Geospatial Digital Rights Management

Cooperative Agreement 03HQAG0151
Final Report
March 2006

Federal Geographic Data Committee (FGDC)
GeoData Alliance
Open Geospatial Consortium, Inc. (OGC)

Preface

What is Geospatial Digital Rights Management (GeoDRM)? Digital rights management involves the use of technology to manage access to digitally stored and managed information. In other fields—think of the entertainment industry, for example—digital rights management is primarily concerned with protecting intellectual property by preventing alteration and uncompensated distribution of electronic files (media). In health care, the primary concern is to secure individual privacy' while facilitating access by attending medical professionals. The geospatial community, in contrast, often assembles data from a variety of sources for the express purpose of manipulating (classifying, altering) the data to create new information. And the geospatial community differs from other fields in that some suppliers (federal government agencies, for example) are more interested in enabling widespread distribution of data than in receiving monetary compensation, while other suppliers (businesses) are as concerned with compensation as with distribution. The possibility of using technology to manage data licenses, so that different uses are enabled at different prices (including attribution rather than money), is intriguing. And the possibility of ensuring the integrity of the data benefits both suppliers and users of data.

Thus the purpose of GeoDRM and of this cooperative effort is to enhance effective and equitable flow and beneficial use of geographic information. This cooperative effort seeks to advance the standards of practice for distribution of geodata through considered implementation of model policies, distribution agreements, and rights management specifications.

This report, a joint effort of the FGDC, the GeoData Alliance and the Open Geospatial Consortium, places GeoDRM in a technical and policy context of ongoing efforts to improve the flow of geographic information.

The primary audience for this report comprises private and public sector geospatial managerial and technical professionals on the leading edge of innovation.

We hope that leaders of allied digital rights management standards and initiatives will also find this status report useful, and that it will facilitate mutually beneficial information exchanges.

Finally, this report is also undertaken to satisfy a contractual requirement by documenting for USGS program officers the progress to date on the Cooperative Agreement for the Development of Open Digital Rights Management for Geodata.

Foreword

The publication, discovery, access and use of information, particularly geospatial information, has become an increasingly complex topic for many individuals and organizations, whether their interest is in serving the public interest or in satisfying private sector and consumer needs. Just as the internet has opened up new avenues for access to and sharing of geospatial information, digital access via the web is driving new challenges in the handling of information rights.

Today, information exists as a freely, publicly available resource from governments and other suppliers. It can also be purchased for a fee or can be made available only to specific users, with limitations on further distribution. All of these conditions exist in today's global information marketplace, and whether we view these trends as good or not, we nevertheless must have information tools that can be used under all these conditions.

CIESIN and other research organizations that produce and use geospatial data cannot avoid the obligation to accommodate (and often to assert the need for) rights to geospatial information. At times, research progress is slowed by the lack of technologies and policies that could normalize procedures involving management of these rights. As a member of the Board of Directors of the Open Geospatial Consortium, I have had ample opportunity to see the importance of these issues in academia, commerce, and government and how consensus standards can be developed and employed to address them.

This report documents an excellent beginning regarding activities designed to advance Geospatial Digital Rights Management (or GeoDRM) policy and technology initiatives. I commend the cooperative spirit and activities of the Federal Geographic Data Committee, the USGS National Geospatial Program Office, and the members of the Open Geospatial Consortium and the GeoData Alliance. Their joint commitment to this project illustrates the value of developing networks to accomplish shared goals. Working together, we can advance the vision of current and accurate geospatial data contributing locally, nationally, and globally to economic growth, environmental quality and stability, and human welfare.

Roberta Balstad
Director, Center for International Earth Science Information Network (CIESIN)
Columbia University

Table of Contents

Executive Summary

This report summarizes the progress to date on the Cooperative Agreement for the Development of Open Digital Rights Management for Geodata.

The introduction to geospatial digital rights management (GeoDRM) includes two workshop presentations, one on the technology of digitally managing rights and one clarifying how geospatial DRM is unlike DRM for other content.

The work of the Open Data Consortium in developing a model data distribution policy is briefly discussed.

This report also includes the full text of a USGS Open File Report which includes an example of a rights expression language (REL) capturing the elements of a data distribution agreement.

Perspectives on policy and technical aspects of GeoDRM are included, and next steps are identified.

Geospatial Digital Rights Management

Enhancing effective and equitable flow and beneficial use of geographic information

This report, a joint effort of the FGDC, the GeoData Alliance and the Open Geospatial Consortium, Inc. (OGC), provides background about Geospatial Digital Rights Management and places GeoDRM in a technical and policy context of ongoing efforts to improve the flow of geographic information.

What Is Digital Rights Management (DRM)?

The first three appendices to this report provide background to the discussion of geospatial DRM; they introduce the concepts of rights management, digital rights management and rights expressions languages, and geospatial digital rights management:

1. *An Introduction to Rights Management Technologies*, a presentation to the GeoDRM workshop held 24 May 2004 in Denver, Colorado by Brian A. LaMacchia, Software Architect at Microsoft Corporation;
2. *Geospatial Digital Rights Management*, USGS Open-File Report 2005-1086, written by Daniel J. Wright. This report includes an example illustrating the use of Open Digital Rights Language (ODRL), one of many Rights Expression Languages (RELs), to capture data distribution agreements;
3. *GeoDRM - Geographic Digital Rights Management Workshop*, a presentation made to the GeoDRM workshop held 24 May 2004 in Denver, Colorado by Todd S. Bacastow.

The State of Geospatial Data Exchange

The opportunity to exchange geospatial data depends on two main factors:

1. some sort of catalog that identifies available data, along with sufficient documentation and standard formats
2. agreement on the terms and conditions of the exchange.

The Federal Geographic Data Committee (FGDC) activity to establish *Clearinghouse* and its activity to develop standards for metadata address the first point. The terms and conditions of the exchange, item two, traditionally differ from transaction to transaction, and are presently captured in legal documents that do not automatically accompany the data during exchange. The OGC Working Group (WG) on GeoDRM seeks to extend existing technology for digital rights management to the case of geospatial data.

The following sub-sections provide more detail on the present state of each of the topics.

Available Data

Topics in this section include catalogs and formats. Examples of catalogs include Clearinghouse, Geospatial One Stop and GSDI. The word format is here used as shorthand for formats, projections and datums.

Catalogs

Clearinghouse is the name for the catalog of digital data initiated and sustained by the Federal Geographic Data Committee (FGDC) in support of the National Spatial Data Infrastructure (NSDI). Participation of US federal agencies in *Clearinghouse* is mandated by Executive Order 12906 (published in 1994) amended by Executive Order 13286 in 2003 (fgdc.gov/publications/documents/geninfo/execord.html).

Approximately 400 websites are listed[1] as being associated with *Clearinghouse* participants. They represent federal, state and local government in the US, federal-level agencies in other countries, commercial entities and educational institutions. The nodes are polled hourly to determine their status. An example[2] result: 396 nodes responded to zping; 264 nodes were up, 65 were down and 67 timed out.

Geospatial One Stop(GOS) includes a portal (www.geodata.gov/) by which anyone can access geospatial information from federal agencies and a growing number of state, local, tribal and private agencies. The GeoData Marketplace component of GOS provides advance notice on future investments in geospatial information, thereby providing opportunities for collaboration and intergovernmental partnerships, and reducing needless duplication of data investment. GOS also supports communities of users interested in a particular topic or application. “2005 Hurricane Season” is an example community: it provides links to web sites, resources, and maps related to that topic, with special pages for Katrina, Rita and Wilma.

Formats

Commercial organizations[3] offer solutions to technical issues of data exchange. For example, Blue Marble Geographics (www.bluemarblegeo.com) offers the Geographic Translator, which supports data and coordinate system translation of map files in the AutoCAD DWG & DXF, Microstation DGN, MapInfo MIF & TAB, and ESRI Shape formats. Similarly, Safe Software (www.safe.com) offers the FME (Feature Manipulation Engine) Suite for data transformation and data translation to/from many different supported data formats. Global Mapper (www.globalmapper.com) is another example of a commercially available solution to the need for viewing and exporting numerous formats, and for converting from one projection to another.

The U.S. Fish & Wildlife Service (FWS) has identified three formats as being in wide use both within FWS and in the GIS community-at-large: the Arc/Info Export (.E00) file format, the ESRI Shapefile format, and the AutoCAD DWG file format. The *Procedure: Geospatial Data Exchange Format* (www.fws.gov/stand/standards/pr_geoex.html) instructs FWS offices to “use at least one of these data formats whenever serving data on the Internet or when creating data that will be widely distributed …”

[1] http://clearinghouse4.fgdc.gov/registry/clearinghouse_sites.html.
[2] http://registry.gsdi.org/serverstatus/ accessed 28 December 2005.
[3] Note: the list here is not comprehensive and is not a recommendation for any specific products.

Terms and conditions of the exchange

Various groups have wrestled with issues related to data exchange. A few examples of groups and their activities are provided here:

The **Minnesota** Governor's Council, "created in 1991 to promote coordination among producers and users of geospatial data" prepared a report, "Making the Most of Geospatial Data Exchange: A Guide for Data Distribution." Published in July 2003, the report shares insights gained in a decade of experience; it is officially described as follows:

> "This report offers guidance and best practices to help public agencies develop distribution policies for their geospatial data."
>
> Source: http://www.gis.state.mn.us/resource.html?Id-2129

The **Ontario Geospatial Data Exchange** (OGDE)

> "… a program of the Ontario Ministry of Natural Resources. Geospatial data from the Ontario Geospatial Data Exchange (OGDE) is now available to all UTM faculty, staff and students for academic use only."
>
> Available formats include ASCII, Coverage and Shape.
>
> Source: http://www.erin.utoronto.ca/~w3libgis/ogde.html

The **Great Lakes Commissio**n (GLC, www.glc.org) has initiated the annual Great Lakes Regional Data Exchange Conference to encourage data exchange partnerships among the GLC member states and associate members. Member states are Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania and Wisconsin. Associate members are Ontario and Quebec. The development of web mapping services is helping to create examples of the benefits of data exchange.

New York State established a New York State GIS Data Sharing Cooperative in the 1997-1998 timeframe. A data sharing agreement[4] has been developed and signed by 549 cooperators; 101 (18%) of the members have identified 416 datasets that they are making available.

[4] The New York State Geographic Information Systems (GIS) Cooperative Data Sharing Agreement for Use with Local Governments of New York State and Not-For-Profit Entities is available online at http://www.nysgis.state.ny.us/coordinationprogram/cooperative/agreement.cfm

Sector Overview, New York State GIS Data Sharing Cooperative Members

Sector	*Number of Members*	*Number of Members Contributing Data*
Academia	95	1
County Government	55	24
Federal Government	17	7
Local Government	193	27
Non Profit	102	16
Other States	6	4
Sovereign Nations	1	1
State Government	80	21
Total	549	101

Source: http://www.nysgis.state.ny .us/gisdata/

A publication sponsored by the GeoData Alliance captures lessons learned by the New York GIS Data Sharing Cooperative and five other groups: **Lessons from Practice: A Guidebook to Organizing and Sustaining Geodata Collaboratives**. Published in September 2001, **Lessons from Practice** is available as a 1.6 meg download[5] at no charge, or a printed version may be purchased for a nominal fee.[6]

Building on the success represented by that publication, the GeoData Alliance also provided sponsorship, along with USGS, URISA and six commercial entities, to support the creation of the Open Data Consortium (ODC, www.opendataconsortium.org). Based on the vision of Bruce Joffe and under his leadership, the ODC has developed a Model Data Distribution Policy document. The 49-page document is available on the Open Data Consortium website.[7] Four categories of issues have been identified:

1. Data ownership
2. Public access
3. Funding geodata maintenance
4. Data distribution and stewardship

For each issue in each category, the document includes alternatives, policy objectives, and an evaluation of the pluses and minuses of each alternative.

