood.
 - Rent terms may be either for unlimited use for a given time period, or for a specified number of uses.
- Rent payments should be cumulative – i.e., rent-to-own.
 - A premium may be paid when ownership is achieved through rental rather than through outright purchase, however that premium should be reasonably small. (Ideally, it would be 0, but a reasonable price shouldn't be much higher than 10% to 20% of outright purchase price.)

4.2.3 +Simuluse Rights

- @ Simuluse = Simultaneous Use
- @ Software that is used simultaneous on multiple machines, with the value increasing roughly linearly with installation will likely need to be licensed on basis of number of simultaneous uses – this should be facilitated.

- Most text, audio or video digigoods, or interactive editors, etc. should not require simuluse rights when accessed by individuals.
 - However, group access to the same digigoods will often require simuluse rights.
- Simuluse examples:
 - Operating system: which might be running on multiple machines simultaneously, one as a personal computer, another as home server, another as a workstation for performing calculations.
 - Server (file, music, http, ftp, mail, etc.) applications
 - Parallel calculation software

4.2.4 +Limited Editions

@ Some cognigoods (typically graphic works) gain value in part through limited availability. Provision should be made for supporting such limited use in the digital world, while at the same time allowing such works to enter the digital record for research and preservation purposes.

@ Note: this is a small market requirement, but it's interesting to consider it and see how it could be satisfied by a digigood infrastructure.

- Examples
 - Currently, this ability shows up primarily in the form of limited edition graphic prints (and paintings).
 - However, given the correct technical infrastructure, the same ability to globally limit copies might have use for any digigood (e.g., a music performance, or the text of a poem).
- Generally, use of this facility should be restricted to artistic works – for informative and historical works, the public good is best served by increasing the breadth of distribution, not by restricting it. (This intent is fundamental to current copyright law.)
- So, two basic intents in supporting this facility:
 - to provide support for a market in limited editions
 - to preserve the public good as served by a wider distribution of informative and historic works

4.2.5 +Group Access

@ Groups of people should be able to purchase access rights to a digigood

@ Examples

- Family
 - Newspaper for home
 - Videos for children
 - Reference library
- Company
 - Software
 - Information library
 - Resources (clip art, etc.)

@ Group access agreements should address:

- Simuluse rights.
- Changes to group membership.

@ Group access will be most useful for small groups (families, small partnerships).

- The value of permanent access rights for a large group of people – especially for a group whose

membership changes over time – is difficult to calculate.

- Large groups will be better served by subscription agreements. (See 4.3.1 +Library Access.)
 - Access vendors should be allowed to refuse to sell permanent access rights to large groups.
- @ Note that as an alternative to group access, access vendors might offer group discounts – e.g., each member of the group would have their own, non-transferable access rights, but would have purchased them at a reduced rate.

4.2.6 +Transfer

- @ Consumers should not normally be able to transfer their access rights.
- However, it should be possible to purchase access transfer rights – at extra cost and subject to substantial limitations.
- @ Current copyright law allows the user to control re-distribution (through loan, rental or resale) of their copy. But there are numerous exceptions and qualifications to this (“first sale”) right.
- First Sale principle in copyright.
 - Various exceptions
 - Not allowed to rent software or audio recordings.
 - Movie videos are subjected to further restriction (FBI warning)
 - Playing music in public venue is not allowed (dance hall, commercial establishments, etc.) ASCAP deals with this.
 - Even when legal obstacles to resale don’t exist, practical obstacles do:
 - Deterioration of copygoods.
 - Transaction cost (find buyer, buyer has to check quality of good, good has to be shipped, etc.)
 - Does not apply to licensed use – which is not a “sale”.
- @ But ability to redistribute digigoods severely threatens the digigood market.
- Because digital copies do not decay, and because their resale costs can be made negligible, “used” digigoods could be resold at the price of “new” digigoods – thus resold access rights would compete directly with initial sales of access rights.
 - If a company were to estimate the price to be charged for a digigood, it would take the desired single use price and multiply it by the number of times that digigood is likely to be resold. Suppose that a digital book takes five days to read – then it is likely to be resold 73 times per year. Multiply that by number of years that the book is protected by copyright (about 100 years), and you get 7300 resales. So a book that should be priced at \$10 will need to be sold for \$73,000.
 - Actually, things get worse than this. Resale value is hurt drastically by reducing demand. E.g., with lots of sellers, many of whom are willing to sell for substantially reduced price, the market will drop radically once peak demand has passed.
 - Thus the possibility to resell digigoods drastically distorts the market. This distortion is undesirable, and should be prevented.
- @ For individuals, resale is not a strong necessity.
- Use of expensive digigoods can be cushioned by rent-to-own as described above, or by subscription models (see 4.3.1 +Library Access).
 - The oft cited case of students need to resell textbooks is countered by several observations:
 - Textbooks are expensive in part because their publishers expect them to be resold. If the ability to resell is eliminated, then the textbook price should drop.

- Textbooks might be rented for the the term of the class. Rent-to-own would allow students to retain particularly useful textbooks.
 - The ability to purchase or rent portions of textbooks should further reduce the price paid by students (see Dis-aggregation and 4.2.12 +Derivation.)
- @ However, for businesses, lack of resale rights might be a major problem.
- For businesses, lack of transferability can be a problem for big ticket items, which can represent a substantial portion of the business assets.
- @ There are two solutions to this:
- @ Mergers and buyouts should result in complete assumption of access rights by the acquiring company, so long as the original business survives as a recognizable accounting entity. The argument here is that the access rights have not actually been transferred, hence there is no need for a resale right.
- @ Organizations should be allowed to purchase resale rights, however those rights should be subject to strong limitations.
- For cases in which the business is dismantled, resale rights might be desirable as insurance against loss of investment. Since such cases are assumed to be rare, this rareness can be made explicit. E.g., resale right might be limited in number and/or frequency (e.g., can only be resold once, or only resold once within a given period (e.g., once per two year period). To prevent abuse by companies that expect to be ephemeral, right to resell might require a vesting period (e.g., resale might not be allowed until one year after purchase). Resale might be further limited by requiring that percentage of proceeds (or perhaps percentage of original sale price) be sent to rightsholder
- @ Or the business may acquire its digigoods through subscription rather than direct access purchase. Such subscriptions can either be allowed to lapse, or can be transferred.

4.2.7 +Machine Associated Access

- @ Sometimes digifacts (especially software) are considered to be part of a machine, and so access rights to such software is vested with the machine – i.e., the machine can be sold or otherwise transferred, with the digifact ownership transferring with it. Such licensing should be facilitated.
- Examples:
 - PVR, videogame OS, modem software
 - Robots (entertainment or recreation)

4.2.8 +Preview

- @ It should be possible to preview the work at no charge or minimal charge.
- E.g., the equivalent of glancing through a book in a bookstore, or skimming audio tracks, or catching a preview/trailer for a TV show or movie.
- @ Publishers are generally desirous to do this to the degree that it increases sales.
- Their main concern is to prevent “previewing” from replacing viewing.

4.2.9 +Printing

- @ Long digital documents are often printed out to facilitate reading – current video displays are too low resolution, too bulky, and too restrained by the mechanics of the underlying hardware and operating system.

- @ However, printed digigoods are susceptible to a number of access violations:
 - Printed documents can be redistributed: either commercially, or non-commercially to friends, family, etc.
 - Printed documents can readily be scanned to extract the text, thus facilitating piracy and other access infringements.
- @ Trusted platforms that have the advantages of printed paper should be developed.
- @ Until such platforms are available, documents with moderate to low security requirements should allow printing for an extra fee to trusted platform printers.
- @ Such printouts would be subject to certain limitations:
 - They may not be redistributed.
 - They may not be scanned or copied, nor may watermarks or copyright notices be removed.
- @ Note: none of these restrictions apply to free-access digifacts, which can be printed and distributed without restriction.

4.2.10 +Public Use Rights

- @ The purchase of public use rights should be facilitated.
- @ Public use rights will presumably be priced in relation to their impact on the author's ability to sell access rights. Widely displaying a work (say a first run movie, either for free or for rent) will obviously impact the further merchantability of the digigood.)
 - Permanent public use rights would likely be expensive – most displayers would rent.
- Examples
 - Music to be played in the background of a place of business.
 - Music to be broadcast for a free radio station.
 - An information kiosk provided for the convenience of visitors.
 - A movie shown at a theater, or at a company party.
 - A football game shown at a sports bar.

4.2.11 +Dis-aggregation

- @ It should be possible to purchase pieces of large works (e.g., tracks off an audio CD, chapters from a book, etc.) without purchasing access rights to the entire work.
- @ Pricing should be reasonable.
- @ The idea of dis-aggregation does *not* include:
 - @ Small pieces of works quoted for commentary or to make a counterpoint etc. (i.e., corresponding to current "fair use" quoting). This usage should be free of charge and access rights requirements.
 - Some people have argued that such small uses might be handled by micro-payments.
 - However, the cost of monitoring such transactions is probably not worth the small payment that would result.
 - More importantly, charging for such uses is contrary to the public interests. Small quotes used for the purpose of illustration enhance public debate – and this use should be naturally allowed without requiring the payment of an access fee for the "use" of the original work.
 - @ "Sampling" for use in another work. Uses such as this should be handled by rights clearance services (see 4.2.12 +Derivation).
 - Note: this can be a fuzzy boundary, but generally a dis-aggregated piece retains its identity (like a

chapter of a book or a track from a music album), while a sampling use tends to merge with the piece that it is incorporated into.

- The boundary is in part economic – dis-aggregated pieces are purchased by the consumer, but sampled pieces are purchased by the creator of the incorporating work.
- Thus access rights to the sampling work does not imply access rights to the sampled work.

4.2.12 +Derivation

@ Derivation of digigoods should be facilitated.

@ All automatic derivations should be included in the access purchase.

- In particular, changing technology should not require repurchase of digigood access rights.
 - Video: Video disc -> Video tape -> DVD, etc.
 - Audio: (LP, (8 Track), (High Fidelity tapes), audio tape, CD, MP3, SDMI?)
- Examples
 - e.g., change image format, compress it, or pass it along to a speech synthesis program
 - also, indices, statistical analyses of text, etc.

- Automatic derivation provide a clear benefit without additional effort on the part of the creator – hence no public good is served by granting the digigood owner additional control over this act.

@ In addition, the service of searching digigoods should be made available – even to consumers who do not possess access rights to the searched digigoods.

- However, care should be taken to prevent the search results from being used to reconstruct the digigood.
 - This could be done by searching a work repeatedly, targeting consecutive sequences, then piecing the consecutive sequences together.
- Searching without access rights provides a public service without substantially damaging the interests of the digigood owner.
 - Actually, such searches are likely to benefit the digigood owner, since they will result in increased sales of digigood of interest.

@ Re-use of materials should be facilitated by designating a re-use manager service for each digigood.

4.2.13 +Annotation

@ Neither annotations nor the sale of annotations should be restricted by the digigood owner.

- Naturally, use of the annotation will require the presence (and independent purchase of) the original work.
- Note that third party errata should fall under annotations (allowed) – not under derivative works.

4.2.14 +Composition by Reference

@ Composition of digifacts by reference should be facilitated.

- “Composition by reference” means that the composite digifact *refers to* rather than *includes* the component digifacts.
 - Note: HTML uses composition by reference.
- Note that a composite digifact is not necessarily a digigood – e.g., it might be a private email message.
- Similarly, a component digifact is not necessarily a digigood – e.g., it might be a public domain

image.

@ Why:

- Composition by reference offers efficiencies in caching when the same components are used repeatedly.
- Composition by reference also supports the business of offering libraries of component digigoods.

@ Examples of composite digifacts:

- An html formatted email message which uses a background image from a commercial library.
- An anthology of detective fiction stories.
- A collection of musical greatest hits.
- A virtual museum of current digital art.
- A custom constructed newspaper.
- A slide show including commercial clip-art.

@ The component digifacts might be:

- software components, images, sounds, animations, etc. intended to be used as components (like components to be used within a web page),
- or they might be dis-aggregated components of a larger work (such as chapter in a book, or articles in a newspaper).

@ Access rights to composite digifacts may or may not include access rights to component digifacts.

- If access rights to components is included, this may be by grace of a re-use negotiation, or it may be that the purchase of the composite is arranged to include the purchase of the components.
- If access rights to the components is not included, then it will be up to the consumer to obtain access rights.

4.3 +Library Access

@ The preceding section centered on the assumption that access would be purchased individually for each digigood of interest. The alternative, that access to libraries of digigoods be purchased, is considered here.

@ Implementation is presented in 5.6 +Library Access.

4.3.1 +Library Access

@ It should be possible to purchase access to libraries of digigoods.

@ Library examples:

- Recent articles of a particular periodical. (E.g., WSJ online)
- Entire current and past set articles of a particular periodical.
- Digital version of "book of month" club.
- A topically focussed collection of books and/or periodicals (e.g., Aerospace Engineers Bookshelf).
- Assorted digigood collections, e.g., "Bill Smiths Favorite Books".
- Musical libraries, e.g., new wave hits of the 80's.

@ Billing

- Consumer would pay a flat fee for unlimited access for some period of time to a library of digigoods.
- Or consumer fee might vary based on level of usage.

@ Access would only be available while subscription is in force.

- Permanent access would be equivalent to direct access purchase, and so has already been covered.
- Purchase of permanent access to an entire library would probably be unacceptably expensive, and would be subject to too many uncertainties (are additions to the library also covered, how to handle transfer rights for such a large investment, etc.). Subscription is a more immediate, and flexible, and thus more workable business model for library access.
- However, it should be possible to join library access vending with normal access vending so that books that are frequently used by the consumer are automatically purchased directly if that makes more sense.
 - Even if the library vendor does not directly provide this ability, the consumer's software might facilitate it.

@ Advantages

- Library access provides access to a broad range of material for a relatively low, predictable fee.

@ Objections to subscription model.

- Ephemeral. Access to digigoods disappears completely if subscription expires – or if library supplier goes out of business.
- Subject to vagaries of market. There's no guarantee that subscription will be well priced in future.
- Subscription provider may limit or otherwise change the list of available digigoods.

@ Response to objections:

- All of these objections are part of the innate tradeoff of library access. Consumers can always purchase permanent access to digigoods.

4.3.2 +Advertising Supported Access

@ Advertising supported access to digigoods should continue to be supported. However, mechanisms to suppress advertising in exchange for a fee should be provided.

@ Methods to suppress advertising should be disallowed (unless the consumer pays a suppression fee – see below).

- Advertising is currently technically countered in several ways.
 - Ad blocking on internet sites.
 - Automatic fast forward over commercials by VCRs.
- Ad blocking is countered by advertisers in a variety of ways.
 - Modifying ad urls to fool ad-blocking software.
 - Modifying television ads to deliver a message even when under fast forward and mute.
 - Post-production advertising lay-over. (Ads on baseball walls, playing fields, laundry detergent boxes added to program.)
- Ad-blocking and counter-ad-blocking might continue to advance.
 - Likely to faulty degree (e.g., misarrangement of web pages).
 - Ad-blocking might win.

@ And thus undermine the commercial infrastructure supporting otherwise free content

@ Extremely time shifted playback of recorded programs should be disallowed.

- The time shifted playback will have lost its value to advertisers, since the included advertisements are likely to be out of date.

@ Advertising tailored to the consumer should be supported.

- This provides an added value for both advertiser and consumer. Advertiser's money is more

efficiently spent, consumers are exposed to more relevant programming.

- Tailored advertising raises privacy issues – see 4.7.3 +Privacy Protection for more discussion.

@ However, it should be possible for the consumer to suppress advertising by paying an access/distribution fee.

- Advertising supported access is essentially library access with the subscription fee paid by consumer attention to advertisements.
- However, commercials are distracting and time consuming – many users will find it worth paying a fee to suppress them.

4.4 +Distribution

@ This section describes distribution related requirements.

@ Implementation is presented in 5.7 +Distribution.

4.4.1 +Distribution

@ The consumer should be able to download copies of digigoods (for which he possesses access rights) on demand.

@ Where demand might be:

- Downloading for first use.
- Downloading to a new device.
- Downloading to replace lost or destroyed copies of the digigood.
- Downloading to replace digigoods that had previously been cleared from local cache in order to free space for other uses.

@ Distribution of digigoods should be a competitive business.

- If the consumer is able to prove that he has a legitimate right to access a digigood, then the download of that digigood should be competitively priced.
- In particular:
 - Consumer should be able to select from a variety of servers when he needs to download a copy of a digigood.
 - Infrastructure should be provided to facilitate finding the best download price.
 - Consumer should be allowed to cache his digigood, either on his own machine or on some server which he owns or has access to – thus avoiding future download fees altogether.
 - Digistore selection and download should be completely automatic in most cases (i.e., the consumer clicks on a link or bookmark, or types in some digigood identifier, and the digigood appears in his viewer – with intrusion of pricing and selection process nor significant delay)

@ Download pricing should be clear and predictable.

- A flat fee subscription service would be an example.
- Bandwidth based downloading would be almost as clear.

4.4.2 +Portability

@ A consumer should be able to view a digigood on any secure viewer.

- In particular, digigoods should not be limited to specific proprietary platforms.