Seven themes have been identified as being of critical importance to the National Spatial Data Infrastructure (NSDI): geodetic control, elevation, orthoimagery, hydrography, transportation, cadastral, and governmental unit boundaries. These themes form the basis of The National Map, where they are presented in a nationally consistent framework.

The Geospatial One Stop (www.geo-one-stop.gov), an intergovernmental project managed by the Department of the Interior, includes the creation of the Geospatial One Stop portal, www.geodata.gov/.

[5] http://geoall.net/docs/lessons_from_practice.pdf
[6] $9.95 plus $3.00 shipping and handling
[7] http://www.opendataconsortium.org/documents/Data_Policy-4b.pdf

Summary

Progress is underway in creating online catalogs of geospatial data, though we are a long way from having a comprehensive search engine that can find all geospatial data meeting specified criteria. Issues involved in translating from one format, projection and datum to another are generally tractable. The creation of metadata is viewed as an onerous burden; however, the availability of web mapping services will increasingly demonstrate the necessity for it.

The OGC has a Working Group identifying and addressing the issues involved in applying digital rights management technology to geospatial data. As this effort proceeds and people gain confidence that terms and conditions can be managed digitally, a desirable consequence is that even more data will become available.

Status of Open DRM for Geodata

In 2004, the GeoData Alliance organized a workshop on GeoDRM and held it 24 May in Denver, Colorado. The program began with an introduction to digital rights management by Brian LaMacchia of Microsoft. Todd Bacastow, President of the GeoData Alliance, then moved the discussion to geospatial DRM. Bruce Joffe of the Open Data Consortium presented the model data policy and requested feedback from the attendees on the identified elements and their purposes.

The OGC initiated a Working Group on geospatial DRM in June 2004. (See Appendix D for the mission and objectives of the Working Group.)

In July 2004, two graphics were created to illustrate the GeoDRM Playing Field. Figure 1 shows the view external to OGC, and Figure 2 is internal to OGC.

On 9 December 2004, the GeoData Alliance held a forum in Washington, DC. Twenty-two individuals from the public, private and non-profit sectors were invited to identify and begin to address the policy challenges presented by implementation of an interoperable digital rights management framework for geographic data and services.

Through 2005, the OGC GeoDRM Working Group initiated four projects:

1. Demonstrator
2. OWS3 Testbed
3. Interoperability Experiment
4. Reference Model

As part of the outreach efforts of the OGC GeoDRM WG, member John Herring (Oracle) wrote “Digital Rights Management for the Geospatial Community,” which was published in the November 2005 issue of *GeoWorld.*[8]

[8]The article is available online at http://www.geoplace.com/uploads/FeatureArticle/0511tt.asp.

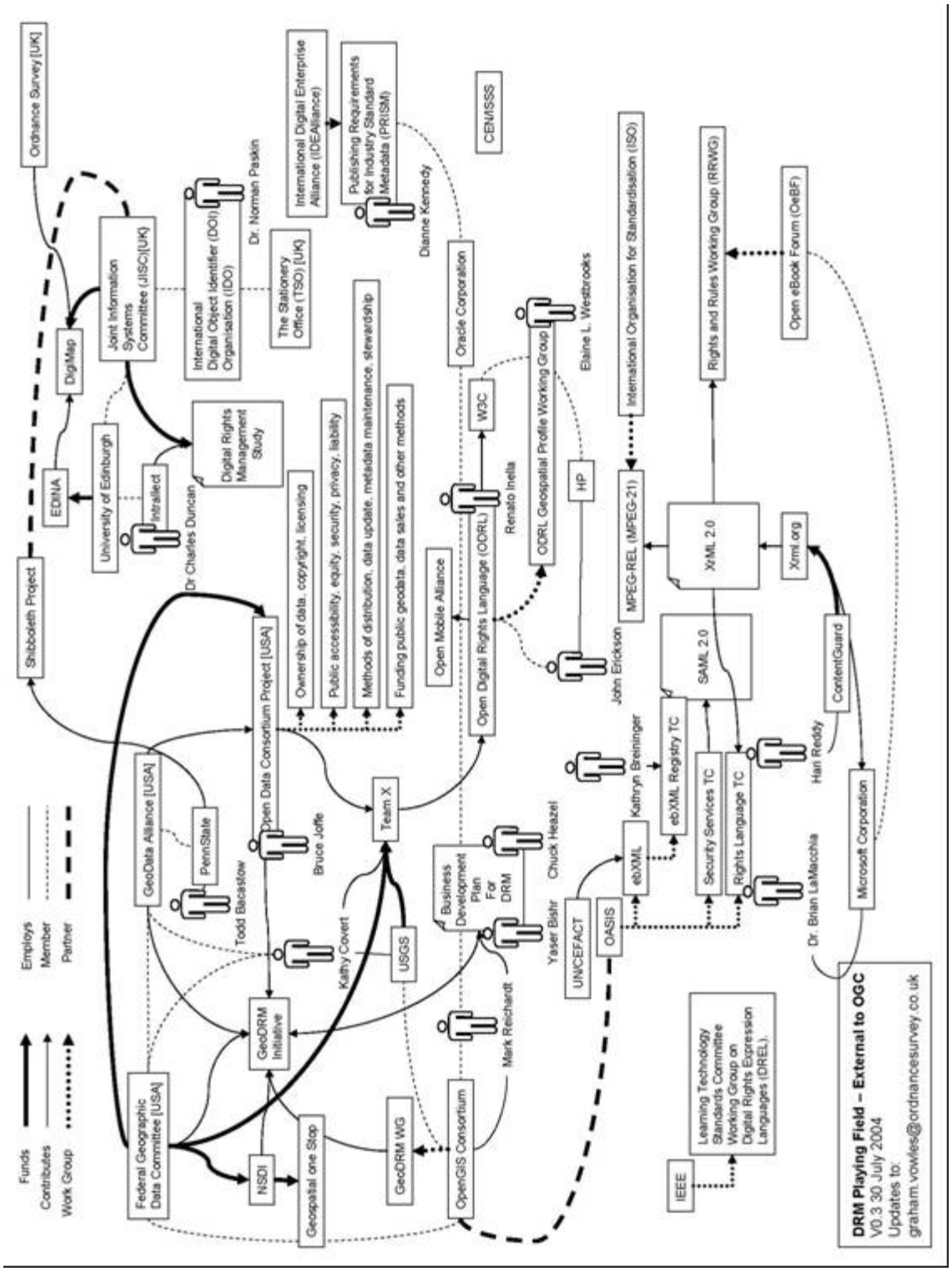


Figure 1. DRM Playing Field External to OGC

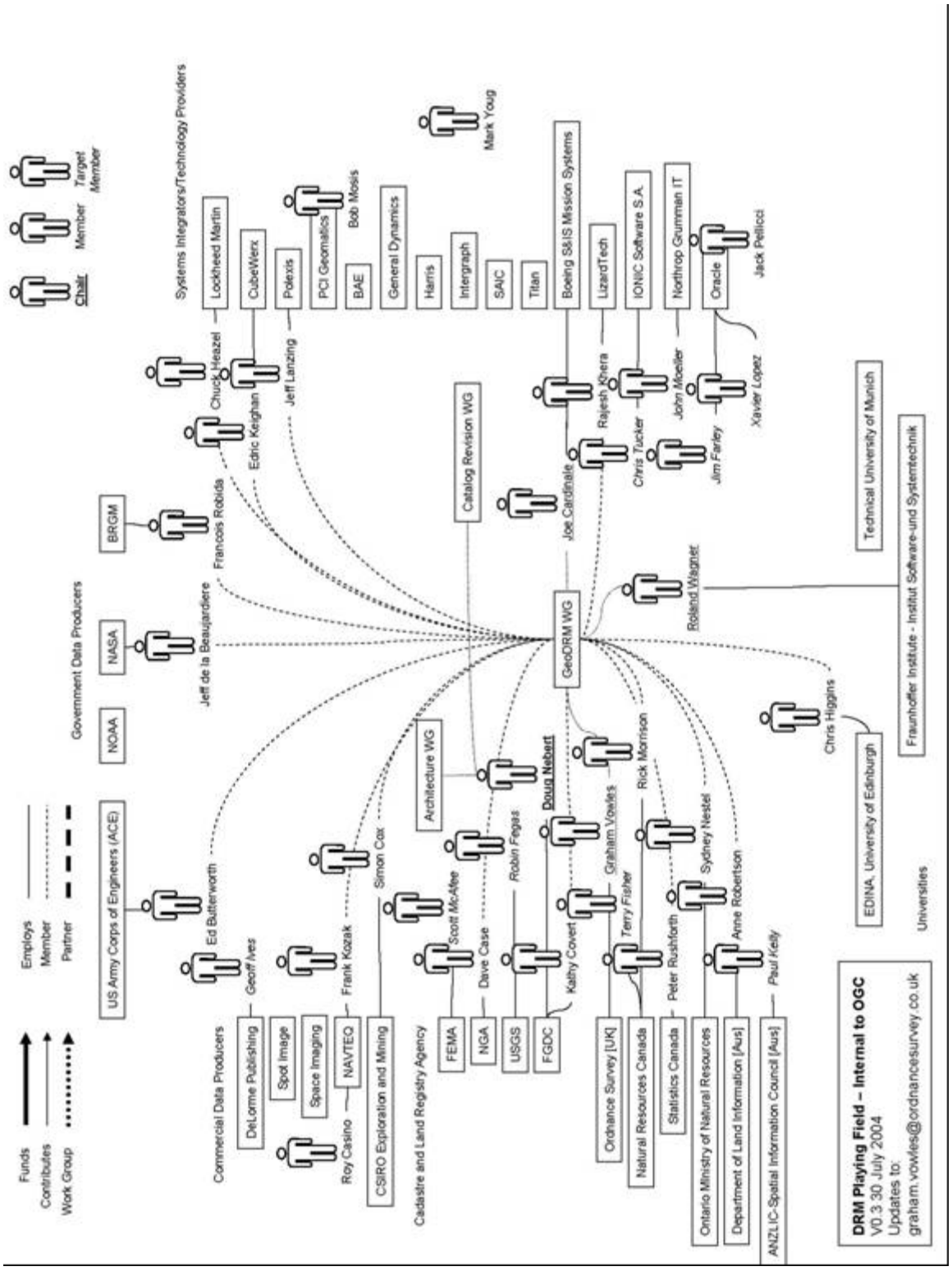


Figure 2. DRM Playing Field Internal to OGC

The GeoData Alliance and the Open Geospatial Consortium sponsored a dial-in panel-and-discussion session on Geographic Digital Rights Management (GeoDRM) on behalf of the FGDC, as part of a meeting of the DC Chapter of the Association of Enterprise Architects (www.aeajournal.org, www.aea-dc.org) on 14 December 2005. See Appendix F for the presentation.

Perspectives on GeoDRM

A set of questions was developed to learn how people view GeoDRM. They were provided to members[9] of the OGC GeoDRM WG, whose answers are reported below, and to panelists at the December 2004 forum, whose answers are reported in Appendix E.

1. What does GeoDRM mean to your organization?
2. What organizations will benefit most from GeoDRM?
3. What job functions will benefit most from GeoDRM?
4. What do you see as the biggest benefit of GeoDRM?
5. What price do we (society) have to pay to realize the benefits of GeoDRM?
6. What is the biggest technical challenge to successful implementation of GeoDRM?
7. What is the biggest policy challenge to widespread use of GeoDRM?
8. When do you think the challenges will be met and we'll see widespread use of GeoDRM?
9. What next step can any motivated individual take to help move GeoDRM forward?

1. What does GeoDRM mean to your organization?

The benefit identified by the most organizations is that GeoDRM is a way to protect their investment, or their client's investment, in data capture. It does this in two ways: by facilitating payment for use, and by complementing existing legal measure to protect the investment.

GeoDRM also offers a way to digitally implement licensing agreements with third parties; absent such a management tool, some organizations will not get a license.

Finally, GeoDRM means authentication of data. GeoDRM provides a safeguard against unauthorized modification of content.

2. What organizations will benefit most from GeoDRM?

The first point noted here is that GeoDRM will only be a viable proposition if all organizations benefit from it and perceive the value they derive.

The GeoDRM working group of OGC has identified the following classes of organizations that will benefit from GeoDRM:

- Commercial Data Providers

[9] Telecon participants and email respondents include Graham Vowles, Ordnance Survey; Joe Cardinale, Boeing; Roland Wagner, The Fraunhofer Institute for Software and Systems Engineering; Rick Morrison, CubeWerx (now with Metalogic Software); Chris Tucker, IONIC Software.

- Government Data Providers
- Commercial Service Provider
- Commercial Integrator
- Users

3. What job functions will benefit most from GeoDRM?

The vision is that GeoDRM will facilitate timely delivery of quality information. People will appreciate the convenience (think of the use of PayPal as a mechanism for e-Bay).

Job functions that benefit the most from GeoDRM are the end user and the decision maker. Data authentication, quality and timeliness are important factors in determining the value of GeoDRM to the end user—the party ultimately responsible for paying the costs of quality data. One of the characteristics of GeoDRM is that it offers a more direct, transaction-level option for payment. At this time however, the value proposition for the end user under a GeoDRM scenario must be further developed and demonstrated

Producers will also benefit because GeoDRM creates the possibility of a new revenue stream for them.

4. What do you see as the biggest benefit of GeoDRM?

One of the biggest benefits of GeoDRM is that data and service providers will have a new business model for pricing and licensing their offerings. An interesting example was described:

> With GeoDRM, one is able to grant access to data based on geospatial attributes. Most work on DRM to date has been done in the music and video industry. This work is concerned with the entire data set (a song or a movie). GeoDRM is a different problem set. It deals with entities at the feature level. A producer may want to grant access to data within 500 feet of a road center line, or inside a parcel. This type of control will allow producers to better control their data.

Another big benefit is that GeoDRM will enable a trading economy in information. It provides a mechanism to provide recognition and compensation, which are incentives to collect and publish useful content. GeoDRM also provides clear lineage and a managed audit trail of how information is derived; this has as much value as the data itself to at least some categories of end consumer. Therefore GeoDRM will enable and support the trading relationship allowing networks and economies of data to evolve.

5. What price do we (society) have to pay to realize the benefits of GeoDRM?

Investment will be required to build and manage the infrastructure, including computing capability, to support the managed digital exchange of data. Certain roles may not appear to add value to content and yet they deliver value to the system and so must be compensated, for example a license manager responsible for enforcing licensing policy on behalf of content providers.

The infrastructure will be a relatively fixed cost and the value must exceed the cost.

6. **What is the biggest technical challenge to successful implementation of GeoDRM?**

The biggest challenge is to develop a shared conceptual model of what GeoDRM is and what it means in human and business terms. This is in a sense a metamodel - a model of models which can support a variety of business models. If that is possible, the biggest challenge then will be to develop an open interface everybody can agree on.

One perspective is that effort should be made to drive toward simplifying things, while another view is that people want constraints that are inherently complex.

Financial markets move money around in complex ways. With GeoDRM, we want to move both money and information around.

7. **What is the biggest policy challenge to widespread use of GeoDRM?**

Two challenges were identified, and they may be variant expression of a single big policy challenge:

1) Human nature - desires for power, control, recognition.
2) The fact that there is no policy.

That is, is the absence of policy a consequence of human nature?

8. **When do you think the challenges will be met and we'll see widespread use of GeoDRM?**

This is envisioned as a phased, cyclical process over time. That is, access, authorization and authentication may be met earlier and enable some functionality, while data security, encryption, watermarking and GeoBusiness services challenges will be met later.

9. **What next step can any motivated individual take to help move GeoDRM forward?**

Study the business processes of their organization and identify where GeoDRM applies; document those applications as use cases and share them with the bodies developing standards.

Attend the next GeoDRM workshop; join the OGC GeoDRM Working Group.

Policy Issues

DRM and GeoDRM are technological tools that can be used to enhance or diminish a variety of societal values. A free market economy, individual privacy, the public good served by data in the public domain, the doctrine of fair use, intellectual property rights and freedom of speech are examples of values that may be enhanced or diminished by GeoDRM technology.

Marketplace model vs. library model

Harlan Onsrud is Professor in the Department of Spatial Information Science and Engineering at the University of Maine and a research scientist with the National Center for Geographic Information and Analysis (NCGIA). He has written a thought-provoking essay on the value of the library as a metaphor and model for access to data, information

and knowledge. He asserts that a marketplace model does not deal appropriately with "public goods," and that geospatial data and the NSDI have significant "public good" characteristics. The essay, "Exploring the Library Metaphor in Developing a More Inclusive NSDI," is available on the GeoData Alliance website.[10]

Elaine Westbrooks has chaired the Open Digital Rights Language (ODRL) Geospatial Working Group (www.odrl.net/Profiles/Geospatial/) since 2004. She is the Metadata Librarian in the Albert R. Mann Library at Cornell University. To provide free access to geospatial data and metadata for New York State, the Albert R. Mann Library created the Cornell University Geospatial Information Repository (CUGIR) in 1998. A paper[11] she presented at the 2003 Dublin Core conference in Seattle, Distributing and Synchronizing Heterogeneous Metadata for the Management of Geospatial Information Repositories, describes differences in the standards of the library community (including archiving and version control) and of the GIS community (including efficient data creation, reduced burden of metadata, and distribution of data according to user requests), and describes how CUGIR created a metadata model and metadata management system.

DRM Technology and Individual Privacy
Julie E. Cohen, Professor of Law at Georgetown University, teaches and writes about intellectual property law and data privacy law. She takes up the topic of how implementations of DRM can facilitate tracking usage in a way that is contrary to ideas of individual privacy in a 2003 article, "DRM and Privacy" (Cohen 2003a)

DRM, Science and the Public Domain
Cohen addresses how DRM technologies may affect science and technology in "The Challenge of Digital Rights Management Technologies," a paper presented at a Symposium of the National Academy of Sciences in 2003. This paper (Cohen 2003b), though about DRM in general, is quite relevant to GeoDRM because it identifies some of the implications of DRM technologies for access to and use of public-domain information.

Fair Use and DRM
Fred von Lohmann, Senior Intellectual Property Attorney with the Electronic Frontier Foundation has written about the possibility of DRM technologies preventing the public from doing things which have been protected under the doctrine of fair use. In his essay[12] "Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension between Them" he spells out the potential challenges. The doctrine of fair use has provided a mechanism for balancing the rights of copyright owners and the public. DRM technology has the potential to shift the balance more to copyright owners. One potential result is that archives and libraries will be undermined, because DRM systems could be set up to prevent free archiving.

[10] http://geoall.net/library_harlanonsrud.html
[11] http://www.siderean.com/dc2003/204_Paper78.pdf
[12] http://www.eff.org/IP/DRM/cfp_fair_use_and_drm.pdf

Next Steps

The GeoData Alliance and the OGC GeoDRM WG will continue to collaborate in carrying out Interoperability Experiments to test and validate GeoDRM concepts, and to further mature a framework for standards based GeoDRM capabilities; these are scheduled to continue through the first quarter of 2006. Interoperability Experiments provide an opportunity for OGC members to plan, launch and run a focused initiative for specification development, refinement, or testing.

The GeoData Alliance and the Open Geospatial Consortium expect to sponsor additional dial-in panel-and-discussion sessions on behalf of the FGDC, similar to the one on Geographic Digital Rights Management (GeoDRM) conducted as part of a meeting of the DC Chapter of the Association of Enterprise Architects (www.aeajournal.org, www.aea-dc.org) on 14 December 2005 (See Appendix F).

The GeoDRM Working Group will continue to meet four times per year during scheduled Technical Committee meetings and to collaborate remotely using the OGC portal and weekly teleconferences. A key focus is the development of the GeoDRM Reference Model, which will be the subject of a workshop being convened in Munich in January 2006.

The GeoData Alliance will convene a digital rights policy forum in the fall of 2006.

Acknowledgments

Numerous people have contributed to the progress made so far.

We thank Todd Bacastow for his leadership of the GeoData Alliance and Bruce Joffe for his leadership of the Open Data Consortium.

Thank you to Brian LaMacchia, Todd Bacastow, Kathy Covert, Carl Reed and Bruce Joffe for their presentations at the Workshop on Geospatial DRM in May 2004, and to Brian LaMacchia, Michael Domaratz, Carl Reed and Brenda Bailey-Hainer for participating in a panel discussion chaired by Tina Cary.

We thank Kathy Covert, Tim Case and Joe Cardinale for their prepared remarks at the GeoDRM forum in December 2004, and Hari Reddy, Elaine L. Westbrooks, Marilyn Otto, Randall Johnson, Jeff Labonte and William G. Miller for serving as panelists.

Thanks also to the following members of the OGC GeoDRM WG for their Perspectives on GeoDRM (see above): Graham Vowles, Ordnance Survey; Joe Cardinale, Boeing; Roland Wagner, The Fraunhofer Institute for Software and Systems Engineering; Rick Morrison, CubeWerx (now with Metalogic Software); Chris Tucker, IONIC Software.

The contribution of Tina Cary in compiling, editing and writing the various components of this report is hereby acknowledged.

Finally, we acknowledge the leadership of all participating organizations in this effort. The advancement of usable, standards-based GeoDRM solutions cannot be achieved without broad cooperation of relevant organizations and individuals. For this initiative, a number of standards development and professional organizations have come together to establish a common path to evolve solutions that could not be achieved by any organization acting alone. This project has helped to demonstrate the ability of diverse organizations to align and partner to achieve common goals.

References

Cohen, Julie E. 2003a. DRM and Privacy. Berkeley Technology Law Journal, Vol. 18. Abstract is available online at http://ssrn.com/abstract=372741. A draft of the full article is available online at http://www.law.georgetown.edu/faculty/jec/drmandprivacy.pdf (both accessed 30 November 2005)

> Given today's technology, when digital technology administers rights, data are available about where the person was at the time of access, in addition to who is seeking access to what data for what use under what license. Are there any safeguards for individual privacy? Should there be?

Cohen, Julie E. 2003b. The Challenge of Digital Rights Management Technologies, in Julie M. Esanu & Paul F. Uhlir, eds., *The Role of Scientific and Technical Data and Information in the Public Domain: Proceedings of a Symposium* 109-16. Washington, DC: National Academy Press. Available online at http://www.nap.edu/books/030908850X/html (accessed 30 November 2005)

> Though about DRM in general, this paper is quite relevant to GeoDRM because it identifies some of the implications of DRM technologies for access to and use of public-domain information. If access to geospatial data is managed by technology, and the technology changes, the data become unavailable. How will libraries and other repositories maintain archives of maps over time?