4.4.3 +Disconnected Functioning

@ Digigoods should continue to be accessible in both completely disconnected mode, and in locally connected mode.

- In locally connected mode, a consumer might download a digigood from his laptop to his OPD.
- Network connections are not always available.
 - Currently, even in well connected areas, consumers are often disconnected from the network for days at a time.
 - Workers in remote parts of the world are likely to be disconnected for months.
 - Networks suffer failures, and may even fail catastrophically due to a hostile attack.

4.4.4 +Caching Efficiency

@ Digigoods that are commonly used provide opportunities for efficiencies from local caching, and in a highly networked world, efficiencies from remote caching. This opportunity for efficiency should be exploited.

@ Digigoods that are used in multiple documents should be stored only once and referenced in a standard way. I.e., there should not be a separate copy for each document, and each document should refer to the shared resource in way that guarantees that the document editor or viewer will be able to find the resource, despite where

4.4.5 +Reduced Cost of Entry for Creators

@ Digital distribution greatly decreases the cost of reproducing and distributing copies of a cognigood. This cost reduction should be reflected in a reduced cost of entry to authors.

- This reduction in cost of entry is already visible in the explosion of free material on the web.

4.5 +Availability

@ Digital technology doesn't just facilitate the distribution of digigoods – it facilitates their restriction as well. Such restriction is often counter to the public interest. This section is concerned with assuring availability of digigoods.

@ Implementation is presented in 5.8 +Availability.

4.5.1 +Publication

@ Digigoods for sale to the general public should be considered to be *published*, and should be made subject to restrictions peculiar to this state.

- This state is to be distinguished from private and secret digifacts, which will not be made subject to the same restrictions – and which will in fact will enjoy certain protections. (See Chapter ?? Secrets.)
- The allowance of and support for private digifacts should not be used to shield what should be considered a digigood from these restrictions.

@ This distinction is meant to mirror a similar distinction in copyright law (though this has been muddled by recent changes in copyright law).

- Works did not receive copyright protection until they had been “published”, which required that the work:
 - Be marked with an copyright notice using a specific format.

- Be submitted in duplicate to the library of congress.
- These requirements been eased somewhat recently – but should be reinstated for digigoods.

4.5.2 +Term Limits

@ Term limits should equal those under copyright law.

4.5.3 +Deposit

@ All digigoods should be deposited with the Library of Congress (or similar public institution).

4.5.4 +Permanence

@ Once published, digigoods should remain permanently available for purchase.

- Availability should not be affected by demise of digigood owner.
- Digigood owner should not be allowed to raise prices exorbitantly in effort to take the work out of publication.
- Even if a work is updated, the outdated versions of the work should remain available for purchase and access.

@ Permanent availability facilitates wide distribution and ensures that the work remains in the public record.

- Both permanence and wide availability are considered to be in the public interest.
- Note that this intent is clearly present in copyright law:
 - First sale and deposit requirements, combined with the availability of libraries ensured that published works remained in the public record.

@ Permanent availability also prevents the digigood owner from forcing unnecessary and undesired updates on the consumer.

- This is particularly a problem with software.
- But is also a problem with textbooks, etc.

@ Note that the digigood owner's motivation to force upgrades is less under AVDS than it is under copyright law:

- Trusted platforms and other measures (see 4.7.2 +Infrastructure Protection) help to prevent unauthorized access to digigoods.
- Digigood owner no longer loses sales due to consumers resale (transfer right is not commonly possessed under AVDS). This is large part of the motivation for new versions of textbooks.

@ Certain exceptions to permanent publication should be allowed:

- Copyright infringement (e.g., work is found to constitute a copyright infringement after it is published).
- Some form of ban (e.g., state secret, material otherwise circumscribed(?))

4.5.5 +Updates

@ One of the advantages of digigoods is the ease with which they can be corrected and updated – this should be facilitated.

@ However, the ability to update a work should not be abused in an effort to keep the work in copyright.

- Previous versions of the work should remain available at a reasonable price.
- Errata corrections should be freely available to all access right holders, and should fall under the

original copyright date.

- Updates to a digigood should be made available to current digigood owners for a reasonable fee.
- @ When regular upgrades are required in order to maintain the utility of a digigood, but the digigood owner fails to provide this, then it should be possible for a third party to assume the right to provide upgrades to the digigood.
 - This is primarily an issue for software, but can also be an issue for resource type texts, which may contain errors, or which may need to be updated to reflect changing conditions. (E.g., encyclopedias, dictionaries, instruction manuals, maintenance manuals, etc.)
 - Considerations
 - Guaranteeing maintenance may not be cost effective for digigood owner.
 - Possibly, the owner will only guarantee maintenance for some period (e.g., a year).
 - And yet, loss of maintenance may be very expensive to consumers.
 - If users are willing to cover cost of maintenance, then their desire to do so should be facilitated.

4.5.6 +Platform Emulation

- @ Emulation of digigood platforms should be encouraged, especially when the original platform is no longer available or when it is substantially outdated. However, such emulation should provide reasonable remuneration to the owners of the emulated platform.
 - Examples:
 - Emulation of Windows OS on Macintosh or Linux
 - Emulation of video game hardware systems.
 - See 4.5.5 +Updates for the converse issue: updating digigoods for compatibility with updated platforms.

4.5.7 +Free Access Digifacts

- @ Distribution of free-access digigoods should be facilitated.
 - There are several types of free-access digifacts:
 - Expired protection digigoods (i.e., out of copyright)
 - Which may be digitized copies of out of copyright copygoods
 - Government digifacts.
 - Donated digifacts (free to use images, templates, tunes, recordings, software, fiction, biographies (vanity press) etc.)

4.5.8 +Indexing and Searching

- @ Indexing and searching functions on digigoods should be available without access charge from the rightsholder – even for those consumers who don’t have access rights to the work.
 - Both of these are valuable functions to users, and can be generated automatically from the digigood.
 - While many digigood owners might be willing to offer such rights for free in expectation of increase sales, others might desire payment – which would probably be supported under current copyright law, since the index or search results might be regarded to be a “derivative work”.
 - However, no work is required on the part of the rightsholder in order to generate these, yet he benefits from them, in the form of increased sales.
 - The benefit to both the consumer and the rightsholder argues for making this ability free of access

charge.

- Note that I have already argued indexing and searching should be covered as part of the access rights – here I’m arguing that they should also be available to consumers who don’t have access-rights to a particular digigood.

@ However, care must be taken when returning search results to prevent the user who does not possess access rights from reconstructing the original digigood from the returned search results.

4.5.9 +Research

@ Access to digigoods for academic, economic, etc. research should be facilitated.

@ Researchers need normal access to digigoods:

- Researchers publish books, meeting proceedings, articles in academic journals. However, their requirements here have previously been expressed in:
 - Advantages of Digital World
 - Reduced Cost of Entry
- Guaranteed publication and availability.
 - These requirements have been described throughout this section.
- Availability of libraries to ensure access to a broad range of materials at a reasonable price.
 - This has been dealt with in Library Access.

@ However, researchers also sometimes need extraordinary, analytical access to texts. This sort of access should be facilitated.

- Examples:

- Determine typical word use (perhaps for authors from a given time or region.)
- Determine the usage tree of some word or phrase. (Who used it first? How did it spread?)
- Trace the development of some musical genre.
- Locate all public writings of a particular author, so as to analyze the development of his style.

4.6 +Coexistence

@ While cognigoods are moving rapidly to digital form, they currently exist primarily in physical form (as copygoods), and will continue to do so in the future. This section is concerned with assuring a peaceful coexistence between digigoods and copygoods.

@ Implementation is presented in 5.9 +Coexistence.

4.6.1 +Copygood Conversion

@ It should be possible for a consumer to convert his currently owned copygoods into permanent access rights to the corresponding digigoods.

- This conversion process should be inexpensive.

@ While copyright law allows the copyright holder to refuse such a conversion process, there are advantages to the copyright holder to allowing it and charging a small fee for it:

- The original copygood could be taken out of circulation – thus preventing loss of revenue by resale.
- If the conversion fee is fairly small, then a larger number of copygoods will be converted, thus bringing more revenue to the copyright holders.
- Such a large initial conversion will help to build up, and thus fund and validate the digigood system.

@ Note: It's reasonable to consider whether "fair use" demands that users be able to convert copygoods to digigood access rights.

- There have been some court decisions in this direction:
 - Consumers are allowed to make backup copies of software, etc.
 - Conversion of audio CDs to MP3 form has been allowed as fair use.
- There are however, problems with this:
 - It would likely be widely abused – a consumer might buy an audio CD, gain digigood access then resell the CD.
 - It would not provide financial incentive for authors, etc. to digitize their creations.
- These problems are severe enough that interpretation of fair use in this way would be counter to the constitutional foundation for copyright, and thus would likely be ruled against in courts or specifically outlawed by congress.

4.6.2 +Digigood Printout

@ The reverse process – creating printouts of digigoods was discussed in 4.2.9 +Printing.

4.7 +Protection

@ Protection of digigoods, digigood infrastructure and privacy is considered in this section

@ Implementation is presented in 5.10 +Protection.

4.7.1 +Access Control

@ Digigoods should be secured against unauthorized access.

- Without sufficient assurance of protection against unauthorized access – both commercial and non-commercial, cognigood owners will not want to risk making their works available as digigoods.
 - Which means that consumers will lose the benefits of digital technology.

@ Care should be taken to ensure that legitimate users feel no need to violate protection measures.

- Consumers should be presented with a digigood deal that is simple, comprehensible, consistent and, above all, *fair*.
- No legitimate use should require circumventing protection measures.

4.7.2 +Infrastructure Protection

@ The digigood infrastructure, like the rest of the digital infrastructure, should be protected against attacks meant to subvert or cripple it.

- Our civilization already depends on the digital infrastructure – this dependence will become much greater as more digigoods become more and more the norm.
- Example: Morris' internet worm crippled the internet – and also left the operators with no way to communicate with each other – they didn't know each other's phone numbers – only email addresses.

@ In particular:

- Progressive failure of the infrastructure should be prevented.
- Access to critical cognigoods should be available even in cases of catastrophic failure of the digigood infrastructure.

@ Note: digital infrastructure protection is further considered in Chapter ?? Civic Digics.

4.7.3 +Privacy Protection

@ The privacy of consumers and digigood owners should be protected.

@ However, the level of protection provided must strike balance with the other requirements of the digigood infrastructure, and with the need for the government to prevent and punish criminal activity.

@ Commercial invasions of privacy should be prevented – except to the degree to which the consumer voluntarily accepts such intrusions in exchange for some benefit (well targeted advertising, discounts, etc.)

@ See Chapter ?? Cyberself Control for a discussion of consumer control of private information, and see Chapter ?? Civic Digics for a discussion of need for governmental invasion of privacy.

4.8 +Consumer Representation

@ The need for consumer representation in the development of the digigood infrastructure is considered here.

@ Implementation is presented in 5.11 +Consumer Representation.

4.8.1 +Consumer Representation

@ Consumers should have an active, truly representative, presence during negotiations over the digigood infrastructure.

@ The potential for abuse for vested commercial interests is large

- Implementation will likely be based on contract law (at least initially). This would generally imply a loss of power for consumers who can't afford to be present during the negotiation process.

Consumers need some way to compensate.

- This has clearly been the case for negotiations over extensions to copyright law.
- It has also been true for the development of UCITA – which will strongly affect contracts software and other digital goods.
- Potential abuses of vendor power.
 - Higher prices, when they should be lower
 - Lack of opportunity to purchase permanent access.
 - Withdrawal of digigoods from publication

@ Consumer advocate organizations are sometimes extreme in their positions – taking stances that are not in line with the desires of consumers (e.g., advocating protection of privacy at all costs).

@ Without representation, consumers will be wary and resentful of radical new changes.

@ A more direct and correct representation of consumers is required.

@ The need for consumer representation is developed in depth in Chapter ?? Consumers Union.

5 +Implementation

@ In order to meet the requirements related above, I propose the AVDS (Access Vendor – Digistore, pronounced “avids”) digigood infrastructure.

@ This section is broken down like this:

- The first three sections describe the commercial, technical and legal aspects of the AVDS system.
- The remaining sections directly address each of the requirements raised in the preceding sections, describing how each is met by AVDS as described in the first three sections.

@ Notes:

- While this chapter is concerned primarily with digigoods, AVDS recognizes other types of intellectual property and provides support other types of digifacts.
- This implementation is not monolithic – it’s possible to change many components, while retaining the core design of the solution. Thus, a disagreement with a peripheral component of the implementation should not be considered sufficient to discard the rest of the solution.
- Most markets are the product of market competition on a playing field defined by regulation. To achieve a desired end, market competition may be sufficient – or it may not. While I hope that market factors will be sufficient, I have tended to state regulatory, or contractual action that might be taken to ensure accomplishment of the desired result.

5.1 +Commercial Infrastructure

@ This section describes the commercial infrastructure of AVDS.

5.1.1 +Access Vendors and Digifact Distributors

@ The sale of access rights to a digigood is firmly separated from the distribution of that digigood.

- This is the central feature of AVDS.
 - “AVDS” is an acronym for the two business roles that embody this separation: Access Vendor and DigiStore.

@ Under AVDS, the digigood owner receives income from the sale of access to the digigood, but *not* from reproduction or distribution of the digigood.

- This is in marked contrast to the current system of copyright, where access is bound directly to reproduction and distribution (at least up to first sale), and income to the copyright holder comes solely or primarily from the sale of copygoods.

5.1.2 +AVDS Roles

@ There are nine basic roles in the AVDS system:

1 Digigood Owner

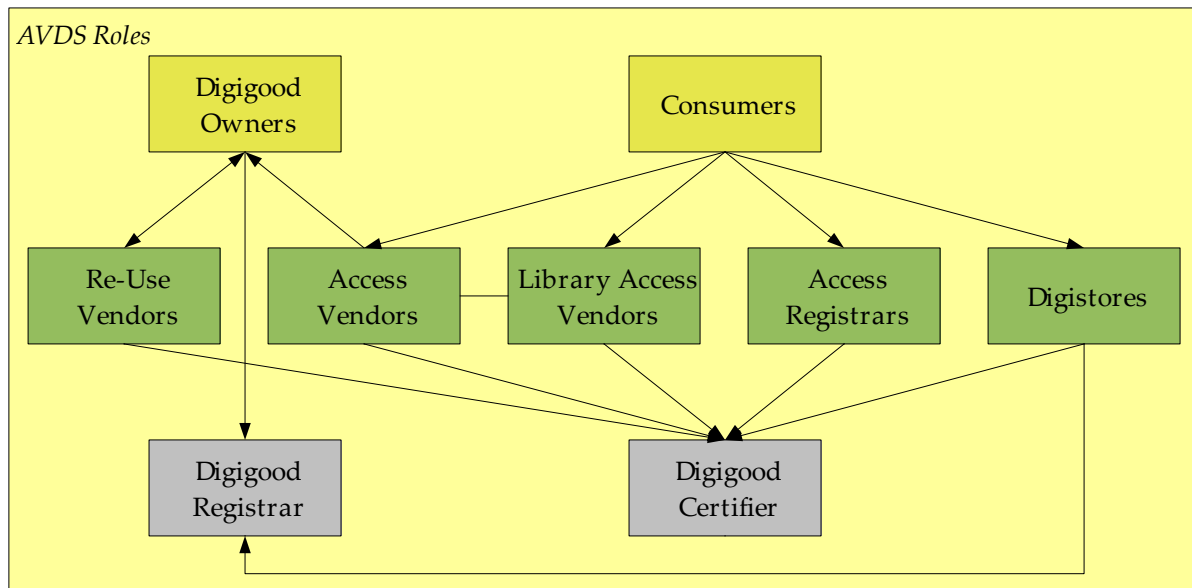
- The owner of the digigood, and thus the holder the monopolistic rights associated with that ownership.
- The owner is either the creator of the digigood (perhaps indirectly by hire) or some entity that has purchased the digigood from the previous owner.

2 Digigood Registrar

- A service for registering digigoods.

3 Digigood Certifier

- Certifies access vendors, access registrars and digistores.
- 4 Re-Use Vendor
 - Sells re-use rights to digigoods and portions of digigoods.
- 5 Access Registrar
 - A service for registering access rights of consumers for digigoods.
- 6 Access Vendor
 - A service for selling access rights to digigoods. Acts as agent for the rightsholder.
- 7 Library Access Vendor
 - A service for selling access to libraries of digigoods.
- 8 Digistore
 - A service for distributing digigoods.
- 9 Consumer
 - A user of digigoods.



Drawing 1AVDS Roles

5.1.3 +Typical Transactions

@ Before examining the AVDS roles in depth, it's useful to consider two typical transactions...

@ Digigood Registration

- Owner creates digigood
- Owner registers digigood with digigood registrar
- Owner arranges rights access vending terms with one or more Access Vendors.

@ Consumer Access

- Consumer acquires reference to digigood.
- Consumer purchases or rents access rights from access vendor.
 - Access vendor archives access rights purchase with Access Registrar specified in consumers request.

- Access vendor returns access rights receipt to consumer.
- Consumer requests copy of digigood from digistore.
 - Digistore checks Access Vendor for access rights.
 - Digigood returns encrypted copy of digigood to consumer.
- Consumer views or plays digigood.

5.1.4 +Digigood Owner

- @ The digigood owner possesses monopolistic control over the sale of access rights to the digigood.
 - The owner is either the creator of the digigood (perhaps indirectly by hire) or some entity that has purchased the digigood from the previous owner.
 - Sale of access rights is handled by Access Vendors. The owner may act as Access Vendor himself, or may contract with other Access Vendors to act for him.
- @ The right to control the sale of access rights is subject to certain limitations.
 - In particular, the digigood may not be taken out of publication.
 - See 5.8 +Availability for more detail on restrictions of access sale control.

5.1.5 +Digigood Registrar

- @ The digigood registrar handles registration of digigoods.
 - The registration process includes:
 - Receiving a copy of the digigood and archiving it.
 - Associating the digigood with a unique and permanent fixref.
 - Associating the digigood with one or more varrefs.
 - A small fee to cover general overhead and archiving costs.
 - (See 5.2.1 +Digifact References for a description of fixrefs and varrefs.)
- @ The digigood registrar also handles modifications to digigoods.
 - Ownership may be transferred.
 - Ownership contact info, etc. may be changed.
 - Varrefs may be modified by adding additional fixrefs or changing the default fixref (see 5.2.1 +Digifact References).
- @ The digigood registrar also makes copies of the digigood available to certified digistores.
 - Presumably charging a fee for doing so.
 - This should not be the primary business for the digigood registrar.
 - Pricing should be configured so that commercial digistores are encouraged to obtain digigoods from each other rather than from the central digigood registrar.
- @ As the central depository for digigoods, the digigood registrar is responsible for:
 - Making sure that all digigoods are stored with adequate redundancy and security to ensure their permanent survival.

5.1.6 +Digigood Certifier

- @ The digigood certifier certifies access vendors, access registrars and digistores.
 - Overall goal is to make sure that the various providers meet their obligations.
 - Certification process may recognize varying levels of security and other restrictions on operation.
 - A digistore might be limited to distributing movies and television shows.

- An access registrar might be limited to consumers of a particular nation.
- @ Certification would require an initial inspection of plans, procedures and facilities.
- @ Once in operation, certification would also incorporate unannounced tests of the security of the entity.
 - Test privacy safeguards.
 - Test digigood download security.
 - Etc.

5.1.7 +Re-Use Vendor

- @ Re-Use vendors, acting as agents for the digigood owner, sell re-use rights to digigoods and portions of digigoods.
 - Re-use vendors are equivalent to current rights clearing houses.
- @ Each re-use vendor operates by contract with the digigood owner.
 - The contract between digigood owner and re-use vendor will cover the obligations between these two entities.

5.1.8 +Access Registrar

- @ Access registrars records access registrations and make them available to digistores.
- @ Multiple access registrars exist and compete for the consumers business.
 - The user specifies the access registrar to use when purchasing access and when downloading the digigood.
- @ The access registrar has certain obligations towards the consumer:
 - It must protect the privacy of the consumer (except to the degree that the consumer allows otherwise).
 - It must provide a means for the consumer to readily check his access receipts.
 - It must facilitate the transfer of the consumer's receipts to another access registrar upon the consumer's request.
- @ The access registrar has certain security requirements:
 - It must demonstrate protection of the consumers privacy (to the degree demanded by the consumer).
 - It must demonstrate security against forgery of access receipts.
 - It must demonstrate security of receipts against destruction.
- @ vs. No Registrar
 - Rather than use an access registrar, receipts might be kept solely by the consumer.
 - This has the advantages of increased privacy, and decreased infrastructure.
 - However, this has the disadvantages of:
 - Note: the problems with this scheme were first raised in 4.2.1 +Access Purchase. They are repeated here for convenience.
 - Loss of receipt means loss of material. Central registry is more secure for user.
 - Development of successful attack on receipt technology would result in collapse of system, while central storage of access receipts would avoid this problem thanks to physical security of databases.
 - Even if databases were corrupted, backup copies of databases could be used.
- @ vs. Single Registrar
 - Rather than allow multiple registrars, a single central registrar might be used.

- This has many of the advantages of a multiple registrars.
- Potentially, it might offer higher security than multiple registrars.
- However, it has many disadvantages, many of which are related to it's likely position as a governmental body
 - The transactional demand would be enormous. Even as a distributed system, a single registrar would be difficult to build.
 - It would constitute a single point of failure or attack.
 - As a governmental authority, it would likely suffer from the inefficiencies of governmental creations.
 - Stated another way, the lack of competitive market pressures, would mean the removal of the forces that would drive the development of efficiencies.
 - Moreover, a governmental organization would be more likely to allow government directed invasions of privacy – it would be less likely to be subject to consumer demand for privacy.

5.1.9 +Access Vendor

- @ Access Vendors, acting as agents for the digigood owner, sell the right to access the digigood to consumers.
- @ Each access vendor operates by contract with the digigood owner.
 - The contract between digigood owner and access vendor will cover the obligations between these two entities.
 - Current rights clearing houses may expand into the access vendor role – especially for small digigoods (photographs, etc.).
- @ Access vendors record access sales with the access registrar specified by the consumer.

5.1.10 +Library Access Vendor

- @ Library access vendors sell access to libraries to digigoods.
- See 5.6.1 +Library Access for more information on library access vending.

5.1.11 +Digistore

- @ Digistores securely distribute digigoods to authorized consumers.
- @ Customers demonstrate access authorization through a receipt stored with a certified access registrar.
- @ Many digistores exist and compete for the consumers business.
 - Income comes by charging for downloads – possibly a per download fee, or a consumed bandwidth fee, or possibly a flat monthly fee.
 - Digistores should respond to requests for bids by the consumer – especially for large downloads.
- @ Secure distribution is accomplished by encrypting the digigood to be delivered so that it may only be played by the receiving consumer on a trusted platform.
- @ Exception: free access digigoods do not require checking for consumers access rights, nor do they require encrypted delivery.
- @ Digistores must be certified by the Digigood Certifier.
 - Certification has various levels: e.g., a digigood might be authorized to only deliver digigoods with low to moderate security requirements.
- @ To achieve and maintain certification, digistores must:

- Demonstrate accurate delivery of requested digigoods.
 - Demonstrate up-to-date translation of varrefs to fixrefs.
 - Demonstrate secure storage of digigoods.
 - Demonstrate secure delivery of digigoods.
 - Demonstrate that digigoods are delivered only to consumers with appropriate access rights.
 - Demonstrate the ability to meet their claims. (E.g., if a digistore claims to be able to deliver any digitized movie to a consumer, then it must demonstrate the ability to do so.)
 - Maintain the privacy of consumers (except to the degree that the consumer allows otherwise).
- @ Digistores do not have any direct relationship with the digigood owner.
- They obtain original copies of the digigood from the digigood registrar or from other digistores – not from the digigood owner.
 - They do not pay the digigood owner for the right to distribute digigoods.
 - They are however liable for damages to the digigood owner, if they fail adequately verify access rights for a digigood, or fail to adequately secure delivery of the digigood.
- @ Digistores will likely store the most requested digigoods, only going to other digistores as necessary, and only rarely going to the digigood registrar.
- It's likely that digistores will form a loose tree structure of digigood distribution, with the digigood registrar at the root, then digistores that specialize in serving other digistores, possibly by specialization (e.g., American newspapers), and finally digistores that serve consumers.
- @ Digistores can provide automatic derivations as requested by consumers:
- Reformatting.
 - Indexing
 - Full text searches
- @ Digistores automatically provide load balancing for heavy demand documents.
- @ Digistores automatically reduce long haul network traffic.
- Nearby digistores will be able to submit lower bids for supplying digifacts (at least for large digifacts).
 - Even if bidding is not common, digistores will be motivated to move popular material close to the consumer in order to reduce their network transmission costs.
- @ Digistores can distribute digigoods on physical media, if that makes sense.
- Digigoods could be encrypted, burned onto a disk and then mailed or released from a local store to the consumer.
 - This would be useful for large digigoods (e.g., movies, large archives, etc.)
 - It might also be useful for constructing an initialization disk for a personal computer.

5.1.12 +Consumer

- @ The consumer accesses digigoods, buying access through access vendors, downloading content through digistores, and then viewing the digigood on a trusted platform.
- @ The consumer's access rights are recorded by the access vendor of his choice.
- The consumer will most likely rely on a single access registrar, however if he wishes to several access registrars for different records – or possibly for redundancy of all records, he may do so.
 - The consumer who uses multiple access registrars will likely rely on software to automate the selection of access registrar for any particular access purchase or digigood download.

- @ The consumer selects which digistores to download from.
 - Software will be used to automate selection of a digistore, with the aim being to minimize download costs.
- @ The consumer must have a trusted platform for accessing the digigood.
 - The trusted platform may be a special purpose device (an e-book reader), or it may be a general purpose computer with architected to provide a trusted platform.
 - Trusted platforms will likely vary in level of security – digistores will refuse to download digigoods to platforms with insufficient security.
 - See 5.2.5 +Trusted Platform for more information.
- @ The consumer may cache downloaded digigoods indefinitely.
 - The digigood may be cached on the trusted platform, or it may be cached on a local server.
 - However, it may not be cached in a public area – even in encrypted form.
 - The consumer will likely delete large, unused digigoods to free space – especially if those digigoods were only rented, and the rental term has expired.
- @ Consumer's software might do a regular background check for updated copies of cached digifacts.
Updates could be automatically downloaded or they might be indicated to user by some sort of mark on his viewer.

5.2 +Technical Components

@ This section describes the technical components of AVDS.

5.2.1 +Digifact References

- @ Digigoods are specified, or referenced through fixrefs and varrefs.
- @ Fixrefs are unique and permanent. Each fixref permanently refers to a single, fixed stream of bits – i.e., to a single version of a digigood.
 - Any new version of the digigood must be assigned a new fixref.
 - Any reformatted version of the digigood must be assigned a new fixref.
 - However, transient reformattings of the digigood (e.g., consumer requests that a jpg image be reformatted as a GIF image) do not require recognition in the AVDS system, and so do not require a new fixref.
- @ Varrefs are also unique and are permanent in many (but not all) ways.
 - Varrefs refer to a set of fixrefs, where the fixrefs are typically successive versions or reformattings of a single digigood.
 - Varrefs have default fixrefs, where the default fixref is one of the
 - Varrefs allow recognition of different versions of a digigood by all of the versions
 - Varrefs are part alias and part like directory.
 - Varrefs are like aliases in that they point by default to a single fixref.
 - However, the default fixref may depend on some parameter specified by the requester (e.g., file format).
 - Varrefs are like directories in that they encompass a set of fixrefs.
 - The default fixref must belong to this set.
 - Varrefs are impermanent in certain ways:

- The set of encompassed fixrefs may be expanded.
 - The default fixref may be changed.
 - Varrefs are permanent in other ways:
 - Fixrefs, once added, may not be removed.
- @ The digigood registrar is responsible for handling changes to varrefs and for maintaining the canonical database of fixrefs and varrefs.

5.2.2 +Encryption

- @ Digigoods are transmitted and stored in encrypted form.
- Encryption is typically done with a symmetric key.
 - Except for free-access digigoods, which may be transmitted and stored in the clear.
- @ Aside from the digigood itself, the encrypted stream includes a copy of the access agreement, including:
- The number of allowed uses, period of allowed use, etc.
 - The identity of the allowed accessor.
- @ In addition to the encrypted stream, the following are also sent by the digistore:
- A clear copy of the the access agreement.
 - This is included for convenience.
 - For each TP system to be used:
 - An encrypted copy of the symmetric key (with encryption done using the public key of the TP)
- @ Note that if the consumer acquires another TP and wishes to use the cognigood on it, then he can go back to the digistore and request a new copy of the symmetric key encrypted for his new TP.
- This avoids the need to re-encrypt and re-download the entire digigood, and so should be available for a near-zero fee.
- @ Encryption raises civic security issues. These are dealt with in a later chapter.

5.2.3 +Watermarking

- @ Digigoods may also be watermarked for each consumer.
- Watermarking is a technical process which modifies the digigood to include information such as the digigood owner and consumer.
 - The purpose of watermarking is to discourage consumers from illegitimately distributing copies of the digigood (i.e., even if the consumer manages to break the TPS, the decoded digigood will still contain the watermark, and so will point an accusing finger back at the consumer).

5.2.4 +Identification

- @ Identification is used repeatedly in the AVDS system.
- In transactions between digigood owners, the digigood registrar and access vendors.
 - In transactions between consumers, access vendors, access registrars and digistores.
 - By trusted platforms, to determine that the authorized user is present.
- @ Identification needs are met by a combination of hardware and public key infrastructure.
- Hardware ID elements were described in a previous chapter.
 - Public key infrastructure is described in the next chapter.
- @ The consumers identification system supports both frequent and infrequent authorization.

- Some high security digigoods might require sub-minute verification of the presence of the authorized user.
 - However, background services might require only occasional re-authorization, and might allow that authorization to be carried out by proxy (i.e., by the user's personal server).
- @ See 4.7.3 +Privacy Protection (requirements) and 5.10.3 +Privacy Protection (implementation) for more comments on limiting the negative effects of pervasive identification.

5.2.5 +Trusted Platform

- @ Trusted Platforms prevent authorized users of digigoods from abusing their limits on access.
- TPs prevent the consumer from storing a decrypted copy of the digigood.
 - TPs prevent the consumer from accessing the digigood in violation of the terms of use (allowed period of use, allowed number of times of use, etc.)
- @ Trusted platforms can take the form of special purpose hardware, or general purpose computers that have been architected to ensure trusted operation.
- @ Re-architecting general purpose computers to serve as trusted platforms requires numerous modifications:
- Limitation of Input/Output channels and software to prevent interception of decoded digigoods.
 - Limitation of player software to prevent copying or insecure printing of digigood.
 - Verification of software to ensure that trusted software has not been replaced by non-trusted software.
 - Etc.

5.2.6 +Simuluse Manager

- @ Simuluse is enabled by a simuluse manager.
- This service ensures the the simultaneous use limitations of the access agreement are met by allocating use of the digigood to other TPs for limited periods of time.
 - These secondary TPs can surrender their "rentals" early, or they can ask for extensions as needed.
 - This service would run on a consumer's TPs, or it might be run remotely by a digistore.

5.3 +Legal Infrastructure

@ This section describes the legal infrastructure of AVDS.

5.3.1 +Superseding Copyright Law

- @ AVDS will initially be implemented entirely through contract law.
- Digigoods will be made available by contract agreement with the copyright holder.
- @ Once the AVDS structure has matured, it may be desirable to move it to civic law – either running in parallel or replacing the existing copyright law structure.
- Contracts will be constructed with this possibility in mind.
 - Contracts will be divided into those that are natural to the AVDS infrastructure, and those that are necessary to connect the AVDS structure to existing copyright law.

5.3.2 +Standard Consumer Contracts

@ AVDS will employ absolutely standard contracts with the consumer.

@ The particulars of a digigood access contract are specified in a single, standard dialog box.

- It will include:
 - Type of access right: permanent, rental (and term), or usage (and number of uses and left)
 - Required security level of TP (e.g., High, Medium or Low)
 - Special provisions: e.g., lack of printing right, presence of resale right, etc.
- Components of the dialog box will be limited in number so that it may be understood in a short glance.
 - No fine print.
 - No extra “advanced” dialogs, or tabs.

@ Consumer contracts with digistores and access vendors will be similarly simple and standard.

@ When the consumer acts as casual, non-professional creator, and thus owner of digigoods, similarly simple contracts are available to to him from access vendors and the digigood registrar.

- Professional authors and creators may desire more complex, non-standard contracts with access vendors.

5.4 +Fundamentals

@ This section describes how AVDS meets requirements specified in 4.1 +Fundamentals.

5.4.1 +Benefit to Public

@ While AVDS radically alters the commercial cognigood infrastructure, it retains the cognigood ownership and the monetary rewards that encompass, while at the same time lowering costs for both digigood owners and consumers.

@ Most fair use is retained and indeed is expanded in some places – but generally not at the cost of digigood owners.

@ First sale is abandoned for the most part because of severe problems with its implications in the digital world.

- However it is expected that the consumer should receive reduced prices as a result.

@ The public benefits deriving from libraries and research uses are retained, in part through the requirement of continual publication, in part through the allowance of automatic derivation, and in part through expected commercial development – namely subscription funded electronic libraries.

@ The existing copyright term limits are expected to be retained.

5.4.2 +Advantages of the Digital World

@ AVDS retains the advantages of the digital world.

- In particular
 - Copying and distribution should be at zero or low cost.
 - Zero-cost when the consumer copies and accesses his own digital files.
 - Low cost when the consumer downloads a copy from a digistore, thanks to competition between digistores.
 - Immediate distribution through digistores.