Onsrud, Harlan J. 2004. Exploring the Library Metaphor in Developing a More Inclusive NSDI. GeoData Alliance website at http://www.geoall.net/library_harlanonsrud.html. (accessed 29 November 2005)

Von Lohmann, Fred. 2002. Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension Between Them. Presented at the conference Computers, Freedom and Privacy, 16 April 2002. Available online at http://www.eff.org/IP/DRM/cfp_fair_use_and_drm.pdf (accessed 7 December 2005).

> The first of Von Lohmann's three aspects of fair use clearly applies to the geospatial realm: fair use allows geospatial information scientists to copy a journal article for personal use. Progress in GIScience, as in any science, depends on being able to learn from the work of others.

Westbrooks, Elaine L. 2003. Distributing and Synchronizing Heterogeneous Metadata for the Management of Geospatial Information Repositories. Dublin Core 2003 Conference, Seattle, Washington, 28 September - 1 October 2003. Online at http://www.siderean.com/dc2003/204_Paper78.pdf (accessed 29 November 2005).

> Describes differences in the standards of the library community (including archiving and version control) and of the GIS community (including efficient data creation, reduced burden of metadata, and distribution of data according to user requests).

Appendices

Appendix A. An Introduction to Rights Management Technologies

The following material was presented by Brian LaMacchia at the GeoDRM Workshop in Denver, Colorado on 24 May 2004 to introduce rights management technologies in general.

About Brian LaMacchia

Brian A. LaMacchia is Software Architect at Microsoft Corporation.

Note: Slide 50 below uses the acronym SDMI. SDMI is the Secure Digital Music Initiative, a group whose goal is to "protect the playing, storing, and distributing of digital music" (from their website at http://www.sdmi.org.) On September 6, 2000, SDMI issued "An Open Letter to the Digital Community," inviting people to attempt to crack specific technologies they are considering for use in their system. They set up a web site where music samples and some other information could be downloaded to aid in analyzing the technologies.

An Introduction to Rights Management Technologies

Brian A. LaMacchia
Software Architect
Microsoft Corporation

GeoDRM Workshop
May 24, 2004

Agenda

- Motivation, definitions and usage scenarios
  - The fundamental problem rights management technologies address
- Background on core technologies
  - Encryption, authentication & secure execution environments
- Policy Management
  - Specifying rights/permissions
    - Rights Expression Languages
  - Policy evaluators
  - Enforcement mechanisms
- Other approaches
  - Watermarking & Code Obfuscation
- Threat models/risk assessments
- The legal environment
- Open problems & opportunities

2

Motivation, Definitions and Usage Scenarios

Protecting Digital Information

Organizations need better protection of sensitive digital information - trade secrets and customer privacy.

The Yankee Group, 2003

Proprietary information theft caused the greatest financial damage of all security failures

FBI Crime Survey, 2003

" But most corporations lose intellectual property through employees. Whether intentionally or inadvertently ...

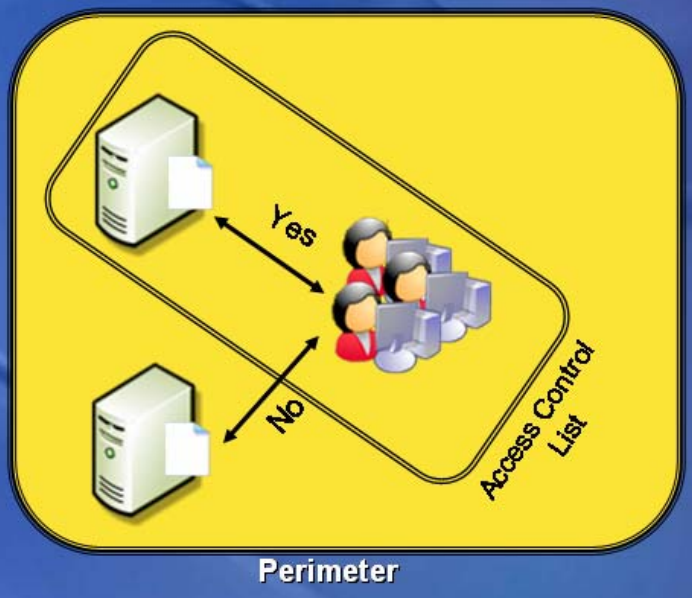
Gartner G2 News Analysis, February 25, 2003

32% of the worst security problems are caused by insiders

PricewaterhouseCoopers (U.K.), 2002

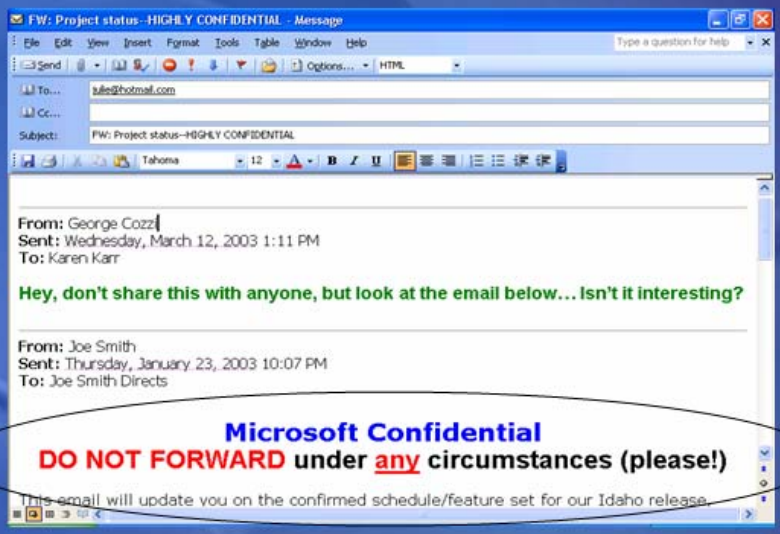
4

Access Control Today



5

Today's Policy Expression…



…lacks enforcement tools

6

Common Goals for Rights Management Technologies

Rights management systems provide

- Safeguards for sensitive information
- Persistent protection as information moves across networks
- Flexible and customizable policy expressions for describing usage rights

7

What Rights Management Is Not

A rights management system will NOT

- … provide unbreakable, "hacker-proof" security
- … protect against analog attacks

A determined, sufficiently motivated attacker, with enough resources can always get at protected content.




8

An Analog Attack …

9

Usage Scenarios

- Protecting confidential e-mail messages
  - Company exec sends an e-mail using a "Company Confidential" template. The template applies read-only rights. The exec then attaches an unprotected document, which inherits the same usage rights as the e-mail. Recipients cannot copy, save, edit or forward the e-mail or document.
- Safeguarding documents
  - A research manager rights-protects a document and sets an expiration date. She grants read-only access to her research team. Only those on her research team can open the document. After the expired time, they can no longer open the document.
- Controlling specified usages of data
  - A Web administrator rights-protects the year-end sales data on the company intranet. Company employees are granted permissions to view the static data, but only selected employees are allowed to use the data with modeling tools to forecast next year's sales.

10

Fundamental Goal of Rights Management Systems

- *Send data with associated policy into a remote, possibly hostile, computing environment and know that the policy will be respected*

- Infrastructure to support secure promotion, sale, and delivery of digital data (content).
- Rights management systems always incorporate "cooperating," autonomous components

11

Content Protection Mechanisms

Marked content	"Forensic rights management" *Find the distribution channel*
Labeled content + compliant device	Macrovision, DTV Broadcast flag, 5C Digital Transmission Content Protection for CE devices *Prevent unauthorized copying*
Encrypted content + compliant device	DVD's, Digital TV (cable and satellite), DVI interface *Prevent theft of content or service*
Encrypted content + use licenses (fine-grained permissions-based systems)	eBooks, Music, Video players *Prevent unauthorized uses*

12

Two Aspects to Rights Management

- Content management
  - How is the data protected/encrypted?
  - How is the data distributed?
  - How are the encryption keys managed?
- Policy management
  - Authoring policy expressions
  - Projecting policy expressions with confidence into remote environments
  - Evaluating policy expressions

13

Background on Core Technologies

Background on Core Technologies

- Encryption
  - Symmetric key (used for content encryption)
  - Public key (used for key encryption)
- Authentication
- Secure execution environments

15

Encryption vs. Authentication

- Encryption
  - Maintaining information secret/confidential, even if the information passes over a public channel
- Authentication
  - Maintaining information integrity and authenticity, including being able to prove that a message hasn't been tampered with

16

Meet Alice and Bob

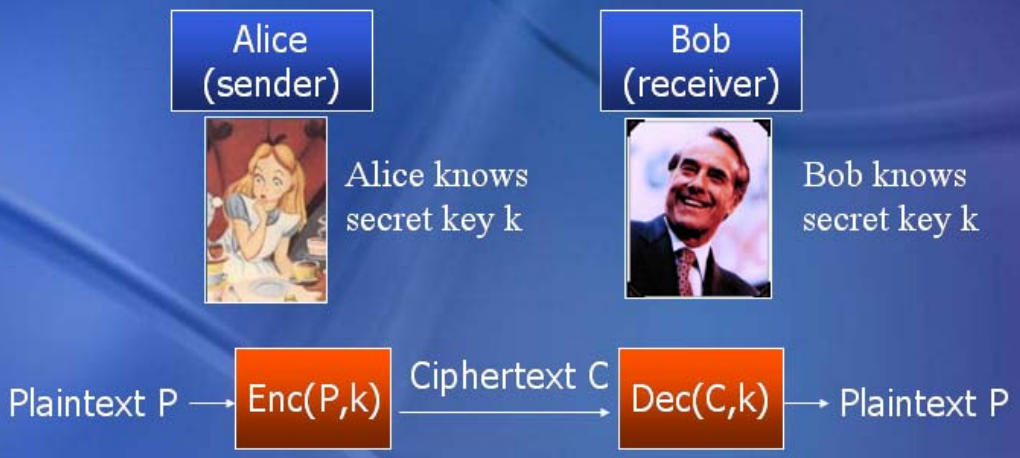
17

Symmetric Key Encryption

- Setup: Alice wants to send a private message to Bob.
- Precondition: Alice and Bob **have previously shared some secret known only to them.**
- The pre-shared secret is the "encryption key" Alice and Bob will use.

18

Symmetric Encryption



19

Public key cryptosystems

- Secret key crypto has a disadvantage: every pair of people needs their own secret key
- In public key crypto, we have two keys
  - One key encrypts, the other key decrypts
    - Infeasible to calculate one key given only the other
  - We can *publish* one key and keep the other secret
    - Published key is the *public key*; secret is the *private key*
    - Anyone can use the public key to send a message, only the holder of the secret key can recover it
- 1975 (Merkle, Diffie, Hellman, Rivest, Shamir, Adelman)

20

Encryption via PK

- Public key encryption algorithms (e.g. RSA) directly encrypt messages
  - encrypt: ciphertext = encrypt(message, pub key);
  - decrypt: message = decrypt(ciphertext, priv key);
- Public key is conceptually simple, with annoying details:
  - Most public key systems use very large numbers (~1-2K bits for reasonable security) and are slow
  - Requires care w/ key generation, small or chosen messages, etc.