- Production on demand through distores.
- Portability across devices thanks to the implementation of encryption.
- Low bulk is natural to digifacts. Also:
 - The AVDS system guarantees that owned digigoods can be offloaded, thus freeing up storage space, without surrendering right to use those digigoods.
 - The right to access does not derive from a copygood, usage is not constrained by the physical bulk.
 - Improved (higher density) storage technology is naturally used – hence the consumers cached digigoods can be expected to become more compact as technology improves.
- Searchability is natural to digifacts, and is covered by derivation access rights. These access rights guarantee that the consumer can search his digigoods himself, or use a distore to perform the search.
- Hyperlinks are natural to digifacts. Annotation is guaranteed by annotation rights (see 5.5.12 +Annotation).
- Backups of consumers digigoods are automatically provided by distores and access registrars.

5.4.3 +Simplicity

- @ While the details of the digital infrastructure can be complicated, the basics of the deal and infrastructure can be stated in few short sentences:
 - Consumers can purchase permanent personal access rights to any digigood.
 - That digigood can then be downloaded any number of times to any secure device.
 - Access rights to the digigood are purchased from the authorized access vendor.
 - Downloads are obtained from distores at a competitive price.
 - Digigoods access rights cannot, under ordinary circumstances, be sold or otherwise transferred.
- @ The AVDS system applies to all digigoods, regardless of digigood type (text, audio, video, resources, software).
- @ Access to digigoods will be 99% transparent, and quite simple when it's not transparent.
- @ Access to any access-allowed digigood is completely transparent: the user clicks on a bookmark or link, or types in the name of the digigood, and the digigood appears in the secure viewer. Access to local cache or remote distore will be completely automatic under normal circumstances.
- @ An attempt to access to a digigood for which the consumer has not yet purchased access will result in an automatic redirect to the access vendor for the digigood, with a dialog box offering terms for purchase or rental. If a purchase is made, then the digigood will appear automatically, as before.
- @ Good user interface design will maximize clarity and simplicity at other times when the consumer needs to manage components of his digigood system.
- @ Contract dialog simplicity is guaranteed by simple consumer contracts (see 5.3.2 +Standard Consumer Contracts).

5.4.4 +Durability

- @ AVDS is designed specifically for the digital world – not just as an extension of copyright law.
- Starting from scratch in this way makes it possible to accommodate potential changes in technology.
 - Changes in file formats, encryption requirements, transmission protocols, etc. are all accommodated because the fundamental transaction is the sale of access to a digigood, not of a particular copy of

that digigood.

- Recognizing levels of security in digigoods, in digigood services, and in consumer hardware, makes it possible to adapt flexibly to advancing technology of attack and protection.
- @ AVDS and its variations are flexible enough to replace copyright law eventually.
- @ AVDS extends naturally down to physical form – printouts of text, etc. can be covered under the basic access purchase agreement.
- @ AVDS can extend naturally into other schemes, such as paid and advertising supported subscriptions, broadcasting, etc.

5.4.5 +Progress

- @ Under AVDS, consumers will see the advantages that digital technology promises, while not losing the fair use freedoms provided under current copyright law. (With the notable exception of first sale rights.)
- @ Creators of cognigoods will also benefit from a more efficient, automatic distribution structure – and thus reduced middleman cost.
 - See 5.7.5 +Reduced Cost of Entry for Creators.
- @ The ability to purchase permanent access to a cognigood should make price comparisons with the current publishing market obvious, and thus should help to keep pricing at a reasonable level.

5.5 +Access Rights

- @ This section describes how AVDS meets requirements specified in 4.2 +Access Rights.

5.5.1 +Access Purchase and Rental

- @ Under AVDS, access purchase and rental are provided through access vendors.
 - The access registrar ensures that access rights, once purchased, are maintained indefinitely.
 - Thus, progress of rentals payments towards full ownership can be tracked easily.
- @ Pricing of digigoods is set by market demand.
 - It is expected that market forces will drive pricing to something close to the goals stated in the requirements.
 - However, a few requirements might encourage reasonably pricing:
 - The digigood must be available for permanent access, and that price must be posted with the digigood registrar and clearly posted by the access vendor on his purchase screen.
 - The access vendor must indicate whether it offers “rent-to-own” and at what terms. The terms must be simple and follow some standard format.

5.5.2 +Simuluse Rights

- @ Simuluse rights can be purchased through access vendors.
- @ Support for simuluse monitoring is provided by the simuluse manager module of the consumer’s TP.

5.5.3 +Limited Editions

- @ Limited edition cognigoods run counter to the thrust of the AVDS system, but can be supported with a little tinkering and the addition of an limited edition manager service.

- The following is speculative – details can be worked out by interested limited edition art authorities and consumers.
- To preserve value of limited editions:
 - Digital form of cognigood is registered with digigood register, but marked as “Limited Edition”.
 - General digistores are not allowed to obtain or serve the digigood.
 - Instead, the digigood is made available through a limited edition manager service, which acts as: access vendor, access registrar, digistore and global simuluse manager.
 - The edition manager makes the initial sale of copies, and then brokers any subsequent sales of access.
 - In this case, the purchasers *are* able to transfer their access rights – this is reasonable since the edition manager forces the digigood to act like a copygood.
 - Access transfers must be made with the cooperation of the edition manager in order to ensure that one licensed instance is terminated before another instance can be used.
 - Number of authorized copies must be small – say less than 500.
 - This information is recorded with the digigood registrar.
 - The edition number and total number of editions must be attached to and clearly displayed with each authorized copy (e.g., “139/500”).
 - Once initially declared, number of authorized copies may not be modified. If general sale of degraded form of digigood is made possible, that must specified at the time or creation, and must be noted on each limited edition copy (e.g., “139/150, GARQ” where GARQ indicates General Availability of Reduced Quality, or something similar)).
 - Derivative works are forbidden.
- To preserve public interest in wider distribution:
 - Use of the limited edition support is limited to works of art.
 - The digigood is made available for research purposes only to historical and aesthetic researchers at specially authorized digistores.

5.5.4 +Group Access

@ AVDS support for group access has several facets: group definition, group membership verification, access purchase and digigood distribution.

@ Group definition is handled using the same infrastructure that is used to define individuals – this is discussed in a later chapter (Cyberself Control).

- For now, it is sufficient to understand that group definition infrastructure provides:
 - Specification of type of group: family, club, non-profit organization, business, etc.
 - Specification of size and identification of members of group.
 - Ability to add and remove members from the group.

@ Group membership verification is handled using the same PKI technology that is used to identify individuals.

- There is a complication in that an individuals membership in a group may expire or be terminated.
- This is handled by:
 - Providing time limits for the group identification keys that the individual carries with him.
 - Or by not storing group keys with the individual – instead the individual must forward identification requests to some group server – which will of course only verify requests for

individuals who are currently members of the group.

- This solution has higher security than the previous solution, but requires more transactions, and is more susceptible to network failures.

@ Group access purchase and digigood distribution are handled in the same way and by the same infrastructure as individual access purchase and digigood distribution.

- Simuluse management is used as required by access agreements, with the simuluse manager being run by a group owned server.

@ Pricing is again left to market forces.

- However the requirement for permanent access purchase is removed.
- Also, it is expected that access vendors may refuse to sell access rights to large groups because of the difficulty of determining appropriate pricing.
- Subscription based digigood access is likely to provide better control and pricing than outright access purchase for large groups. (See 5.6.1 +Library Access.)
- Note that groups will still have the option of buying individual access rights for their members – and likely will be able to make such purchases at bulk discount.
- The presence of this alternative should provide a cap to large subscription charges.

5.5.5 +Transfer

@ Under AVDS, transfer rights will not normally be part of access purchases, however they may be purchased at extra cost and subject to substantial limitations.

@ Price for transfer rights will be determined by market forces.

@ Restrictions on transfer rights may include:

- Limits on number of transfers (typically once).
- A vesting period may be required (e.g., access rights may not be transferred within six months of purchase).
- A portion of the transfer price, or of the original access purchase price may be required to be returned to the access vendor.

@ Changes in group identification due to mergers and buyouts are not considered to be transfers so long as the original business remains a distinct accounting entity.

5.5.6 +Machine Associated Access

@ Machine associated digigoods is handled under AVDS by treating the machine as an entity possessing certain access rights.

- Digigoods are then downloaded in the normal way (with the consumer paying the digistore download fee) using the access rights associated with the machine

5.5.7 +Preview

@ AVDS supports previewing by several methods:

- Sampling: in which pieces of the digigood are made available to the consumer. Movie trailers are an example of this, as are short samples of music tracks.
- Scrambling: in which large portions of the digigood are left in the clear while other portions are scrambled into nonsense. This is particularly useful for previewing text works.
- Time limited preview: in which the full work is made available, but for a short time only – so that

the potential consumer can check any particular portion of the work, but doesn't have time to make use of the full work.

- @ The first two methods require no special abilities (i.e., they can be performed without encryption or identification of the consumer).
- The third method, full preview, requires identification of the end user and a trusted platform to display the digigood on – both of which are provided by AVDS.
 - Without identification, the access vendor cannot be sure that the consumer has not already “previewed” the work repeatedly, thus gaining full use of the digigood.

5.5.8 +Printing

- @ Under AVDS, printing rights would be purchased through access vendors for an extra fee.
 - @ Documents with high access security requirements might forbid printing entirely.
 - @ The price for printing rights would probably depend on:
 - The likelihood for illegitimate access (including casual sharing with friends and family).
 - The security needs of the document. (Newspaper articles are ephemeral, and so would have low security requirements.)
 - The term of the users access rights.
 - Printing a document potentially gives the user permanent access (unless a fading ink is used) – hence it implicitly upgrades temporary access rights to permanent level.
- @ Printing will generally be restricted to trusted platform printers:
 - TP printers will be configured to include watermarks on all printed pages.
 - Such watermarks will communicate the identity of the access right holder – thus the unauthorized distribution of such documents would point an accusing finger back at the access rights holder.
 - Copying machines and scanners might be required to refuse to duplicate and scan watermarked material.
- @ Low security, innately ephemeral documents (e.g., newspaper articles) might be printed to non-TP printers.
- @ Despite the possibilities given above, the final solution to the printing problem will be to bypass it – with a trusted platform that possesses the advantages of printed paper.
 - @ Such a platform might take the form of a binder containing thin, flexible sheets of electronic “paper”.
 - Each piece of paper would be high resolution, low power display, with a semi-fixed image.
 - Contents of each page would be varied according to the users desire. E.g.,
 - He might configure e-pages 1-5 to display the table of contents of a digital book.
 - Then configure the next 5 e-pages to display sections of the book that he has highlighted or annotated.
 - Then configure the next 5 e-pages to match the last 5 book pages read
 - Configure the following e-page to be the current book page. A “forward” tab at the bottom of the e-page would cause the current and five previous e-pages to shift one book page forward.
 - Configure the e-page after that as a scratch page page.
 - Displayed text could be highlighted and annotated using a stylus and/or keyboard and mouse.
 - The binder, though actually a computer with a very large effective display area, should behave like a book in many ways – instant on, low power consumption, rugged enough to be tossed around, shoved in a backpack and dropped on the floor – and inexpensive (preferably under

\$100).

- Unfortunately, these are some pretty rigorous technical demands – this sort of hardware will not be available soon.

@ A less demanding, but nearly as satisfactory a solution would be the presence of several low weight high resolution tablets – such as described in the first user story and in the subsequent hardware chapter.

- These would still more bulky than desired, but would likely make up for the bulk with the convenience that would come from digital operation (annotation, highlighting, etc.)

5.5.9 +Public Use Rights

@ Under AVDS, public use right would be an extra right to be purchased or rented from access vendors.

@ Pricing is driven by market forces.

- Pricing of public use rights would likely be handled similarly to group access purchase – i.e., it would take into account duration of use, total number of users, etc.
- Also like group use, a subscription approach is likely to be more desirable than a simple access purchase.

5.5.10 +Dis-aggregation

@ Under AVDS, the division of a digigood into pieces and the pricing of those pieces is left to the discretion of the digigood owner and access vendors.

- It is expected that market forces will encourage such dis-aggregation.

@ However, AVDS requires that purchase of pieces will count towards purchase of the whole – similar to the “rent-to-own” requirement mentioned previously.

- A premium may be charged for such piecemeal purchase, but this premium must be stated clearly with each piece purchase.

5.5.11 +Derivation

@ AVDS facilitates derivation through technical means and contractual restrictions.

@ All automatic derivation is included in the access purchase.

- Such derivation may be carried out by the consumer or by the digistore supplying the consumer.

@ Searching of all digigoods, even those to which the consumer does not possess access rights, can be performed by any digistore.

@ Re-use of digigoods is facilitated by re-use vendors.

5.5.12 +Annotation

@ AVDS facilitates derivation through contractual restrictions and technical means.

- Contractually, neither annotation, nor sale of annotation may be restricted by the digigood owner.
- Technically, annotation is facilitated by standard digifact references (fixrefs and varrefs), and by the guarantee of permanent availability of each version of a digigood.

5.5.13 +Composition by Reference

@ AVDS supports composition by reference.

@ Component references are in the form of standard fixrefs and/or varrefs.

- @ Component pieces of a composite digifact are indicated by fixref or varref.
- @ Access rights to component digigoods could be acquired in several ways:
 - @ If the composite digifact does not include access rights to the component digifacts, then the consumer would need to purchase the access rights in the normal way – through access vendors or subscription vendors (see below).
 - @ When a published digigood includes other digigoods by reference, then the stored digigood includes those references, and so access authorization for the master digigood automatically includes authorization for the referenced digigood (at least for use within the master digigood – use outside of master digigood may not be allowed).
 - @ When a private digifact includes digigoods by reference, then there is no public copy of the digigood to check for authorization. Instead, the private digigood must include authorization for each of the referenced digigoods in the form of a secure receipt (presumably signed by the author of the composite digifact).
 - Since references in private digifacts are not registered with the Access Registrar, this type of reference is inherently less secure than a reference in a published digigood.
 - Thus, creators of digigoods that permit use in non-published communications must be willing to accept the lower level of access control that goes with this type of use.
- @ Downloads of referenced digigoods are obtained from digistores in the normal fashion.

5.6 +Library Access

@ This section describes how AVDS meets requirements specified in 4.3 +Library Access.

5.6.1 +Library Access

- @ Under AVDS, library access rights are purchased through library access vendors. (LAVs)
 - These vendors may be authorized directly by the cognigood owner, or indirectly through other owner appointed access vendors.
- @ The primary differences between library access vendors and direct access vendors are:
 - Library access is available by subscription only. Once the subscription terminates, access to the digigoods included in the library terminates.
 - In particular, there is no equivalent to the rent-to-own.
 - LAVs also act as access registrars for their subscribers.
 - Because access is entirely dependent on the LAV involved, there is no need to maintain access records that will survive the termination of the LAV.
- @ Library subscriptions may be transferable, and refundable for partial use, depending on the agreement between library access vendor and consumer.
 - Since library access is purchased as a subscription, potential losses are limited to the period that has been prepaid.
 - Thus, there is reduced need to arrange transfer rights and refunds in the library access contract.
- @ Distribution of digigoods is handled by digistores.
 - Downloaded digigoods would have short use terms (say 24 hours).
 - If the user chooses to re-view the digigood after the initial period has expired, then it's only necessary to obtain an updated license, rather than re-download the entire digigood.

- @ Library access pricing is left to market forces. Pricing may will likely reflect:
 - The desire of the consumer to have predictable pricing.
 - Quantity of digigoods available through library. Larger libraries are more likely to meet the needs of the consumer.
 - Quality of library content. Higher quality digigoods are more likely to be satisfying and useful to the consumer.
 - Timeliness of library content. Rapidly moving fields require continual access to the newest information.
 - Note that bandwidth should not be a factor, since distribution will be handled by digistores.
 - The quantity of material accessed by the consumer.
- @ If the consumer wishes to permanently purchase a digigood, then they can do so through a direct access vendor
 - The consumer's viewer software can facilitate such a purchase by supplying a "Buy Direct Access" button in the interface.
 - Agent software running on the consumers computer might automate such purchases – especially when library subscription rates are dependent on usage, and the user is repeatedly using particular digigoods.
 - The library vendor might also offer a discount on direct access purchase of displayed digigoods.

5.6.2 +Advertising Supported Access

- @ Trusted platforms will disallow (uncompensated) suppression of commercials and extremely time-shifted playback.
- @ However, trusted platforms combined with the access vendor infrastructure will also support:
 - Playback of previously downloaded digigoods with up-to-date advertising insertion.
 - Suppression of advertising thanks to library or direct access purchase.
 - Note that broadcast television acts like a combination of a digistore and an advertising supported library access vendor. It should therefore be possible to suppress commercials in a recorded broadcast by paying an access fee to the broadcaster.
 - Who does access-payment go to? Presumably to broadcaster to replace commercial viewing obligation. But a cut of that payment would also go to cogniright holder. Division of payment should probably be explicit. (There would be a fixed digistore fee from broadcaster plus a cogniright fee from the cogniright holder.) Note that there might be cases such as user has a subscription to "60 minutes" or to all Star Trek family shows, and so user would only have to pay the digistore fee.

5.7 +Distribution

@ This section describes how AVDS meets requirements specified in 4.4 +Distribution.

5.7.1 +Distribution

- @ AVDS supports on-demand, competitive distribution through:
 - separation of access vending and distribution
 - de-monopolization of reproduction and distribution rights

- consumer agent software to select between digistores
- @ Particulars of download pricing are left to market forces, however it is likely that pricing options will likely be include:
 - A flat periodic fee
 - A transaction fee (based on the number of downloads).
 - A bandwidth fee (based on the cumulative size of the downloads).

5.7.2 +Portability

- @ Through its consumer centered access authorization and separation of access purchase from distribution, AVDS prevents access rights from being limited to any particular machine (except for machine specific software – see 5.5.6 +Machine Associated Access.)
- @ AVDS technology and infrastructure is not limited by proprietary interests.
 - @ AVDS infrastructure is independent proprietary interests. I.e., it does not rely on particular operating systems, etc.
 - @ AVDS does require that the end consumer have a trusted platform – however proprietary limitations on the technology for such platforms are specifically disallowed.
 - @ If a particular technology is required for AVDS, but is held by a proprietary company, than that technology must be licensed to all qualified implementers for a reasonable fee.

5.7.3 +Disconnected Functioning

- @ AVDS supports disconnected functioning through caching and long term access rights.
- @ The encryption system allows digigood keys for different trusted platforms to be stored at minimal cost. (E.g., a single copy of the encrypted digigood suffices for all consumer owned TPs, so long as digigood key for each of those TPs has been acquired.

5.7.4 +Caching Efficiency

- @ AVDS provides caching efficiency through: registered references (through the digigood registrar), digistores and consumer caching.

5.7.5 +Reduced Cost of Entry for Creators

- @ AVDS reduces the cost of entry for digigood owners by:
 - separating distribution from access vending
 - automating digigood registration
 - encouraging the development of mass market access vendors
 - Since access vending is a fairly simple service which is almost entirely automated, there will likely be a good business in providing access vendor services to non-professional digigood authors.

5.8 +Availability

- @ This section describes how AVDS meets requirements specified in 4.5 +Availability.

5.8.1 +Publication

- @ Under AVDS, all digifacts to which access is sold to the general public are considered to be *published*.

- These digifacts, called digigoods, are granted certain protections, but also restrictions.
- In particular, digigoods must be submitted to the digigood registrar.
- @ Private groups are allowed to own and distribute private digifacts (e.g., club newsletters) that are in many ways similar to public digigoods, but because of their private nature are protected from most of the restrictions placed on published digifacts (e.g., term limits, access requirements, etc.).
- In order to prevent abuse of ability to avoid the restrictions associated with publication, the following restrictions is applied:
 - A digifact distributed by a private group may not be declared private if:
 - a direct or indirect fee is charged for access or distribution of the digifact (where indirect includes group membership fees), **and**
 - any of the following are true:
 - The digifact is distributed outside the membership of the group.
 - Membership in the group is defined primarily by locality and/or interest in the digifacts distributed by the group.
 - The digifact is not concerned primarily with the focus of the group.

5.8.2 +Term Limits

- @ Under AVDS, term limits are identical to those under copyright law.
- @ Term limits begin at the date of publication, which is the earlier of:
 - the date of submission to the digigood registrar,
 - the date of publication of the original work, if the digigood is produced by digitizing a previously existing cognigood.

5.8.3 +Deposit

- @ Under AVDS, deposit is made to the digigood registrar (which may be a function of the Library of Congress).
- @ Note that under AVDS, deposit serves as an integral part of distribution (since the digigood registrar serves as the root digistore) – thus digigood owners are given a clear incentive to deposit.

5.8.4 +Permanence

- @ Under AVDS, permanence is assured in part by registration, in part by lack of need for stockpiling of copygoods, and in part by specific legal requirements:
 - The digigood once published, may not be removed from publication.
 - Digigoods once registered with the digigood registrar may not be removed or altered.
 - Note that new versions of existing works are handled by modifying varrefs (see 5.2.1 +Digifact References.)
 - The price for permanent access rights must be recorded with the digigood registrar.
 - This price must be reasonable (though it may take the form of an upper limit – e.g., “list price”).
 - At least one access vendor for the work must be specified at all times.
 - If an access vendor is not specified, or if the specified access vendor goes out of business, or otherwise fails to function properly, another access vendor will be appointed.
 - Proceeds from sales by an appointed access vendor will either be delivered to the digigood owner or held in escrow if the digigood owner cannot be located.

- @ Note: AVDS for the most part steers clear of attempting to specify “reasonable” prices, however it will do so in cases when necessary to support the rules cited here.
- The details of such determination are likely to be complicated, and so are not developed here.
- @ When it is necessary to block availability of a digigood (by reason of copyright infringement, or proscruption), then:
- Further access sales are blocked.
 - The digigood is retained in the digigood registrar,
 - but access is limited, and digistores are ordered to purge their copies of the digigood.

5.8.5 +Updates

- @ AVDS infrastructure makes updating easy and mostly automatic:
- The digigood owner registers the updated digigood with the digigood registrar.
 - And modifies the appropriate varref record during registration.
 - Such additions are automatically communicated through the digistore network.
 - Consumer software can check for updated versions of digigoods as each work is accessed.
 - Access registrars can notify consumers of updates to their accessible digigoods.
- @ AVDS provides additional legal restrictions to prevent upgrade abuse:
- All versions are guaranteed to be available for purchase at their originally specified fixref, and within the fixref listing of their originally specified varref (see 5.8.4 +Permanence).
 - Sale of digigood by varref automatically includes all fixrefs listed under that varref at the time of the sale.
 - Errata corrections, if they exist, must be freely available to all access right holders, and are considered to have the same copyright term as the original work.
 - Digigood owners are not allowed to restrict 3rd party errata annotations.
 - Updates to digigoods must be made available to the previous access owners for a price equal to the difference between the *current* price of the original work and the current price of the updated work.
 - Note that this update price is independent of the price with the access holder *originally* paid for the digigood.
 - E.g., suppose a consumer purchased version 1 of a digigood for \$20, but the current price for version 1 is \$18, while version 2 is available for \$19. In this case, the upgrade price from version 1 to version 2 would be \$1 (\$19 - \$18).
 - Note that this restriction combined with the requirement that previous versions of the work not be removed from publication, implies that the upgrade price will be kept low – oftentimes zero. (If the upgrade price is high, then the price of the original work must be correspondingly lowered – which will tempt new purchasers to purchase the original version instead of the current version).
 - To prevent digigood owners from claiming that the new version of the work is actually an entirely new work, new works will be required to be sufficiently different from existing works. The legal standards for “difference” will be closely related to the legal standards for identifying copyright infringement.
- @ AVDS provides legal procedures to permit third party developers to assume the right to update a digigood when the digigood owner has abandoned this right by failing to provide the required updates.
- The determination of abandonment of the update right (which is essentially the right to create

derivative works) is made by legal judgment (either a court of law, or some digigood specific legal body).

- The judgment of abandonment will require determination that:
 - The digigood's continuing value requires periodic updates.
 - That the availability of future updates be reasonably expected at time of purchase.
 - That the digigood owner has failed to provide such updates within a reasonable period of time, or be provably incapable of providing such updates in the future.
 - That significant damage will result to customers from lack of updates.
 - That a third party exists and is willing and capable to take on the task of providing updates.
- If abandonment is determined and a third party is given the right to perform the update, and if the updater requires access to source code and other resources held by the digigood owner in order to carry out their work, then:
 - the third party may reverse engineer the original work.
 - the third party may take legal action to gain access to that source material from the digigood owner.
 - The digigood owner might require 3rd party maintainers to maintain secrecy – i.e., maintainers would have to follow certain standard procedures in order to insure preservation of trade secrets, etc. (of course, if company no longer exists, then it can't have trade secrets, can it? But it might be going through bankruptcy – i.e., existing, but unable to maintain its previous products.)
- For consumers, the price for the updated work is equal to the price of the original work (paid to the original digigood owner) plus the update fee (paid to the updater).
 - The updating party may take legal action to reduce the price that may be charged for the original work (thus allowing him to raise his update fee). Such reductions will require that the updating party present evidence of reasonable expectations of reduction of the price of the original work. (E.g., the original party used to release yearly updates of the digigood, each time dropping the price of the previous version by 5%.)
- @ Allowing a third party to take over updating of a digigood is a radical step – a substantial reduction of the right to produce derivative works. AVDS ensures that such a step not be taken lightly by:
 - Reducing the financial motivation of third parties to do so – since they only benefit by the update fee, their payoff is inherently limited by the market demand for such an update.
 - Imposing substantial legal barriers to gaining the right to update.

5.8.6 +Platform Emulation

@ Under AVDS, there are two options for digigood platform emulation:

- If emulation can be carried out without infringing on the intellectual property rights associated with the original platform, then emulation can proceed without hindrance from the original platform owner.
- However, if infringement would be required, then party desiring to emulate would have to win a legal judgment that the owner of the original platform had abandoned his rights to produce the emulation (as a derivation).

@ The legal procedures permitting third party developers to develop and sell a platform emulation are similar to the procedures permitting third parties from assuming the right to update a digigood:

- A legal judgment of abandonment of the right to create the derivative work (the emulation) is required.
 - Emulator party would have to show failure of the platform owner to create the emulation, and his own ability and willingness to create the emulator.
- After winning such a judgment, the third party may reverse engineer the original platform.
- Sales of the emulator may require that:
 - the consumer purchases access to the original platform (which he may have already done), or
 - that a legally adjudged reasonable payment be made to the owner of the original platform.

5.8.7 +Free Access Digifacts

- @ The AVDS separation of the cognigood infrastructure into access vending and digifact distribution automatically facilitates distribution of free-access digifacts.
 - Digistores are naturally inclined to provide free-access digifacts, since they provide more bytes to transmit, and thus to charge for.
- @ Expired protection digigoods can be released by digistores unencrypted and without checking access rights.
 - Digistores are responsible for verifying the protection term has expired.
 - They'll be able to do this by checking with the digigood registrar.
 - The digigood registrar will be responsible for determining the date of the death of the rightsholder (when that is relevant, as it is now for copyright law) as well as factoring in changes in law governing the length of the protection term.
 - Expired protection digigoods can be sent in the clear and viewed on non-trusted platforms.
- @ Most public US government documents are available free-access to US citizens. In this case, an AVDS digistore only has to check the identity of consumer (at least to the extent of his nationality) before providing him with such a document.
- @ Voluntary or sponsored digitization of free-access copygoods is encouraged by AVDS.
 - Because AVDS provides a distribution channel with a wide audience at no cost to the digitizer, the digitizer is guaranteed that his effort will enjoy use.
 - Moreover, the digigood registrar service can be leveraged to prevent duplication of effort between different digitization teams. (By providing a standard naming convention – i.e., the fixref/varref system, and by providing a record of existing digitizations.) With a little extra effort, digitization teams could coordinate their future efforts also do not collide with each other.)
- @ Donated digifacts are facilitated by AVDS.
 - Authors of donated digifacts are generally willing to allow distribution of their products, so long as no non-distribution related charge is associated with them – AVDS gives them exactly this assurance.
- @ Open source software is facilitated by AVDS.
 - Open source allows free access, but requires the derivative products be published and made open-source under the same terms as the original software.
 - Under AVDS, this could be implemented like this:
 - A standard open source re-use contract would be developed.
 - A creator of an open source digifact would then register it as a digigood, but guarantee in the access contract that digigood would be permanently free and open source. The re-use vendor

would present these same terms to those who wish to re-use the code.

- Subsequent developers could then either donate their code modifications back to the original digigood owner to be shared under the same contract, or they could use the re-use contract to fork the code, then register themselves as digigood owners for a forked version of the code.
- It would probably be useful for open source digigood ownership to be consolidated under a single entity.
 - Such an entity could provide necessary staffing and continuance of operation.
 - It would have the resources to take legal action in response to re-use violations.

5.8.8 +Indexing and Searching

@ Digistores are allowed to offer indexing and searching functions for any digigood – regardless of the consumers possession of access rights to that digigood.

- The digistore would allowed to charge for this function.

@ The digistore would be obliged to limit the context returned for any single search.

- This is to prevent original text from being compiled from repeated searches targeted at adjacent pieces of the digigood.

@ Index and search results might be limited to display on a trusted platform. Again, the intention of this is prevent the reconstruction of text from repeated adjacent searches.

5.8.9 +Research

@ Focussing on the extraordinary needs of digigood research (since the normal requirements have already been dealt with)...

@ Extraordinary research requirements (determining word usage, etc.) can be met through the use of custom software operating on the contents of a digistore.

- This software would be similar to indexing and searching software, and so should fall under much the same reasoning – it provides a public service without substantially impacting the rightsholder – and thus should be allowed free of access charge (though the digistore running the program would no doubt charge for the processing time required).
 - Academic digistores might provide this service free of charge to qualified academics.
- However, custom software would run a a greater danger of infringing use, then the well checked indexing and searching software would.
 - This danger could be countered by requiring a non-infringement certification.
 - Or again, it could be countered by restricting use of the software to academic digistores by qualified academic researchers.

5.9 +Coexistence

@ This section describes how AVDS meets requirements specified in 4.6 +Coexistence.

5.9.1 +Copygood Conversion

@ Under AVDS, copygood conversion has two steps:

- Digitizing the copygood and registering it with the digigood registrar.
- Converting copygoods held by the consumers to digigood access rights.

- @ Legally, copygood conversion would be treated as the sale of the copygood to the appropriate digigood owner, in exchange for permanent digigood access rights.
- The copygood might then be retained by the digigood owner, destroyed, or (for an additional fee) licensed back to the consumer as part of his access rights.
 - If the copygood is licensed back to the consumer, that license would require that the copygood be marked as having been converted, and most likely would disallow transference – or at least commercial transference.
- @ Digitization is primarily a legal problem.
- Technical process of digitization is solved:
 - books can be scanned,
 - audio is already digitized on CDs,
 - video is already digitized on DVDs
 - Primary legal problem is the determination of the rightful digigood owner.
 - Likely this will become very complicated legally.
 - Probably it will become complicated enough to require some legislation to clarify the problem.
 - However, for textual works, the situation is basically:
 - The author holds rights to the work
 - Unless the author has contracted electronic rights to publisher
 - Of course, if the work is out of copyright, then digigood ownership is not a problem.
 - Secondary legal problem is performing digitization when the owner is unknown or unwilling to digitize the work.
 - Several ways this might happen:
 - Rightful owner is known, but slow.
 - Rightful owner is known, but unwilling.
 - Rightful owner is known, but can't be located.
 - Perhaps address is unknown.
 - Perhaps author used a pseudonym, and real name is not known.
 - Rightful ownership is in dispute.
 - AVDS would require that a work already published as copygood, must be published as a digigood.
 - While copyright law allows creators to not publish their copyright protected work, it also includes rules to ensure that once a work is published, that it remain available in the public record.
 - First sale rule combined with the existence of libraries.
 - Term limits.
 - If the rightful owner of a copygood is unknown or unwilling to digitize, AVDS would allow parties to sue to act as their representative digigood owner.
 - The legal action would determine what price could be charged for the digigood, and whether any part of that price should be delivered to the rightful owner, or held for him in escrow if the owner is unable to be contacted.
 - This requirement and approach is expected to encourage rightful digigood owners to act on their rights and digitize their works.
- @ Converting consumer held copygoods to digigood access rights:

- @ Copygood is processed by an authorized copygood conversion company, which
 - determines that the copygood is eligible for conversion
 - it has not already been converted,
 - it is not a remnant, discard, or otherwise marked as destroyed
 - determines which digigood the copygood corresponds to
 - purchases digigood access rights for the digigood from an access vendor
 - indelibly marks the copygood as converted, destroys it, or forwards it to the digigood owner
- @ If processing in bulk, the conversion company would likely proceed in two passes:
 - In the first pass it would separate convertible and non-convertible copygoods
 - Develop an itemized conversion bid, showing the discounted access price for each item
 - Allow the consumer to select which items to convert
 - Purchase and mark (or destroy) the selected copygoods
- @ Authorization of the copygood conversion company would establish that the company:
 - accurately determines conversion eligibility
 - accurately identifies copygoods and their digigood equivalent
 - acts appropriately as an agent for the consumer in obtaining the discounted access price
 - correctly marks converted copygoods
 - safeguards the privacy of the consumer
- @ Note that this process applies for both individually held and group held copygoods – though the access vendors will likely offer different purchase plans and prices for groups than they will for individuals.
- @ Since the process of converting copygoods and adding them to the digigood registrar will take years – if not decades, it will be necessary to provide a service that notifies the consumer when digigoods of interest become available.
 - Such a service would take a list of copygoods from the consumer, and immediately inform him whether or not corresponding digigoods were available. For copygoods lacking corresponding digigoods, the service would send a notification to the consumer when the corresponding digigood became available.
 - If the consumer does not already possess a list of his copygoods, he might hire a conversion company to create the list, or he might use technical means to help him create it (e.g., a handheld scanner, attached to computer with appropriate software, to scan ISBN numbers of books).
 - Note that this service could help to drive digitization – especially of out of copyright copygoods.
 - Consumers could specify a digitization support donation for free-access items in their list – this donation would be contingent upon digitization of the work.
 - Digitization companies could then direct their attentions to free-access copygoods with the highest bids and claim the accumulated donations upon digitization. (See also 5.8.7 +Free Access Digifacts.)
- @ As for pricing, AVDS again refrains from imposing requirements.
 - However, it is expected that market forces would encourage digigood owners to offer substantial discounts on access purchase through conversion.
 - The consumer already has a copygood, and thus has a reduced need for the digigood.
 - The consumer would surrender transfer rights of the copygood, thus reducing loss of sales for the digigood owner.