21

Public Key Encryption

22

Encryption in RM Systems

- Goal: prevent tampering & unauthorized copying during distribution
  - E.g CSS for DVDs, Pay-per-view
- Symmetric ciphers: used to encrypt content to be protected
  - Always use a randomly-generated "content encryption key"
- Asymmetric ciphers: used to encrypt and distribute content-encryption keys securely
  - This technique is called key wrapping
  - Key sharing (management) is the hard part

23

Authentication for Rights Management Systems

- Process of establishing confidence in the truth of some claim
- Goals in rights management systems:
  - Content authenticity
  - Device authentication -> authorization
  - User authentication -> authorization

24

Authentication Technologies

Content Authenticity	Watermarking (embed a secret message in an image) Fingerprinting (identify and compare images)
Device Authentication	Shared secret: smartcards (DirecTV) Public Key certificates: (eBooks) TPM: (TCG)
User Authentication	Biometrics (Sony) Tickets/tokens (Passport, Liberty Alliance)

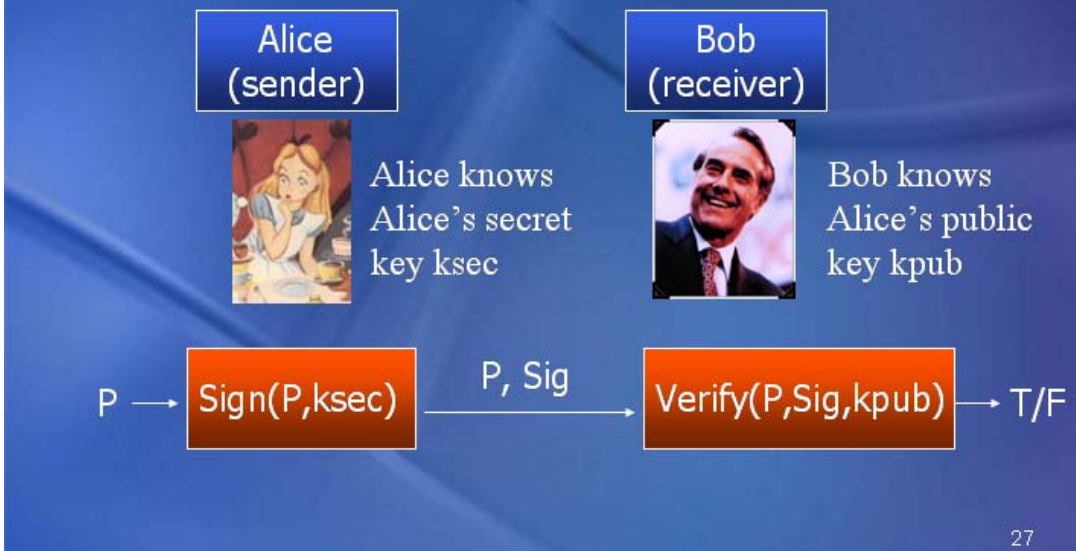
25

Authenticating w/ PK Digital Signatures

- Still have two related keys, one private key (for signing) and one public key (for verifying)
  - Sender creates sig = sign(priv,message)
  - Receiver checks that message = vrfy(pub,sig)
- Establishes integrity & authenticity, but also allows *3rd party* to verify (receiver can't forge)
  - Unless private key was compromised…

26

Public Key Authentication



27

Secure Execution Environments

- Hardware "Closed" Systems
  - Purpose-built boxes with "trusted" software, no programmability, and controlled outputs
  - E.g. eBook reader
- Software Analogs
  - "Trusted" subsystem within a PC
  - Use of "containerized" content controlled by permissions derived from machine-readable licenses
  - E.g. Printing along with personal annotations allowed in an eBook on a PC

28

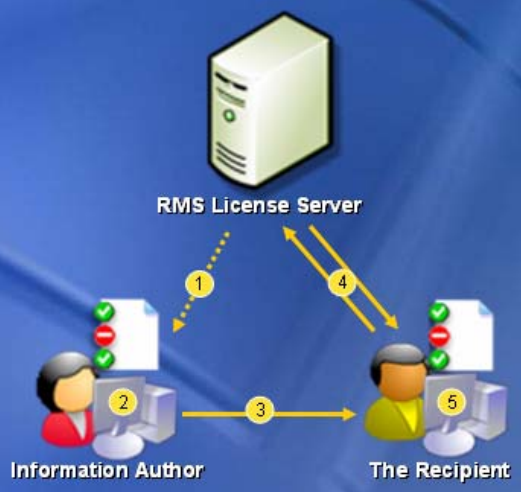
Putting it all together (1)

Steps in a permissions-based system:

- Encrypt the content/data with a content-encryption key
- Authenticate the end-user device that will receive the content
- Create a license specifying the contents rights to be granted, and associate the license w/ content
- Encrypt the content-encryption key with the device key and embed this in the license
- Send the encrypted content and license to a secure execution environment on the end-user device
- Within the execution environment, when access to the content is requested a policy engine evaluates the license terms to determine whether the access should be granted.

29

Putting it all together (2)



1. Author receives a client licensor certificate (CLC) the first time they rights-protect information.
2. Author defines a set of usage rights and rules for their file; Application creates a "publishing license" and encrypts the file.
3. Author distributes file.
4. Recipient clicks file to open, the application calls to the RMS server which validates the user and issues a "use license."
5. Authorized application decrypts the file and enforces rights.

30

Policy Management

- Specifying rights and permissions in licenses
  - Rights languages
- Policy evaluation mechanisms
- Rights management systems built on today's platforms are useful for a wide variety of solutions; the features provided by rights languages and richer policy evaluation mechanisms will further expand that set.

32

Policy Management Tasks

- Content owners (or their agents) author policy statements for content.
  - Owners license their exclusive rights (in a copyright sense) to consumers or distributors.
- Rights management-aware servers (or networks) distribute policy statements.
  - Maybe they distribute the content too.
- End-user rights management systems consume and abide by policy statements when processing the content.
- As an industry, we understand the "crypto" aspects of rights management better than we understand the "policy" aspects
  - Key management is easier than policy management

33

Rights Vary by Scenario

- E-mail/document workflow
  - Open/Read
  - Edit
  - Print
  - Forward
  - Reply
  - Save
- Music
  - Playcount
  - AllowBackupRestore
  - AllowBurnToCD
  - AllowPlayOnPC
  - BeginDate, ExpirationDate
  - DeleteOnClockRollback
  - DisableOnClockRollback

34

Goals for Rights Languages

- A rights language is a type of policy authorization language.
  - Focus is on expressing rights granted by one party to another.
  - Issuance and delegation rights for other grants are core concepts.
    - Can be used to model lending, loans, transfers of rights.
  - Conditional grants of rights
- Rights language requirements:
  - Provide a flexible, extensible mechanism for expressing authorizations.
  - Enable interoperability across various policy evaluation systems.
  - Make it easy for policy authors (e.g. content owners) to express their desired policies.

35

Authorization language standardization efforts

- ISO MPEG REL (ISO/IEC 21000-5:2004, based on XrML2)
  - Designed for rights transference statements
- OMA rights language (based on ODRL)
  - Limited expressiveness for constrained environments
- SAML (Security Assertion Markup Lang)
  - AuthN/AuthZ statements
- XACML (eXtensible Access Control ML)
  - Language for describing policy evaluation algs
- X.509/PKIX certificates
  - Really only intended for authentication, although some try to use them for carrying simple authorization statements

36

ISO MPEG REL (based on XrML2)

- In the rights management context, REL allows content owners a systematic way to express their intent for distribution and consumption.
- Like other policy languages, REL licenses (statements) declare authorizations, but cannot enforce compliance.
  - Systems that consume REL licenses must be trusted by the license issuer to properly enforce the grants specified within the license.
- Licenses may be embedded within content or move independently.

37

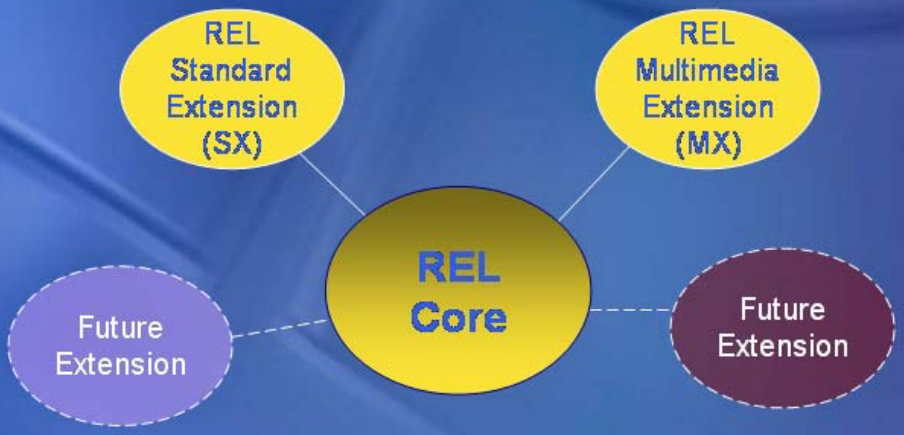
Semantics of a Grant

- Every REL grant has the following form:
  - Issuer authorizes principal to exercise a right with respect to a resource subject to conditions.
  - A license is a collection of one or more grants made by the same issuer.
- Grants may be chained together:
  - Bill's rights management system trusts Tom and his delegates.
  - Tom delegates the right to license printing to John.
  - John issues a license: "Bill has the right to print the book."
  - Therefore Bill can print the book.

38

REL Extensibility

- REL Core is basically an abstract object model. Extensions (subtypes) define domain-specific semantics.



39

Sample REL License

```
<?xml version="1.0" encoding="UTF-8" ?>
 <license>
 <grant>
  <keyHolder>  …  </keyHolder>
  <mx:play />
  <mx:diReference>
    <mx:identifier>urn:mpeg:example:2002:twotonshoe:album</mx:identifier>
  </mx:diReference>
 </grant>
 <issuer> … </issuer>
</license>
```

40

REL authorization model

- Input
  - Principal
  - Right
  - Resource
  - Time interval
  - Licenses
  - Designated "root grants" (implicitly trusted)
- Output
  - "No"
  - "Yes," unconditionally
  - "Maybe," if a set of conditions are also met

41

REL Key Language Features

- Mechanisms for enhanced expressivity
  - Patterns, variables and quantifiers
  - Grouping grants
  - Delegation
- Meta-rights
  - Issue
  - Obtain
  - Revocation
  - PossessProperty
- Linking conditions
  - PrerequisiteRight

42

Policy Enforcement Systems are Prolific

- When you view a rights management system as one instance of a policy distribution & enforcement mechanism, you find lots more of them exist than you might expect…

43

Policy Enforcement Mechanisms in Common Use Today

- Rights management for mass-market content (eBooks, music, video)
- License servers for server services (e.g. file & print services)
- Hardware anti-repurposing (e.g. XBOX)
- Personal Video Recorders (digital storage of video)
- File system protection mechanisms (ACLs)
- Enterprise policy management
  - Group policy in domains
- Aspects of PKI
  - Extensions for AuthZ
- Mobile code sandboxing (e.g. Java & .NET Framework)

44

Evaluating Policy Expressions

- Rights management systems attach policy expressions to content and then project that policy along with the content into a remote system.
- All parties to the transaction need to agree on the behavior of the entire distributed system with a high degree of confidence.
  - Content authors are only going to allow content & policy to flow to remote systems (and, recursively, applications) that they believes will implement policy as defined.
  - Policy creators need to have confidence that the receiving system will faithfully implement the defined policies.
  - Content consumers are only going to let code they understand run on their systems.

45

Policy Evaluation in a Distributed System

- Two general approaches in distributed systems theory to defending against malicious nodes
  - Demand some sort of proof from the node that it has certain properties before sending it any information
  - Use protocols designed to withstand a certain percentage of node failures
    - "Byzantine Agreement" protocols
- Example scenarios
  - In an enterprise rights management environment, servers could be configured to only release classified documents to non-portable machines.
  - Before sending personal information to a server, a client could demand proof that the server is running a software stack certified to comply with privacy-protecting principles.
  - In a consumer rights management environment, content could be licensed such that it could freely migrate among all devices within a single "household".