@ It is expected that after AVDS is well established, copygood publishers will likely explicitly include terms of conversion on the copygood.

- Such terms may include denial of ability to convert (which should be accompanied by reduction of price to reflect loss of value).
- Notices of such terms should be made obvious.

5.9.2 +Digigood Printout

@ AVDS provides support for the reverse process – creating printouts of digigoods. This was discussed in 5.5.8 +Printing.

5.10 +Protection

@ This section describes how AVDS meets requirements specified in 4.7 +Protection.

5.10.1 +Access Control

@ As with any crime, it is impossible to entirely prevent violations of access rights.

- In order to be useful to consumers, digigoods must be decrypted – and even the best trusted system can be compromised – by hardware attack if not software attack.
- However, access control systems do not have to be perfect to be useful.
 - If the access right violation level is reduced far enough, then digigoods will be economically viable.
 - Just as credit cards are viable despite a certain level of fraud.
 - Just as people walk the streets at night despite a certain level of danger of robbery and murder.

@ AVDS deploys several mechanisms to reduce the level of access right violation.

- Design is used to eliminate the need and reduce the desire of the consumer to violate access rights.
- Technical and infrastructure mechanisms are deployed to prevent casual violation of access rights.
- Policing mechanisms are used to detect and stop the sharing of decrypted digigoods.
- Structural and legal mechanisms are used to prevent the sharing of decrypted digigoods.

Reduce Desire to Violate Access Rights

@ The fundamental design of AVDS is arranged to eliminate need and reduce desire of the consumer to violate access rights:

- The consumer is presented with a simple, comprehensible and fair deal. (See 5.4.3 +Simplicity and 5.4.5 +Progress.)
- Digigood availability is guaranteed both by fundamental structure (separation of access vending from distribution) and by specific legal rules (see 5.8 +Availability).

Prevent Access Rights Violations by Individuals

@ AVDS prevents violation of access control through technical, structural and legal mechanisms.

@ Access rights violations are outlawed and subject to criminal and civil penalties.

- Punishment may include the revocation of access rights of abusing users.
 - In fact, this might be necessary to some degree in order to end the act of access protection violation.
 - E.g., if the user had published his unlocking keys to some digigood. Revoking the key would disallow his access as well as the access of other, illegitimate users.

- @ Technical prevention of casual access violation by the consumer is provided by trusted platforms (see 5.2.5 +Trusted Platform).
- @ Structural and legal mechanisms are used to secure digigood servers:
 - The certification all AVDS vendors depends in part on their ability to secure digigoods against unauthorized access. (See 5.1.9 +Access Vendor, 5.1.8 +Access Registrar and 5.1.11 +Digistore.)
 - In addition, these services are also liable under civil law for failing to adequately protect access rights.

Detect and Stop Illegitimate Sharing

- @ AVDS used technical and policing mechanisms to detect and stop the sharing of decrypted digigoods.
- @ Several mechanisms are used to detect illegitimate sharing of digigoods:
 - Network archive sites are scanned for decrypted digigoods and outlawed decryption tools.
 - Hacker organization are monitored for information on access violations.
 - Digigoods are watermarked in an effort to trace the origin of violations. (See 5.2.3 +Watermarking.)
- @ Once illegitimate sharing is detected, legal and technical action is taken to remove the material:
 - Offending servers are ordered to remove violating material.
 - Offending servers are physically shut down and/or removed from owner.
 - Offending servers are isolated from the network
- @ Note: There is something of a myth that this sort of action is impossible on the internet. In fact, a number of mechanisms exist:
 - Currently, the geographical location of any server can be determined within a matter of seconds.
 - All major nations are participants in treaties supporting the protection of intellectual property.
 - The few minor nations that do not provide such support do not have significant network connections and so do not have the bandwidth to support substantial violation.
 - If they developed sufficient bandwidth to become a haven for access violation, IP protecting nations could act to break that network connection, or use other force deployments against them.
 - Peer to peer supported violation can also be countered:
 - True peer to peer has suffers from substantial performance problems. In order to achieve acceptable performance developers have found themselves force to re-instate backbone servers – these would provide substantial legal targets.
 - Even if such large targets did not exist, small violators could be prosecuted heavily – thus providing a substantial disincentive against participating in such peer to peer schemes.

Prevent Illegitimate Sharing

- @ AVDS uses structural and legal mechanisms to prevent the sharing of decrypted digigoods.
- @ AVDS outlaws sharing of decrypted digigoods and the distribution of tools of intended to assist in violating access rights.
 - Punishment for these crimes is substantially higher than the punishment for violating access rights simply for one's own interest.
- @ Network hosting services are held criminally and civilly responsible for the posting of decrypted digigoods on their sites.
 - However, the network hosting providers are able to reduce or eliminate their liability by demonstrating that adequate measures were taken to eliminate access violation.

- @ Posted digifacts are required to include signed notices specifying ownership and allowances for distribution.
- This requirement may be applied either directly, or indirectly (as part of “adequate measures” imposed on network hosting services).
 - The notice must include more than copyright notices currently do:
 - It must specify the copyright owner, or at least the poster – and this person must electronically sign the digifact.
 - Pseudonyms might be allowed, but the pseudonym would have to be traceable to the actual person after appropriate legal action has been taken.
 - It must specify to what degree the digifact may be redistributed. Typically, this will be limited to:
 - Digifact may not be reposted at all (i.e., only original site is allowed to post digifact).
 - Digifact may be reposted and reused anywhere.
 - Note: Ideally, the digifact will be a registered digigood, for which access vendors and re-use vendors can be readily located.

Encryption Research

- @ AVDS does not outlaw encryption and other security research, though it may restrict access to it:
- Open security research provides a greater benefit than danger.
 - Security weaknesses in technical systems are often not exposed until the system is exposed to hostile review – this requires open security research.
 - This opens the door to the possibility that attackers could gain knowledge of the weaknesses while defenders remained ignorant.
 - However, while open research is desirable, it is not necessarily true that such open research requires making the results of the research available to all eyes.
 - Research results might be limited to registered security researchers.
 - Such registration should be similar to gun registration:
 - Open to all demonstrably competent individuals without criminal records.
 - Registered researchers might have to expect a closer level of surveillance over their activities than the ordinary citizen would be subjected to.
 - In particular, tools for breaking security could not be released to general public.
 - Research discussions might be limited to guarded forums.
 - Conferences
 - Online discussion limited to registered researchers.

5.10.2 +Infrastructure Protection

Attack Countermeasures

- @ AVDS provides technical, structural and legal mechanisms to protect the digital infrastructure against attacks.
- @ Caching is a fundamental to AVDS architecture.
- Caching provides protection against service, and even network failure.
 - Separation of access and distribution transactions makes caching possible.
 - Distribution charges provide incentive to develop caching at multiple levels (digistore, local servers, personal servers).

- @ AVDS recognizes critical priority levels of digigoods, services and consumers.
 - The priority level of digigoods is specified during registration.
 - Registration of a digigood as having critical priority requires:
 - That the digigood owner have authority to do so. Such authority is granted by the digigood registrar.
 - Or that digigood pass a test for criticality performed by the digigood registrar.
 - High priority digigoods are marked for mandatory caching throughout the network – even out to the consumer’s personal server.
 - Extremely high priority digigoods are marked for mandatory printing and storage at certain physical locations.
 - Some consumers will have critical priority in requesting service from digistores, access vendors, and access registrars – again, this capability will be awarded by the digigood registrar.
 - Under heavy load conditions, digistores, consumer software, etc. take criticality of both digigood and consumer into account when making and handling requests.
- @ Most infrastructure components are decentralized.
 - Access vendors, library access vendors, access registrars, digistores are all decentralized.
 - The digigood certifier is non-service component and hence, continual access to it is not required.
 - The digigood registrar is critical, and will be protected in other ways:
 - Though it acts as a single entity, it will be physically distributed, with different locations capable of acting independently of each other when necessary.
 - Since it charges a high price for distributing digigoods, commercial digistores will naturally develop to minimize digigood type demands on the digigood vendor. The resultant loose, tree like structure will reduce the impact of loss of the digigood registrar. (See also 5.1.5 +Digigood Registrar.)
 - Other high security precautions and redundancies are established to further reduce the impact of an attack.
- @ Loads are automatically distributed.
 - Digigood demands are distributed among digistores.
 - High demand digigoods would quickly be replicated to all digistores to meet demand.
 - Failure of digistores due to attack is automatically compensated for by consumer software – which would simply go to other digistores.
 - Criticality of distribution can be reflected by increasing distribution charges for non-critical information. Consumer agents would likely automatically reduce demand in response to such price increases.
- @ The digigood certifier acts as infrastructure security manager:
 - Certifies various entities – with certification depending in part on that entity’s ability to resist attack – and continue to provide services.
 - Awards critical priority posting and service requesting capability to appropriate institutions: critical governmental agencies, news organizations, financial institutions, etc.
- @ National security and policing institutions are responsible for preventing and responding to attacks on the digigood infrastructure.
 - Research is undertaken to determine possible modes of attack and develop countermeasures to such attacks.

- Action is taken to seek out and stop groups preparing to attack to the digigood infrastructure.
- Facilities with high resistance to physical attack, and backup power supplies are mandated to provide access to high priority digigoods.
- Printout and storage of extremely high priority digigoods in findable locations is mandated.
 - This is similar to mandating the provision of fire combat systems (sprinklers, fire extinguishers, etc.)
- See also Chapter ?? Civic Digics.

Attack Scenarios

@ The application of the measures described above can be understood by considering how AVDS responds to varying levels of failure:

@ Network and or digigood infrastructure is under attack, and some portion of decentralized services are down:

- Remaining servers of all types continue to function, with demand being automatically switched to surviving servers.
- If load levels reach high enough levels, then priority pricing and other priority restrictions come into effect.
- National police and security agencies respond to attack.

@ Network is up, but centralized services, and some portion of decentralized services are down.

- Most services continue to function, but high priority agencies and digigoods continue to receive greater attention from servers.

@ Some computers available, but network is down.

- Computer rely entirely on locally cached digigoods.
 - Local cache contains high priority digigoods which have marked for mandatory caching.

@ Computers are down.

- Populace resorts to printouts of extremely high priority digigoods, which by regulation have been pre-printed and stored.

5.10.3 +Privacy Protection

@ An in-depth discussion of the needs for privacy and for (strictly limited) governmental invasion of privacy is beyond the scope of this chapter (see Chapter ?? Cyberself Control and Chapter ?? Civic Digics.)

@ The AVDS system, in many places, requires the definite identification of individuals.

- The ability to perform this sort of identification is in fact, a fundamental design assumption of AVDS.
- Put more strongly, AVDS is based on the conclusion the requirements presented of a digigood infrastructure requires repeated definite identification of individuals.
- Reasons for strong identification have been described above. See in particular 4.2.1 +Access Purchase.

@ Few things in life come without any cost – with AVDS (and digital technology in general), one of the most substantial costs is the danger of invasion of privacy.

- However, this is a danger – not an inevitability. Just as AVDS implements legal and technical mechanisms to protect the security of digigoods, so it also implements mechanisms to protect the privacy of individuals.

@ Below, I examine how the design of AVDS raises dangers of invasion of privacy.

- I then describe measures taken by AVDS to limit those dangers and actively retain consumer control over consumer information.

Dangers

@ AVDS identifies users and collects personal information at many stages:

- Both digigood owners and consumers must identify verifiably themselves.
 - Verifiable identification will require a public key infrastructure (5.2.4 +Identification) that will be used to definitely identify users on a frequent basis. This system assumes the equivalent of presenting a person ID card with virtually every transaction.
- Access right ownership is recorded by access registrars – such registrars provide in depth time profiled information on the interests of consumers.
 - E.g., the consumers access to a book on explosives might be found to precede the discovery of a bomb at that person's place of work.
- Digistores also might provide deep information on the consumer's interest – potentially even deeper than the access registrar, since the digistore would record each instance in which a given digigood was fetched from the digistore.
- Since digigoods access is built around consumer identity instead of machine identity, trusted platforms must constantly verify the identity of the individual operating them.
 - Note that while today's personal are ultimately controlled by their owners, trusted platforms *require* that the control of their owner over them be limited in substantial ways.
- Posters of material to the internet are required to sign the material as they post it (unless it is already verifiably signed by another party).

@ Such information might be abused by both commercial and governmental agencies.

@ Examples:

- Companies might use such information to profile consumers, targeting advertising for their particular interests.
- Conversely, companies might decide that the consumer offers too low a sales potential and refuse to sponsor library access (in the form of advertising) by that consumer.
- Companies might use profiles garnered from digigood access records to recognize individuals with diseases, or other undesirable traits – and then discriminate against the individual accordingly.
- Governments might use such information to detect or predict likely criminal behavior.
- Governments might profile individuals for various undesirable activities – fomenting rebellion, even reading books that are secretly marked as proscribed.

@ However, the undesirability of such behavior is not entirely clear:

- Individuals might find targeted advertising to more useful than generic advertising – a man is more likely to find an advertisement for jock itch powder more interesting than an ad for tampons.
- Why should companies be required to subsidize digigoods for individuals who will never purchase their goods? Note that ultimately, the cost of such wasted advertising is paid by the consumers who *do* buy the companies products.
- The detection and even prediction of criminal behavior are certainly admirable goals – the prevention of assault and murder of thousands, even hundreds of thousands of individuals each

year would be a fantastic achievement.

Countermeasures

@ The degree of privacy desired by individuals and by society for its individuals is already the subject of passionate debate – and will continue to be debated fiercely in the coming years, if not decades or centuries.

- However, AVDS assumes that individuals do not wish their private information to be made available beyond the degree to which this is required to ensure a secure and workable digigood infrastructure.
- The measures described below are designed to meet that need.

@ Commercial invasions of privacy are prevented by:

- Privacy protection requirements imposed on digital service vendors.
 - Adherence to these requirements is checked by the digigood certifier as part of the certification process.
 - Commercial vendors are liable under civil law to consumers for breaches of the consumer's privacy.
- In contracts between consumers and the various digigood vendors, consumers are given control over the re-use of their personal information by companies.
 - In general, companies are not allowed to redistribute personal information unless that is specifically allowed by consumers.
 - Consumers control access to their personal information through online personal information services.
 - These services act as representatives for the consumers in their negotiations with vendor companies.
 - These services take an active role in defending consumer privacy interests.
 - See Chapter ?? Cyberself Control for a much longer description of personal information services.

@ Governmental invasions of privacy are limited by:

- The same technical mechanisms mandated of digigood vendors by the digigood certifier to prevent invasion of privacy by commercial interests.
- Access to consumer data held by digigood vendors require a search warrant or similar legal device.
 - Personal information may be ranked at different levels of privacy, with each level of privacy requiring a corresponding search warrant
 - Legal standards for acquiring a high level search warrant are higher than for a low level search warrant.
- Personal information services can act as representatives of the consumers with respect to invasion of privacy by the government.
 - Again see Chapter ?? Cyberself Control for a much longer description of personal information services.
- Watchdog groups and privacy advocates are expected to monitor for governmental invasions of privacy.

@ While identification is repeatedly required by AVDS, such identification may be provided in the form of a pseudonym.

- However, such pseudonyms must be traceable to an actual person after appropriate legal action is

taken.

- Moreover, the various vendors may refuse to provide certain services to pseudonymous persons (e.g., preview may not be available because of the danger of abuse).

5.11 +Consumer Representation

@ This section describes how AVDS meets requirements specified in 4.8 +Consumer Representation.

5.11.1 +Consumer Representation

@ The need for consumer representation can be met through a Digital Consumers Union.

- The structure of such a union and methods of building it are described in depth in Chapter ?? Consumers Union.
- The problem with building a consumers union is primarily with providing a benefit for cost

@ However, in brief:

- In order to successfully and accurately represent consumers, a consumers union must provide sufficient motivation for consumers to join the union.
- One such method to achieve this is to have the union provide a simple and useful service for consumers.
- The personal information services mentioned previously (in 5.10.3 +Privacy Protection) represent one such venue.

@ Although the need for representation by consumers seems to clash with the need for expertise in order to understand the complexities of requirements of a digital infrastructure and the tradeoffs involved in constructing such a structure (not to mention the complexities involved in connecting such a structure with current copyright law), such expert representation is possible.

- Such representation could take the form of a board of consumers selected at random from a pool of qualified volunteer members of the organization.
- Or perhaps elected by the membership.
- The members of this board would serve for a limited period of time – either being paid or serving as volunteers.
- The board members would study and listen to testimony and then render their decisions as to the correct course of action.
- In other words, the union would have a representative form of government.

@ Again, see Chapter ?? Consumers Union for more detail.

@ Such a form of a consumer representation is not a part of AVDS.

- Indeed it is the other way around – AVDS is presented as a proposal to such a body, and to the digigood creators and publishers as a potential solution the requirements for distribution of digigoods.
- Nor should AVDS, as presented here, be considered monolithic and unalterable. There are a vast number of details in it's design – most of which can be modified as the negotiating parties see fit.

6 Transition

6.1 Infrastructure Issues

@ How to achieve the desired implementation.

6.1.1 Digigood Registrar Service

- Technically, no substantial challenges.
- However, some sort of central service will be required which would likely result in a political battle – such as that over domain name registration.
 - Concerted effort on part of commercial developers and other interested parties should be applied at the beginning to prevent this issue from becoming politicized.
- Also, there's a question as to whether

6.1.2 Access Registrar Service

- Technically, no substantial challenges.
- However, some sort of central service will be required which would likely result in a political battle – such as that over domain name registration.
 - Concerted effort on part of commercial developers and other interested parties should be applied at the beginning to prevent this issue from becoming politicized.

6.1.3 Access Vendor Service

- ??

6.1.4 Digistore Service

- ??

6.2 Technical Issues

6.2.1 Reference Format

- Technically, this is fairly simple, quite similar to specifying the format of URLs.
- However, there will likely be substantial contention over the root name space – just as there is contention over the root name space of urls. (Trademark issues, etc.)
 - Trademark issues.
 - Moreover, must be dealt with on the international level.
 - Moreover, reference roots must be permanent – unlike current url roots which can expire and be transferred.
 - This is not necessarily true. Reference wise, it does not matter if bobbus.com is one company this year and another company next year – so long as works can be uniquely referenced, i.e., so long as works registered by the new root name owner do not obscure names registered by the original root name owner.
 - Perhaps any resolution of the current debate over resolution of the internet root names can be leveraged – e.g., just take that namespace and apply it to reference format namespace.
 - Full digifact references are likely to be long, so are less likely to be typed in manually, so longer root

names might be acceptable/desirable.

- Maybe, but people often type in short names, then navigate through pages/directories to the longer names – the same would like be true of references. (E.g., type in StephenKing, then navigate to “The Shining”.)

6.2.2 Encryption

- Technically, quite doable with today’s technology
- As with any security critical protocol, implementing this will substantial work and testing, but none of the problems are of the “we don’t know how to do this” type.
- Encryption
 - Unbreakable encryption appears to be possible and is publicly available.
 - Possible to deny unauthorized parties access to given material.
 - Possible to deny governmental authorities access to material.
 - Publicly available. (Genie is out of the bottle.)
 - Probably not possible to prevent authorized users from abusing their authorization.
 - Printouts can be scanned, screens can be accessed, sound output can be recorded.
 - However abuse can be made more difficult.
 - Specialized hardware (information appliances, etc.)
 - Current general purpose computers are probably not protectable.
 - Protection might require measures that could compromise privacy, so some sort of agreement needs to be reached on this.
 - Privacy protection groups tend to scuttle such measures.
 - Reduce motivation to abuse.
 - Technical copy protection is breakable, but perhaps not easily.
- Main problem with encryption is the implications for public safety – danger of criminals unbreakably encrypting their files and transmissions.
 - But this level of encryption is already publicly available (PGP), so even if unbreakable security is outlawed, criminals will have it and be able to use it.
 - OTOH, outlawing it would at least reduce the level of secret transmissions and give police a tool to restrict law breaking. (Like Al Capone being jailed for tax evasion, suspected criminals could be jailed for using unbreakable encryption.
 - Note that the hardware identification approach described in earlier chapters will eliminate one of the back doors for breaking encryption – namely capturing keystrokes of a password as the user types them in. In the hardware ID approach, there is no password – an active device on (or in) the user’s body secures the keys. (OTOH, there are ways to break this approach as well, which might be themselves countermeasured, etc. Trusted Platforms are likely to be difficult to tap.)
 - This issue is discussed at length in a later chapter. For now it’s sufficient to note that the encryption used might be either breakable or semi-breakable (key escrow).
 - Moreover, an advantage of the digigood infrastructure described here is that it compatible with changing legal infrastructures. E.g., if the legal requirement for breakable encryption is relaxed, or vice versa, such modification can be readily incorporated into the infrastructure without loss of registered ownership of digigoods to the owner.

6.2.3 Encryption Schemes

- Unique key encryption. Each sold copy of digigood gets a unique key. User might store that key separately, or it might be encrypted with the user's personal key and stored on disk.
- Unique key encryption presents dangers of unique encryption (government would prefer key escrow of some sort). This does not occur for DVDs which are standard items manufactured at some plant.
- Larger infrastructure costs. Encryptions must be carried out on demand at

6.2.4 Encryption Approaches

- No encryption
 - May rely on secondary income streams
 - fundamentally unfair
 - often not available (no toys associated with "Digital Needs" book!)
 - advertising: annoying, customer would rather do without
 - fosters attitude that content should be free
 - Can't be used for non-good digifacts (e.g., corporate documents, private conversations, etc.)
 - Can be accessed by anyone
 - Very susceptible to piracy including 1 to 1 piracy (copying to a friend or relative).
- Universal Encryption
 - e.g., DVDs
 - tied to buying a copygood, so loses much of the benefit of digigoods
 - Can't be used for non-good digifacts (e.g., corporate documents, private conversations, etc.)
 - Once the key is broken, it's broken for everyone. All past content is now accessible.
 - Moreover, all future content is broken until people go through the capital intensive process of replacing the old universal key (which is likely encoded in hardware).
 - Replacing the old key would make all old content inaccessible (thus ruining a collection of DVDs). Possibly new keys might be added instead of replacing the old key, but that's still capital intensive.
 - Legal solutions seem to be outlawing particular knowledge (e.g., the code key, or software to implement the code key). Since this knowledge may not occupy much space (13 lines of code), it is likely to be hard to do.
 - Breaking the system requires clear, extraordinary effort, which may be outlawed.
 - If the user basically gets a good break that allows all fair use at a reasonable price, then he is less likely to feel entitled to break the rules.
- Custom encryption
 - Different key for each copy of good
 - There are a variety of solutions here, all of which require some degree of computerization.
 - Custom burn media in store (probably too time consuming)
 - Just burn customer encrypted key into media (media can only be used once)
 - Write key onto customer's smart card
 - Might encrypt key so that only the customer's machines (not customer himself) can read them
 - Machine specific encryption raises a problem when multiple users can access that machine.
E.g., one call center worker might store his music files on it, and then another worker in a later

shift might access them. Individually encrypted files makes more sense.

- Customer ID'ed encryption
 - Somehow customer's ID is associated with good.
 - Increases accountability if customer's ID is inextricably associated with good.
 - Allows convenient permanent purchase of goods. Pay IP owner once, then just pay digistores for distribution.
 - Technological change resistant. No matter what happens with encryption standards and various technologies, there's a clear record that you've bought access to that good
- Suppose that I encrypt some digigood, then hand you the key. You can access it so long as you have the key. If you lose the key, that's your loss.
 - I lose some of the efficiency of an digistore. I now have to store all of those encrypted files somewhere – I can't just re-get them from a digistore. On the other hand, if I have my own computer system acting as a digistore, then I might be able to retrieve them from my own machine.
 - This system doesn't work for varstreams – e.g., a subscription to NYT.
 - So, then I can copy the encrypted file around on my own file system
 - Suppose that I post the encrypted file somewhere on the web, and then publish they key elsewhere.
 - But this can happen under my system as well. And a valid key system might specify that the encrypted file can not be posted in a public place.

6.2.5 Identification and Public Key Infrastructure

- Technically, quite doable with today's technology
 - Identification done using PKI, which is a known technology.
 - The consumer side of identification has been described in earlier chapters on hardware.
- Raises privacy concerns.
 - Anonymous

6.2.6 Trusted Platforms

- Technically, trusted platforms especially within general purpose computers may require substantial modification to existing hardware and software.
 - Essentially, general purpose computer are built at a fairly basic level to be open – in particular I/O streams, which will carry the decrypted content for final display, are currently easy to access (at least if the user has complete access to machines, which their owners do).
 - The modifications are doable, but will require care, and will touch substantial numbers of systems (base computer, chip sets, cards, video and audio displays, printers).
 - Thus there will be a substantial capital cost associated with turning general purpose computers into trusted systems. (At least this will give computer manufacturers something to do, now that the PC market is saturated!)
 - This modification may well affect performance. Such a performance loss will be offset by increasing computer power – still this relative loss will need to be justified to users. (Though the performance loss, if it occurs will probably be restricted to trusted mode.) Again, I'm being speculative about a performance loss – it may not occur.
 - This modification will also take time. Time to develop and time to deploy systems to users – which will take time given the currently decreasing turnover rate for PCs.

- TPS may also require modifying computer architecture in a way to make to the computer unique and identifiable. This could obviously be used for a gross invasion of privacy.
 - Previously proposed TPS tie digigoods to machines, while my digigood infrastructure ties digigoods to persons (and thus uses personal ID).
 - Of course, personal ID is a privacy issue in itself, but it may be a trusted platform based on personal ID does not require machine specific ID, and thus raises no privacy issues so long as the personal ID is not used. I.e., by itself, the machine might not be identifiable.
 - *If* machine ID is required, then its presence will be a substantial source of contention.
 - Previous efforts to ID machines have raised substantial objection from privacy advocates and the press.
 - Unique identification in Pentium III CPUs.
 - Unique serial number identification of hard disks.
- This is one of the most time-critical issues in deployment of the digigood infrastructure described here. Deployment will take time, and yet consumer agreement must be obtained first or else there will be strong popular objection to the development of trusted platforms.
 - This is a case in which hardware vendors cannot pursue “business as usual” – i.e., develop the hardware and then let the consumer decide.
 - There must be a public discussion, with credible representatives of consumers – not just “consumer advocates” or special interest groups who claim to represent the public, but in reality represent some small portion of the public who care deeply about a few issues (e.g., privacy advocates, etc.)
 - Digital consumers unions are discussed at length in a later chapter.
- Other approaches:
 - Limited Trusted Platform Deployment
 - Hardware can be developed and deployed on a selective basis (possible to corporations), who might have more advance interest in secure systems than the general public.
 - Hardware could be developed and deployed to the general public – but lack an insertable hardware identification element (some small ID chip). Without the ID chip, the computer would pose no identification risk, and so would not be a threat to the privacy of the consumer. Since the ID chip could be easily added, converting semi-ready TPS computers to fully ready computers should be an easy operation.
 - While these approaches lessen the privacy threat of identifiable computers, the substantial investment on the part of manufacturers would raise concern among the privacy-sensitive (paranoid). Again, these concerns are best addressed openly, even loudly, at the beginning of the hardware development process.
 - There is also a bit of chicken and egg problem here. Reducing the spread of trusted systems would reduce their likelihood of being used, and thus would reduce the investment in the rest of the digital process.
 - Security-level Factoring
 - Hardware systems might be rated at varying levels of security – digigoods with lower security levels could be made available on these less trusted systems. I.e., higher hardware security means higher digigood access.
 - Another approach would be to provide a financial incentive to user to switch to hardware with a higher security level. E.g., lower security levels increases the risk of piracy, and thus the cost of

- policing – users might be charged for more for accessing digigoods on hardware systems with lower security levels.
- Non-general purpose viewers
 - Special designed devices (ebook readers, digital video players, etc.) can be more easily deployed with higher security levels, and would not suffer the same level of privacy objections that hardware IDed general purpose computers would.
 - This allows a more gradual and voluntary deployment, and it builds consumer desire for turning general purpose computers into trusted platforms.
 - This could be done *now* – switching current hardware e-book readers to the digigood infrastructure described here could be done rapidly, thus providing consumer experience with this system in the near term (probably within a year of beginning development effort).
 - Military as sponsor for trusted systems.

6.2.7 Consumer Software

- ??
- Software for resolving reference and downloading file from digistore
 - Digistore selection should be intelligent: it should seek least expensive download
 - Agent should be easy to use, but configurable
 - May use an external agent (e.g., go to an agent and ask it to find the cheapest source)

6.3 Legal Issues

6.3.1 Copyright Law

- @ The foundational principles of AVDS are radically different from those of copyright.
 - Cognigood owner surrenders rights of reproduction, distribution, etc.
 - Cognigood owner gains explicit right to control the sale of access rights to the cognigood.
- @ Because AVDS is so fundamentally different from copyright law, legally it cannot be implemented as an extension of copyright law – instead it will be necessary to establish it through a complex set of contracts.
- @ AVDS cannot be established immediately in civic law
 - Legal system is too slow to produce this fundamental a change in civil law – initial versions of the AVDS legal infrastructure is needed within a few years.
 - ? AVDS is too complex and untried – it will no doubt require tinkering in order to work well
 - ? Digital technology is too much in flux.
- @ The size of AVDS commercial and legal infrastructure is daunting, but construction can be carried out in pieces, with the expectation that the structures involved will increase in formality over time.
 - Lessons should be taken from the development of the internet. Some institutions, such as DNS, were performed initially in an (extremely) informal fashion, then later formalized.
 - A similar development approach could be taken with the commercial and legal infrastructure of AVDS.

6.3.2 Publication

??

6.3.3 Moral Rights

6.3.4 Other

??

6.4 Stakeholder Issues

6.4.1 Consumers

- Provide a financial incentive to consumers to move to systems with higher IP protection. Extreme case: make some material unavailable on systems with insufficient IP protection.
- @ Even after a digigood system is in place that meets the access, distribution and availability requirements described previously, consumers will (to some degree) continue to demand copygoods
 - Tradition: Consumers are used to practicalities of copygoods. (Simple buy-it-own-it paradigm.)
 - Greater privacy.
 - Need will probably fade over time as infrastructure builds and as consumer become used to access-rights approach.
 - Copygood deal:
 - First sale: consumer can resell copygood.
 - Consumer has to pay for each copygood, even if they represent the same cognigood.
 - Distinct copygood must be associated with each used instance – often by actual insertion of copygood.
 - If danger of piracy is higher, then copygoods may cost more than digigoods to make up for increased danger of piracy. (E.g., DVDs with cracked encryption.)
 - Copygoods may cost more because of sales lost to resale.
 - No replacement if copygood is lost, stolen or destroyed.
 - Damaged copygood might be replaced – but probably at a charge.
 - No replacement for normal wear and tear. (E.g., scratch in CD, or worn out book.)
 - No automatic updates, etc. (Though these *might* be made available for free over net as diffs – manufacturer is not under any obligation.)

6.4.2 Advertisers

- I speculated above that advertising might be hit by a system in which all uses are trackable and payable.
- Thus, one might expect advertisers to fight such a system.
- However, the suggestion is pretty speculative (advertisers have a number possible options, including paying (directly or indirectly through rewards) consumers to watch advertising, so this threat does not seem large enough to motivate them.
- Also, their leverage is limited since they do not own the content, distribution technology, or distribution channels.

6.4.3 Decline of Advertising?

- As consumers move to more direct purchase – perhaps specifically choosing to avoid the annoyance of

advertising, and as costs of distribution drop, advertising venues might begin to disappear. If a consumer listens entirely to subscribed and purchased content, then advertisers might simply lack access to his attention.

- Advertiser reaction
 - Product placement in video might be pushed more strongly. (A consumers union might react by requiring video producers to forego accepting money for product placement – or they might demand a discount for video that included product placement.)
 - Instant audio/video advertising. Even if you listen to pre-recorded music or video, advertisers might subsidize your purchases – or they might pay directly for your time.
 - For example, imagine commercials that only came on when you hit the pause button (and which was bright enough to respond to whether or not you were physically present, and/or had the mute button pressed).
 - More public advertising? On the side of cars, buildings, clothing, etc.
 - Advertisers paying people directly (instead of just subsidizing various items) to listen to advertise. Payment might take the form of general discounts at various stores, etc.
 - Turn advertising into entertainment. (BMW movies.com?)
- Review services might thrive – especially if they can automate recommendations in in-store conditions (helping you select between two product based on quality, personal desires, current price, and expected future shopping opportunities, or directing you to particularly good specials that you would not ordinarily consider). Such services might help cause the demise of advertising anyway. It could even be programmed to “advertise” good purchases to you!
- Development of un-marketed goods. If advertising doesn’t pay, and if review services are widely available, then don’t spend money on advertising! (Either reduce the price or spend more money on quality.) Since non-marketed goods would be cheaper, even people who endure advertising might purchase non-marketed goods. Thus marketing might not be worth the cost and consequently be abandoned (or drastically reduced). Thus, there would be less advertising dollars available for financing various entertainments.
- Impact might be substantial – perhaps a move away from a consumer culture. (Of course, this might strongly impact the economy – so that would not necessarily be an entirely good thing!) But surely less waste would be a good thing – people would find other ways to spend their time. Again, one might self-program commercials, say for playing sports, various ethical behavior.
- These seem like pretty radical ideas – but given the specified digigood infrastructure, a real reduction in amount of advertising seems quite possible, even probable. And that this would have a substantial effect is pretty credible.
- Never underestimate the power of human stupidity!

6.4.4 Book Industry

- Technical
 - Converting text to digital format is technically accomplished. This is not a factor.
 - For some applications, digital text has already succeeded wildly – especially news.
 - Digital market is limited by quality viewers (low resolution, high weight, high cost, and lack of portability and “instant on” quality of physical books) and by lack of acceptable good business model (no guarantee of permanence of access rights, access limited to single piece of hardware).