46

Other Approaches

Watermarks

- Robust Watermarks
  - Meant to withstand transformations that leave original recognizable
    - Images: scaling, cropping, rotation, etc.
    - Sound: transposition, noise, time dilation, etc.
      - Lossy compression
- Fragile Watermarks
  - Any change is detectable
- Both: meant to be imperceptible by people

48

Uses of Robust Watermarks

- Usage tracking
  - "Branding" content with IDs of authorized users
  - Deters unauthorized distribution
- Metadata storage
- Rights management policy enforcement
  - Embedding licenses in content

49

SDMI Challenge

- September 2000, 3 weeks
- No documentation
- 4 "robust" watermark technologies
- Devastating results:
  - Craver, Wu, Liu, Stubblefield, Swartzlander, Wallach, Dean, Felten, "Reading Between the Lines: Lessons Learned From the SDMI Challenge," USENIX Security Symposium, 2001.
  - Stern and Boeuf, "An analysis of one of the SDMI candidates," Information Hiding Workshop, 2001

50

Uses of Fragile Watermarks

- Integrity protection of originals
- Detecting lossy compression
- This appears to be solvable

51

Code Obfuscation

- Software is malleable
  - It is relatively easy to modify software to bypass security and policy checks
- Tamper-resistant hardware is rare and expensive
- Can we obfuscate software for better security?

52

Code Obfuscation

- In a completely general way, no
  - Barak, et al., On the (Im)Possibility of Obfuscating Programs, CRYPTO 2001
- Cloakware has tried hiding a key in a DES implementation
  - Jacob, Boneh, Felten, "Attacking an obfuscated cipher by injecting faults," ACM DRM Workshop, 2002
- No good, uniform definitions of the problem

53

Threat models/risk assessments

Content Protection Threat Models

- Theft of service:
  - Clone the smartcard
  - Create a distribution channel and sell it
  - E. g. DirecTV cards
- Theft of content:
  - Crack the crypto
  - Publish the tools rather than the content
  - E.g. DeCSS, ConvertLit

55

Risk Analysis

- Digital content = a replica of the original work
- Unauthorized re-distribution via the Internet is the sum of all fears for mass-market content owners
  - What's the greatest risk for your community?
- Technology trend line: better compression, improved P2P networking protocols and ubiquitous net access

56

The Legal Environment

Copyright & Rights Management

- Rights management technologies limit access to digital intellectual property.
  - Example: An e-book reader using a rights management system might let you read a book only a fixed number of times.
  - Example: A rights-managed streaming audio player could charge you based on bandwidth and content consumed.
- Major issues:
  - How restrictive can a rights management system be?
  - How restrictive should a rights management system be?
  - How do rights management systems interact with "fair use" and other copyright rights reserved to the public?

58

REL and Multiple Authorities

- REL offers a new level of expressiveness
  - Enables representation of a wider range of scenarios.
- Example scenario: evaluating authorizations from multiple authorities for a resource.
  - Today, rights management systems operate using a "closed-world assumption."
    - Any action not explicitly authorized by the content owner is prohibited.
  - Copyright doesn't work like this.
    - Copyright is a liability-based system.
    - Some actions are permitted by law even if they are not explicitly authorized by the copyright holder.
  - How might we use REL to represent authorizations as well as limitations built into the law?

59

REL and Multiple Authorities (cont'd)

- Content creators are given exclusive rights by law; these rights are then licensed to consumers.
- Limitations on the exclusive rights contained in a copyright can be thought of as independent grants of licenses by Congress to the consumer.
  - "Congress says every library has the right to make an archival copy of a work" (17 U.S.C. 108).
  - Variables allow us to write licenses that apply to (potentially undefined) sets of content and users.
  - Congressional grants can be conditioned on possession of a licensed copy of the work.
- Rights mangement systems would need to recognize both the content owner as well as Congress as authorities for a given work.

60

Copyright Protection Systems

- Copyright enforcement measures are now protected by U.S. law (part of DMCA, U.S. implementation of WIPO treaties)
  - 17 USC 1201 *et. sec.*
    - "No person shall circumvent a technological measure that effectively controls access to a work protected under [copyright]…"
- Limited exemptions for
  - Encryption research
  - Reverse-engineering computer programs for interoperability.

61

Open Problems and Opportunities

General Open Problems in the Rights Management Field

There are lots; here are a few of the larger areas that need work:

- Designing user interfaces for authoring, configuring, describing and reasoning about complex policies.
- Resolving the tension between explicit expressions of rights (which computers like) and liability-based systems (e.g. U.S. copyright law)
- Figuring out how to make distributed systems more reliable and resilient while providing sufficient confidence that all nodes are behaving properly.

63

Rights Management and Geospatial Data

Some things to think about:

- What is your threat model?
  - Are you concerned about protecting a single data item, or only collections of items?
  - Protecting small amounts of data is usually harder than large amounts
- What types of use restrictions do you envision?
  - Do mechanisms exist that can enforce those restrictions?

64

Rights Management and Geospatial Data (2)

- What sorts of business models do you want to support?
  - Superdistribution, loans/lending, etc.
  - Choice of rights language plays a big part
- Are your rights management standards extensible?
  - Can users define new types of rights as they create new classes of data?
  - There is a correspondence between the data you want to protect and the languages you use to protect them

65

Rights Management and Geospatial Data (3)

- Access to individual geospatial data objects might depend on the object's metadata
  - There are many ways to slice a dataset
  - Difference licenses could provide access rights to different "views" of the dataset

66

Summary

- "Projecting policy, with confidence that it will be respected, from a content owner into a remote environment."
- Content management
  - Encryption & Authentication
- Policy management
  - Specifying policies with rights languages
  - Evaluating and enforcing policies

67

Questions?

68

Appendix B. What Is Digital Rights Management?

USGS Open File Report 2005-1086 on the subject of Geospatial Digital Rights Management is reprinted in its entirety on the following pages

Geospatial Digital Rights Management

By Daniel J. Wright

Open-File Report 2005-1086

U.S. Department of the Interior
U.S. Geological Survey

Geospatial Digital Rights Management

Daniel J. Wright
U.S. Geological Survey
511 National Center
Reston, VA 20192

Daniel J. Wright is a student working with the Cooperative Topographic Mapping Program for the U.S. Geological Survey. He will begin his freshman year at the University of North Carolina – Chapel Hill in the Fall of 2005.

Abstract

Distributors of geospatial data must ensure that agreements made with data providers are adhered to by controlling the access and use of data. Digital Rights Management is a way to ensure that these agreements are honored. Digital Rights Management systems include a framework for implementation and rights policies which are attached to data and describe the rights users have regarding the data. Rights policies are written in rights expression languages, one of which, Open Digital Rights Language, is particularly well suited for digital rights management systems for geospatial data.

Geospatial Data and Rights Management

Distributors of data, especially geospatial data, desire control over their data's movement and use, both for their own advantage and to protect certain rights of others. The chief concerns when dealing with geospatial data are privacy, information security, and property. Privacy is defined as "an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed, or used" (Privacy Working Group, 1995). Information security is the protection of information from unauthorized access and ensures the information's integrity. Property is the protection of the rights of the owner of data with regard to the data.

Different rights will be more important to different distributors, notably a greater importance of property in the private sector and security in the public sector. Also, control over data can protect the distributor (or provider) from liability for data, ensure regular data update to maintain quality, and ease the process of data distribution itself (Joffe, 2003).

The rights of privacy and security are usually preserved by simple limitation of access to particular data to those specifically authorized to access them, and limitation of how they can use and distribute those data. Property is more difficult to deal with because of the many legal aspects of intellectual property that must be considered, and the great variety of possible agreements among data providers, distributors, and end users (Joffe, 2003).

Wright, D.J., 2005, Geospatial digital rights management: U.S. Geological Survey Open-File Report 2005-1086, 8 p.

Such agreements would prevent actions, such as redistribution of data, that are not advantageous to providers. Parties involved in data movement and distribution must decide what can and cannot be done to or with the data, and be certain that these terms will be followed (Joffe, 1998).

Data providers that depend on revenue from the sale of data to remain economically viable must be able to put limits on the use of their data. However, once data providers send data out to distributors and users, they no longer have any direct control over the use and movement of their data. Therefore, they must make agreements with distributors to protect their interests. To maintain relations with data providers, distributors must be able to control who can access and use data, and how they use the data.

Geospatial data pose unusual problems for the protection of property rights. A typical use of geospatial data involves extracting information from multiple data sets and integrating that information to create a new data set, thus entering gray areas of intellectual property. It is, therefore, necessary to have detailed terms and conditions for the many aspects of access, use, and dissemination to protect the providers' interests. Historically, these agreements have relied upon subjective human judgment, the goodwill of users, the threat of litigation, and the discretion of individuals involved in the distribution process.

However, as Coyle (2004) notes, "Neither copyright law nor contracts assert any actual control over the behavior of users of materials. Instead, they rely on the parties to act within the stated agreement or law." With the advent of digital methods of data distribution, the scale and ease of data movement have both increased, placing more emphasis on enforcement of these agreements, while simultaneously becoming more difficult to enforce solely through human judgment. Digital Rights Management (DRM) allows new possibilities in precise and rigorous management of data access and use.

What is Digital Rights Management?

DRM is the concept of digital enforcement of rights for the access and use of data. DRM provides an automated system that will consistently and rigorously enforce agreements made among users, providers, and distributors. It allows the distributor of data to control how and by whom data are used, in accordance with rules and agreements.

A good DRM system serves several purposes. First, it makes sure that agreements and contracts are rigorously observed. Second, it eases the process of data distribution, and works to ensure data quality and oversee any necessary financial transfers. Third, it protects the basic rights of privacy, property, and information security.

There are several main components to a DRM system. One is the data. Another component is the rights policy, which is a document attached to the data that specifies what can and cannot be done to and with them. A third component is the DRM framework, which provides for the movement of data and ensures that the rights specified by the rights policies are enforced (Iannella, 2001).

The DRM framework serves to preserve and apply rights policies to the data to which they are attached. The DRM framework must ensure that the rights policy is followed, and also ensure that the policy remains attached to the data, unchanged unless the policy itself provides for modifications.

A functional architecture of a DRM framework is split into three areas: intellectual property (IP) asset creation and capture, IP asset management, and IP asset usage. At asset creation, the provider of the asset (in this case, geospatial data) assigns a rights policy detailing what can and cannot be done with the data. In asset management, the data asset is transferred, but the provider's interests remain identified in the rights policy that accompanies the asset. In asset usage, the asset is accessed and used by the end user, in accordance with the terms of the rights policy. All of these components of the framework must be within the same system, otherwise it is impossible to ensure that the rights policy will be enforced (Iannella, 2001).

Coyle (2004) notes that, "Because digital materials must be mediated through software and hardware for use, it is possible to exercise *a priori* control over access to and use of the content through that technology." Effective controls require that the data and the software used for data management, transmission and usage remain within a unified DRM framework.

What is a Rights Expression Language?

A rights expression language (REL) is a language that provides a syntax and vocabulary for the expression of agreed-upon rights and the conditions to which those rights are subject. Every rights policy is written in a REL. RELs are designed to be machine-actionable, so they must have a precise and organized syntax. They must also have a very precise vocabulary, so as to avoid vagueness in instructions (Coyle, 2004).