- What do publishers do now that disappears in digital age?
 - Physical publishing and packaging
 - Distribution (send books out, accept returns)
 - This accounts for what percent of cost of publishing?
 - This accounts for what percent of employment by publishing?
- What do publishers contribute in digital age? (Assuming digital cognistructure described above.)
 - Handling of access-rights purchase
 - Pre-selection of good authors.
 - Editing
 - Advertising
 - Help finance policing of piracy. (Direct plus advertising and anti-piracy PR)
- Transition
 - ! But all of post-digital uses can readily be farmed out to outside agencies.
 - As bulk of business goes away, stature of publisher may reduce to partners, or even just hired hands for authors. (Publishers would have their greatest utility when dealing with new, non-established authors.)
 - Presumably if current publishers fail to accommodate authors, especially once digital books become acceptable to most people, then new publishing houses will spring up that do accommodate authors.
 - Transition of existing libraries: For many older books, publishers do not hold cognirights, but for recent books (past 5-10 years) they do to varying degrees.

6.4.5 Copyright Office and Library of Congress

- Both groups should continue unchanged or will grown in scope under new system (depending on whether they serve as digigood registrar and/or access registrar).
 - I'm inclined to think that LoC is natural for digigood registrar role.
 - However, access registrar might be better handled by private company.
 - Perhaps it would be semi-public, funded by digistores.

6.4.6 Music Industry

- vs. Book Publishing
 - No technical problems
 - Digitization is solved. Several protocols are available. Playing through computers is acceptable (though not without problems – mainly due to lack of efficient play, lack of instant on features). These problems are solved by portable MP3 players. However, networked stereo component MP3 players have yet to appear(?).
 - Networking is completely solvable.
 - Lack of trusted hardware is main barrier for music industry.
 - Non-technical
 - Main music publishers own large libraries of music recordings(?) This is substantial source of revenue and will become their dominant strength in the digital age.
 - Rights clearance is important for broadcasting and re-use of music (background for commercials, etc.). However, this can be automated or handled on behalf of artist by rights clearance houses.
- Recent Developments

- Napster
 - exploded demand – for free music
 - legal rulings against
 - transformation to music broadcasting?
- Gnutella, etc.
 - Peer to peer communications, harder to trace and prosecute.
 - Problem is that the advantage of peer to peer is overstated. Location and download are real problems, which means that in effect backbones have been put back in. These make fatter legal targets.
 - ISPs can be targeted, who in turn can demand that users not engage in file sharing, and terminate their contract if they do. ISPs who fail to take action against abuse occurring on their network will become larger legal targets (they lose the defense of taking adequate action).
 - Moreover, end users can be targeted, as Metallica did. While the cost of going after small abusers may be high, making examples of a few of them would cut down on file sharing. (Having your neighbor pay \$10k for sharing a few files is a powerful incentive against sharing files yourself.)
- Secure Digital Music Initiative (SDMI)
 - Technical problems. Watermark technology broken by several groups.
 - But basic problem is that music industry just doesn't seem that anxious to get into digital world – they're being dragged into it by Napster, etc. In any case, it's not moving very rapidly.
- Digital Music Broadcast
 - Several groups are pursuing this.
 - Bypasses encryption issue to some degree because music is streamed. (But obviously, this should still require encryption – non-encrypted streams can be intercepted.)
 - Not clear how this business model is going to work out. It's basically a subscription approach.
- Transition
 - Expect that publishers will move towards being partners and/or hired hands (aside from their use of existing libraries).
- Transition: ASCAP
 - Current
 - Bill bars, restaurants and other establishments a rate based on size(?)
 - Distribute moneys according to estimates of number of times tracks are played.
 - Bars that have the technology would use a subscription or per-play system instead.
 - Would probably go through some subscription service (possibly ASCAP, but could just as well be anyone else licensed by rights vendor).
 - Summary: ASCAP would likely fade away to be replaced by technically efficient and accurate rights clearance. (Or it might transition to this role itself – but probably it would have to accept competition.)

6.4.7 Audio Broadcast

- Advertising supported broadcast is essentially a rights clearance problem, and is essentially solved – digital technology will not change this significantly (at least as far as consumer is concerned).
- Recording is generally not a problem

- Only a few of tracks of given audio CD are broadcast
- Insufficient pre-announcement of audio tracks being played
- Relatively low quality of broadcast audio signal
- Digital broadcast audio?
- Has been bypassed by internet based copying
- ! So, I'll skip further consideration of recording audio broadcasts.
- OTOH, caching of audio news (and possibly entertainment) shows would probably be useful and efficient – especially for commuters.
- ! However, we can assume that solution for this system would be much like solution for video broadcast, so there's no need to go into the complexities here.

6.4.8 Advertising Supported Internet

- vs. Ad-blocking software
 - Outlaw ad-blocking software?
 - Move content to trusted viewers (which don't allow ad-blocking)
 - public outcry unless users have a way to avoid ads (nuisance and invasion of privacy)
 - Subscription or access-purchase would bypass ads (thus removing nuisance for a fair price)
 - Semi-privacy obtained by pseudonymity

6.4.9 Video

- General
 - Video is limited by bandwidth availability. Solutions are available for supplying bandwidth, but they're expensive in one way or another (infrastructure costs and/or time to deliver). This limited bandwidth problem will reduce the effects of digital transition since broadcasting, theaters and video rental businesses will still have advantages.
 - Also, high quality video production is still expensive, requiring large numbers of talented workers (writers, directors, producers, actors, special effects, editors, etc.) - this will strongly reduce the effect of transition to digital.
 - Probably largest effect will be on independent television producers. Small high quality productions will have longer audience lives. There will be a greater likelihood that high quality shows will be continued. Less frequent production rates (e.g., an "episode" every two months or so might be acceptable).
- Existing Venues
 - Movie theaters
 - Broadcast television
 - Cable Television (normal, plus pay-per-view)
 - Satellite Television
 - Video rental
- Alternatives
 - Customized delivery over internet
 - Customized delivery over cable or satellite (should be cheaper if consumer was willing to wait up to a day – this would allow delivery in otherwise low usage time, plus multiple users could be served simultaneously). Cable would have a substantial advantage over satellite here because it would be

more physically fine-grained. OTOH, cable reception is limited in some areas and inferior to satellite. OTOH, there are other local broadcast options such as low altitude satellites, and high altitude automated aircraft satellites.

- Customized physical delivery.
 - low tech. Effective for low consumption rates (1-2 movies per week)
 - time delay for delivery, but this could be made small (next day postal delivery) by printing and mailing locally
 - alternatively, users might pick up their order at local blockbuster store
 - might recycle disks (probably not necessary – you’re talking about a little plastic and a little metal foil)
- Alternative delivery methods fit into access purchase/rental + digistore model.
- Movie theaters
 - Probably continue at pretty much current level.
 - Movies are safe public venue for dates, and they provide people with an excuse to get out of the house, so they’ll probably continue to have a strong appeal.
 - They’ll probably maintain their current first release status, with a 3-6 month lead over home viewing.
 - So no reason to resist new model.
- Television (Broadcast, Cable, Satellite)
 - Will move to merger of current advertising supported model and digistore model, probably moving further towards digistore model over time.
 - No reason to resist new model, so long as can transition from one model to the other.
- Video Rental Stores
 - Probably phase into other delivery methods (custom printing – order from blockbuster on the web, then either pick up at local blockbuster store, or receive in mail) As cable meets demand though, video rental stores would probably disappear.

6.4.10 Video: Mixed Advertising and Digistore Model

- No significant change for non-recorded broadcasts. Rest of this deals with recording technologies.
- Corruption of implicit deal between broadcasters and viewers
 - Deal is clearly “watch these commercials and we’ll broadcast interesting shows”
- Utility of Recording a Commercial Suppression
 - Time shifting
 - Remove annoyance of commercials
- Technical
 - VCRs
 - PVRs (Personal Video Recorders)
 - Personalized Advertising
 - Commercial advance
 - vs. Post-production commercial placement
 - vs. shared screen advertising (would be damned annoying, but possible)
 - Magnavision copy protection system
- Legal story

- Broadcasters buy right to broadcast from copyright holders.
- Broadcasters have right to make ephemeral copies of material in course of broadcast – they do not hold general copying rights.
- Advertisers pay for ads for certain days and for certain shows. The utility of those ads will decrease over time – so long term storage of taped shows is against their interests. Also, it would be against advertiser interests to not be able to specify which shows they wish to show their ads in. Also, if you could specify the audience for the ads, some audiences would be much less interesting to the advertisers, so they might not be willing to subsidize that audience.
- Supreme court decision allowed users to time-shift shows.
- However, some broadcasts are protected by anti-copy technology, and VCRs are required to respect that anti-copy signal.

6.4.11 Collection Agencies

- Agencies which collect “tax” on copying equipment, which is then distributed based on some estimation of usage between rightsholders.
- E.g., for photocopiers, CD-burners, ASCAP, etc.
- Expect that this will disappear in digital age, to everyone’s pleasure.

6.4.12 Software Publishers

??

6.4.13 Libraries

- Digitization of existing libraries should be a substantial business for a period of ten years or so, with a slower business in following years.
- Public donations and projects could finance the conversion of material of public interest.

6.4.14 Public Libraries

- Utility of libraries
 - Access to out of print books
 - Digital books never go out of print
 - Low cost access to books
 - Short term rental of books from copyright holder
 - Subscription to online libraries (i.e., not physical libraries that are online, but digital libraries accessed over the network)
 - Perhaps children could be awarded reduced cost subscriptions (at least for educational material).
- Repository for historical literature (previously printed books)
 - Out of copyright works can be digitized and made available online (Gutenberg project)
 - In copyright books can also be transferred, but there is difficulty of contacting rights holders and securing the rights. This will probably take time and legal action (e.g., act of congress to simplify the proceedings – sales might be held in escrow pending legal resolution)
 - So, there will be a transitory value here.
- Network access for those who otherwise can’t afford it
 - Network access is inexpensive, and probably will grow more so as computers integrate with home

devices. Even low-income families will often have video-game systems, and these should be capable of full network access.

- This may continue to be useful for children in low-income homes. Libraries can provide escape for children seeking to escape from poor home environments. This might best be provided through schools.
- Electronic library access for those who can't afford subscription fees.
 - This might be provided over the network instead of through physical facilities.
 - This is pretty direct charity – those who can afford information have already purchased it, so it's only useful to those people who are too poor to afford purchase. There is likely to be resistance to such direct social welfare. OTOH, this might be handled by an extension of the big brother/sister program, or otherwise handled by voluntary charity.
- Projection
 - Libraries will decline gradually after introduction of good reader technology and introduction of desirable pricing scheme for on-line libraries. As patronage drops, libraries will attempt to repurpose their physical facilities. A debate will occur in regards to economic division – poor have a greater use for libraries than the wealthy do; however the poor will not use the libraries enough to justify their continuance (for the most part). Given the generally liberal nature of library employees and bureaucrats, and their status as government employees (in most cases), the debate will be loud. Libraries will drag on for a while, but eventually die as public support fades.

6.4.15 Corporate and Organizational Libraries

- These exist for fairly specific commercial reasons, and will probably be replaced by electronic versions which are much cheaper to maintain.
- One can expect businesses to arise to assist in the conversion of existing corporate libraries.
 - Handle conversion of licenses (corporate digigood licenses will likely be subscriptions which take number of concurrent or peak users into account)
 - Make sure that digital versions of texts are available. Digitize and register texts as necessary.

6.4.16 Free Access Digigood Providers

- People who are willing to provide free-access digigoods for prestige or public benefit reasons.
- This would be facilitated because easy distribution would be assured.
- Tendency to produce reams of garbage would be offset by small registration, storage fee.
 - This would presumably take the form of a one time fee for registration and storage at Digigood Access Vendor.

6.4.17 Privacy Advocates

- E.g., Privacy groups, libertarian groups, freedom of information
 - Privacy protection groups as counter to developing digigoods – they refuse to allow any developments that might compromise privacy – even when consumers in general are willing to accept that risk.
 - vs. Consumer demand for privacy
- ??

6.4.18 Free Information Advocates

- Technical Attacks and Action
 - Attempt technical attacks on digigood infrastructure
 - Provide software to users for subverting TPS.
 - Host free copies of decrypted digigoods
- Raise attention through press
 - Raise “fair use” issues. (Often misinterpreted.)
 - Part of the point of the digigood infrastructure suggested here is to counter such points by suggesting a rational, consumer oriented system for handling digigoods. I.e., current system should be replaced with a system that is both simple and fair to the consumer.
 - Raise issues of abuse of TPS by totalitarian governments.
 - Frankly there’s a limit to what free countries can do about this.
 - Loose laws on our part in no way guarantee loose laws in totalitarian countries (witness China, Cuba).
 - Loose technology in our country does not guarantee loose technology in other countries. China is a huge market – even if they can’t develop restrictive technology themselves, they can pay software developers in other countries to do it for them. (E.g., “Great Firewall” of China being developed and deployed by western companies.)

6.4.19 Lawyers

- Looks like there’s a lot of work for lawyers under this scheme:
 - Formation will probably be contract initially, but might migrate to civic law later.
 - This seems unlikely – if contract system works, then why change it?
 - One reason might be that some parts of society might not benefit from contracts, thus laws might be passed to extend useful contracts to general public.
 - Contract-creating lawyers should keep this inevitability in mind.
 - Legal construction of various agents and the nature of the contracts between them.
 - consumers and access vendors
 - consumers and access registrars
 - consumers and digistores
 - authors and access vendors
 - access vendors and access registrars
 - etc.
- Privacy law.

7 +Generalization

@ In this chapter, AVDS has been presented as a solution to the requirements of accessing and distributing digigoods. However, broader requirements were kept in mind during its development, and hence its application can be generalized significantly.

7.0.1 +Property Generalization

@ From digibobs, we can move to consideration of cogniprops.

- This generalizes in two ways:
 - We move from digital to intangible ideas – independent of either digital or physical manifestations of those ideas.
 - We move from property to which access can be sold, to intellectual property in general (e.g., patents, trademarks, trade secrets, private papers).

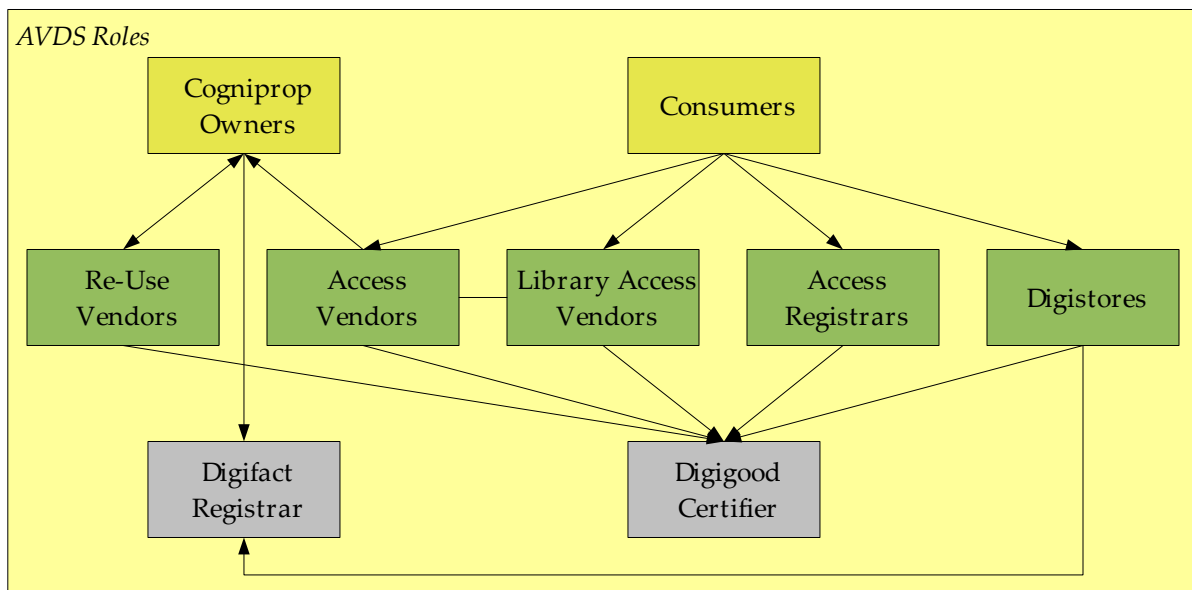
@ Under AVDS, this generalization is recognized by generalizing the role of digigood ownership to the role of cogniprop ownership.

- Cogniprop ownership is achieved by either creating the cogniprop (perhaps indirectly by hire) or by purchasing the cogniprop from the previous owner.
- While AVDS recognizes cogniprop ownership, it is only concerned with that aspect of ownership that involves the registration, access control and distribution of the derivative digifact(s).

7.0.2 +Digifact Generalization

@ From concern with registration, access control and distribution of digigoods, we can move to similar concerns for digifacts in general.

@ This generalization will be described in Chapter ?? Digital Secrets.



Drawing 2 Generalized AVDS Roles

8 Summary

@ Here's a summary of the major points in this chapter.

8.0.1 Requirements

- Strong ID required
- Encryption required – probably with ID information, and probably with some form of decryption allowed by the government.
- International policing of the net will be required.

8.0.2 Action

- Need for consumers union.