To have a functional DRM system, it is necessary to have a standard REL throughout the entire framework. Different software can process the REL and apply the policies, but as long as all software involved understands the same REL, that REL is precise, and the software works correctly, the same results will always occur.

The choice of REL is integral to the design of a DRM system. The DRM framework must be able to distinguish among the types of data for which control is exercised, and the various types of control to be exercised. RELs provide an initial syntax and vocabulary for basic data types and actions. However, geospatial data have unique data types and processes for extracting and combining data. Therefore, the most important qualities of a REL for geospatial data are extensibility and flexibility to handle these unique aspects of geospatial data. Another desirable characteristic for a REL is that it be sufficiently abstract to allow for any needed extension and modification.

There are many rights expression languages. Two prominent ones are MPEG-21/5 and Open Digital Rights Language (ODRL). MPEG-21/5 is designed especially for use with

media, such as video and audio recordings, and is integrated into a system of standards for such digital resources. This gives it the great boon of being extensively implemented from the beginning.

ODRL is "a standard language and vocabulary for the expression of terms and conditions over assets. ODRL covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations" (Iannella, 2002). ODRL is designed to define almost any type of agreement, is independent of media or content, and is extremely abstract (Coyle, 2004).

The most important characteristics of ODRL are its flexibility and extensibility. It has no intended media type for its use, and can be modified extensively. Because it is open-source and based on the eXtensible Markup Language (XML), modification is free and simple. Another advantage of its flexibility is that it does not mandate any specific DRM software to use it; it is merely a language for expressing rights. ODRL, however, does have some disadvantages. One is that ODRL does not control access, but only usage. Therefore, another system must be used for identification and validation of users. ODRL, though not initially designed with an implementation available, has also been tested and a form of it is used in the popular OMA DRM standard.

The key element to the flexibility of ODRL is the data dictionary. This is a part of ODRL that defines data types, constraints, and many other parts of ODRL, and can be very easily added to and modified. The basic categories of the ODRL data dictionary are rights, expressed as permissions, and the limits on those rights, expressed through context, constraints, and requirements. Permissions are actions that a user is able to perform if they meet the constraints and requirements on the permission. Contexts apply not only to permissions, but also to parties involved, and merely serve to give more information about the entity with which they are associated. Constraints define things that must be true for the user to have the permission, and requirements are actions, such as payment, that a user must take to exercise the permission. The data dictionary can be easily extended or modified, to create new entities of any type within the basic ODRL syntax, which can also be modified.

Geospatial Data and ODRL

Geospatial data are a fairly specialized use for a REL, and the geospatial community may find it inefficient and too costly to develop a completely new REL specifically for geospatial data. A better choice is to find an existing REL that is sufficiently extensible, flexible, and abstract to take advantage of uses that the REL has in common with other application communities, but also to allow the expression of interests unique to the geospatial community. ODRL is a REL that meets those criteria.

As an example of the application of ODRL to geospatial data, consider a provider of Digital Orthophoto Quadrangles (DOQs). The provider wishes all of their DOQs to be available freely for viewing and aggregation to Emergency First Responders. All others will be able to view DOQs for free at a resolution of 1 (measured by an arbitrary scale

from 1 to 10), but must pay $10.00 per view at higher resolutions. Also, all will be able to aggregate these DOQs into other data by paying a one-time fee of $75.00.

The permissions to be granted are “display” and “aggregate.” The exact meanings of these terms are defined by the software that reads the rights policy. In general, display is the right to simply view the data, and aggregate is the right to use the data by integrating them into another set of data.

The first step to express this rights policy is the definition of terms within the data dictionary. If one wishes to add a way of dealing with resolutions to ODRL, the basic vocabulary of ODRL can be extended to include this concept. A new constraint named “res,” an integer with a range of 1 to 10, is declared. The resolution of the data will be contained within the data themselves, and the software checks the data’s resolution against the constraint to enforce the rights policy.

The dictionary extension begins by incorporating into itself the base ODRL data dictionary and syntax at http://odrl.net and declaring itself as existing at http://example.net as GEO-DD.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://example.net/GEO-DD"
                        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                        xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
                        xmlns:geo="http://example.net/GEO-DD"
                        elementFormDefault="qualified"
                        attributeFormDefault="qualified">
    <xsd:import namespace="http://odrl.net/1.1/ODRL-EX"
            schemaLocation="http://odrl.net/1.1/ODRL-EX-11.xsd"/>
```

A new constraint of resolution, defined as “res,” is added to the basic ODRL vocabulary.

```
    <xsd:element name="res" type=”xsd:positiveInteger”
            substitutionGroup="o-ex:constraintElement"/>
</xsd:schema>
```

The rights policy begins by accessing the ODRL syntax and data dictionary at odrl.net and the geo data dictionary extension at http://example.net.

```
<?xml version="1.0" encoding="UTF-8"?>
<o-ex:rights xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
                        xmlns:o-dd=”http://odrl.net/1.1/ODRL-DD”
                        xmlns:geo=”http://example.net/GEO-DD”>
```

The policy begins the agreement, defining the asset (the DOQ) attached as having the unique id UNIQUEDOQ112.

```
<o-ex:agreement>
    <o-ex:asset>
        <o-ex:context>
            <o-dd:uid>UNIQUEDOQ112</o-dd:uid>
        <o-ex:context>
    </o-ex:asset>
```

The first permission granted is the right to display the asset at the resolution of 1.

```
    <o-ex:permission>
        <o-dd:display>
            <o-ex:constraint>
                <geo:res> 1 </geo:res>
            </o-ex:constraint>
        </o-dd:display>
    </o-ex:permission>
```

The second permission is to display and aggregate the asset, with no cost, if the group constraint is met by the user being in the group of Emergency First Responders (EmFiResp).

```
    <o-ex:permission>
        <o-dd:display/>
        <o-dd:aggregate/>
        <o-ex:constraint>
            <o-dd:group>
                <o-ex:context>
                    <o-dd:uid>EmFiResp</o-dd:uid>
                </o-ex:context>
            </o-dd:group>
        </o-ex:constraint>
    </o-ex:permission>
```

The third permission introduces a requirement, which is an action that must be taken to enact the permission granted. In this case, the permission is to display, and the requirement is that the user pay a fee of $10.00 U.S. Dollars (USD) per use.

```
    <o-ex:permission>
        <o-dd:display/>
        <o-ex:requirement>
            <o-dd:peruse>
                <o-dd:payment>
                    <o-dd:amount o-dd:currency=”USD”>
                        10.00
                    </o-dd:amount>
                </o-dd:payment>
            </o-dd:peruse>
```

```
            </o-ex:requirement>
        </o-ex:permission>
```

To aggregate the data, a single one-time prepayment of $75.00 USD is required.

```
        <o-ex:permission>
            <o-dd:aggregate/>
            <o-ex:requirement>
                <o-dd:prepay>
                    <o-dd:payment>
                        <o-dd:amount o-dd:currency="USD">
                            75.00
                        </o-dd:amount>
                    </o-dd:payment>
                </o-dd:prepay>
            </o-ex:requirement>
        </o-ex:permission>

    </o-ex:agreement>
    </o-ex:rights>
```

This example shows only a few of the possible rights that can be expressed using ODRL, but represents the form all expressions would take. Many more permission, constraint, and requirement types are available. As shown in the data dictionary extension above, it is very easy to define new elements of various types needed for geospatial data.

Conclusion

Geospatial Digital Rights Management is a way of ensuring that agreements made between creators, distributors, and users of geospatial data are adhered to and honored by all parties. The distributor must create a DRM system with a framework to implement the rights described in right policies, written in a REL. Because the REL is the foundation of a good DRM system, it must be carefully chosen. ODRL has the qualities of flexibility and extraction needed for geospatial data.

Bibliography

Coyle, Karen. 2004. Rights Expression Languages, A Report for the Library of Congress. Library of Congress Website at www.loc.gov/standards/relreport.pdf (accessed August 4, 2004).

Joffe, Bruce. 1998. The GIS Data Sales Dilemma: Finding a Middle Ground. Open Data Consortium Website at www.opendataconsortium.org. (accessed July 12, 2004).

Joffe, Bruce. 2003. Data Distribution Policy Issues. Open Data Consortium website at www.opendataconsortium.org. (accessed July 12, 2004).

Iannella, Renato. 2001. Digital Rights Management (DRM) Architectures, D-Lib Magazine, June 2001, 7(6).

Iannella, Renato. 2002. Open Digital Rights Language (ODRL) Version 1.1. W3C Note, 19 September 2002. W3C website at www.w3.org/TR/odrl. (accessed August 4, 2004).

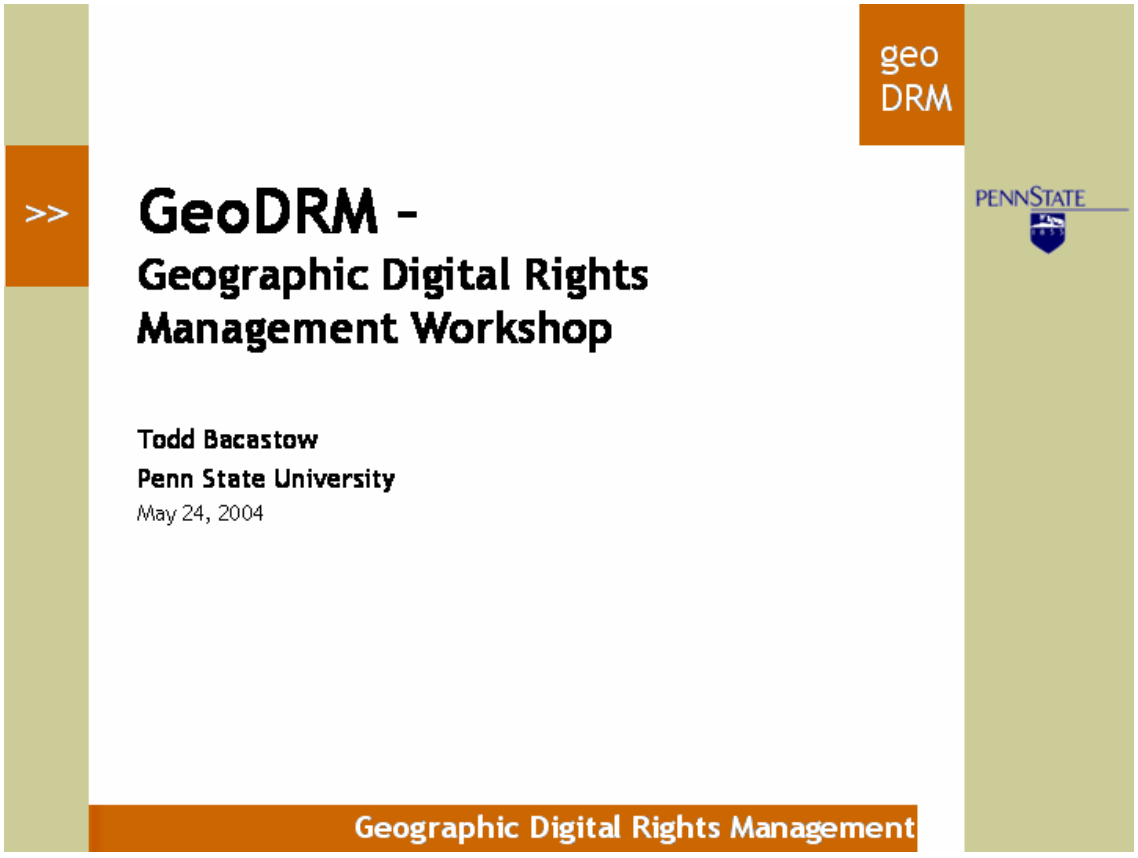
Privacy Working Group, US Information Infrastructure Task Force. 1995. Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, October 1995. U.S. Department of Health and Human Services Website at http://aspe.hhs.gov/datacncl/niiprivp.htm (accessed August 19, 2004).

Appendix C. GeoDRM - Geographic Digital Rights Management Workshop

About Todd Bacastow

Todd S. Bacastow, PhD, is Assistant Director of the Earth and Environmental Systems Institute in the College of Earth and Mineral Sciences at Penn State University. He served as President of the GeoData Alliance from 2002 to 2004.

The 18 slides of a presentation Todd Bacastow made 24 May 2004 in Denver, Colorado are provided on the following pages.



geo DRM

PENNSTATE

>>

Topics

- geoDRM – what is it?
- geoDRM requirements
- geoDRM initiative
- Your input is appreciated

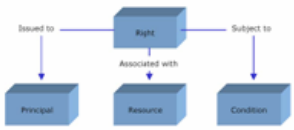
geo DRM

PENNSTATE

>>

Almost Indisputable Truisms

- The owner of a resource gives usage rights to a user
- These rights are associated with the use of a particular resource, e.g., a data set or service.
- The rights can be subject to certain conditions, e.g., the right to copy



Geographic Digital Rights Management

geo DRM

PENNSTATE

>>

Definition

- Geographic Digital Rights Management (geoDRM) - providing the owner a means to issue and manage rights associated with their geospatial resources

geo DRM

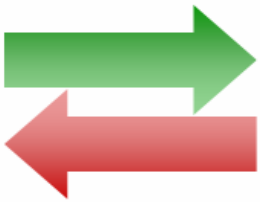
PENNSTATE

>>

Geographic Rights Management Challenges

- US spatial industry behind Europe
- Existing approaches have limitations, are immature, and don't generally apply to the spatial domain
- **Ripe for proprietary schemes!**

Technology
- Convenience
- Standards
- Control



Expectations
- Free content
- Open access
- Easy-to-use

Geographic Digital Rights Management

geo DRM

PENNSTATE

>>

Geographic Rights Management

- **Prospects**
  - Enforce standards
  - Protect Innovation
  - Understand their customer
  - Commingle public and private data and services
  - Meet the need of public agencies that want to retain IP rights to their geospatial data
  - Serve to the web services sector
  - Address emerging HS needs
- **Problems**
  - Could be used to inappropriately limit access
  - Can be seen as going against tradition
  - Increase complexity
  - Opens the door to Big Brother

Geographic Digital Rights Management

geo DRM

PENNSTATE

>>

What's Different About Applying DRM technology to the Spatial Domain?

- Scales matters
- Data is a complex mix of BLOBs and tables
- Type of control can depend on representation
- Large data volumes
- User seeks synergism of including different data sources (a.k.a., layers)

Geographic Digital Rights Management

geo DRM

PENNSTATE

>>

DRM

- Different approaches abound …..
  - Provider approach: *Protect* the owner's rights through *enforcement*, and support licensing model
  - User approach: *Enable access* while managing intellectual property and protecting user's privacy (i.e., distributed sharing and collaboration model)

Geographic Digital Rights Management

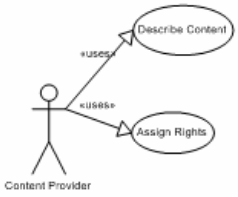
geo DRM

PENNSTATE

>>

"Content-based" DRM Model

- One-to-one
- Pay-per-view
- Trusted systems
- Use monitoring
- Static content
- User as consumer
- Proprietary hardware/software
- Not readily adaptable to services



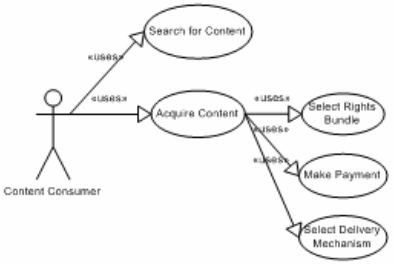
Geographic Digital Rights Management

"Usage-based" DRM Model

geo DRM

>>

- One-to-many
- Flexible access
- User as consumer and producer
- Dynamic content and services
- Inter-organizational, cross realm access
- Privacy
- Interoperability



PENNSTATE

Geographic Digital Rights Management

What's Needed?

geo DRM

>>

- Combination of both views
- Federated approach for both data and services
- Flexible yet secure access
- Trust communities
- Maintain privacy
- Open standards
- Open source

PENNSTATE

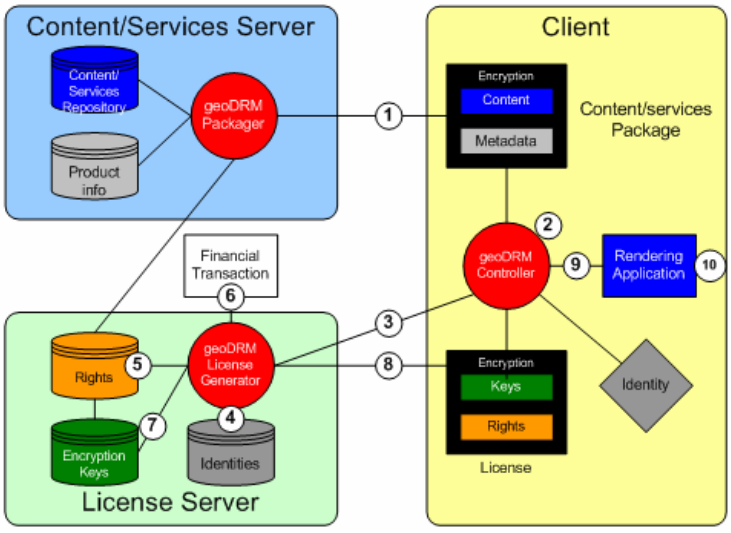
Geographic Digital Rights Management

geoDRM Project

- Fundamental Project Goal:
  - Enable intersection of attributes about user, content and usage to manage content and services
- Cooperative effort
  - GeoData Alliance
  - Open GIS Consortium
  - FGDC
  - Open Data Consortium

Geographic Digital Rights Management

geoDRM Reference Architecture



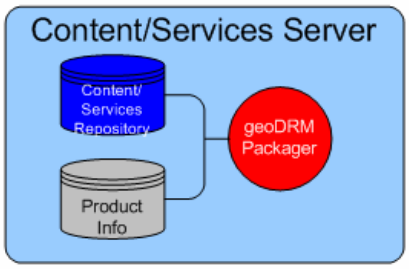
Geographic Digital Rights Management

Content/Services Server

geo DRM

PENNSTATE

- Content/Services Repository
  - Content and services management system
  - File and services server
- Product Info
  - 'Traditional' metadata
  - Services metadata
- geoDRM Packager
  - Applies unique user rights
  - Packages
  - Encrypts



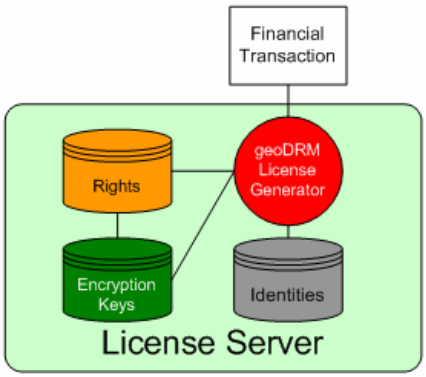
Geographic Digital Rights Management

License Server

geo DRM

PENNSTATE

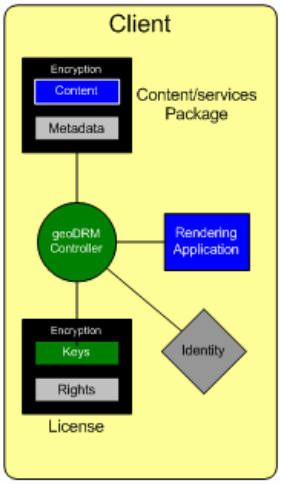
- Encryption key repository
- User identity database
  - Usernames
  - Machine IDs
- geoDRM License Generator



Geographic Digital Rights Management

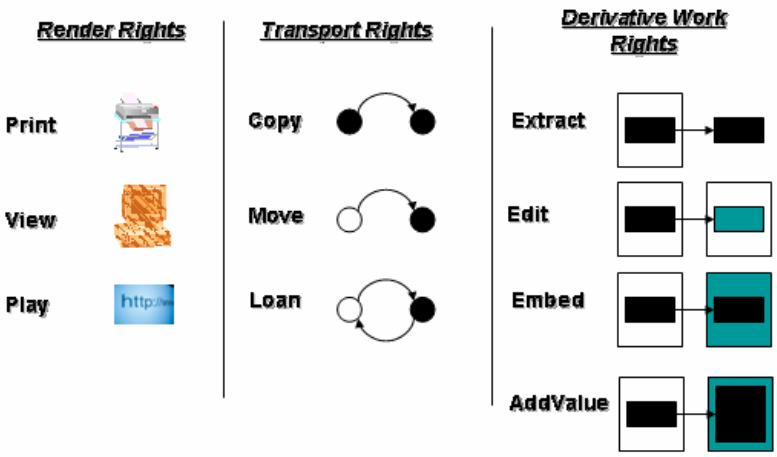
Client

- geoDRM Controller
  - Integrator
- Interfaces with rendering application
- Content/services packages
- Licenses
- Identity



Geographic Digital Rights Management

A Few Metadata Elements



Geographic Digital Rights Management

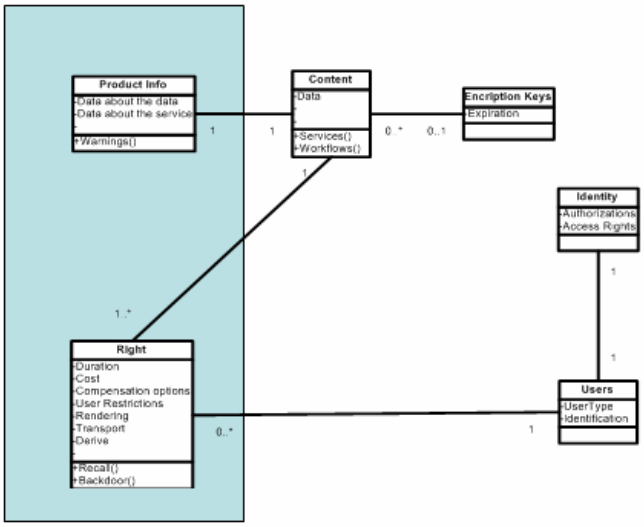
geo
DRM

PENNSTATE

>>

Metadata

(data+process+rights)



Geographic Digital Rights Management

Appendix D: Mission and Objectives of OGC GeoDRM Working Group[13]

Mission

A great deal of work has been done in the area of data ownership and rights management. This work is of interest to the Geospatial community in that many geospatial data providers need to control or track who has access to their data and how it is used. The lack of a Geospatial Digital Rights Management (GeoDRM) capability is a major barrier to broader adoption of Web based geospatial technologies. The mission of the GeoDRM Working Group is to coordinate and mature the development and validation of work being done on digital rights management for the geospatial community.

Background and Problem Statement

As geographic content (geodata) and services become more widely available in digital form over ubiquitous networks, data becomes easier to distribute, share, copy and alter. While this is generally a good thing, many organizations involved in the production and trading of geodata find the need to protect their Intellectual Property (IP) assets through the digital distribution value chain. Organizations want to specify, manage, control and track geodata distribution within secure, open and trusted environments. A system of operating agreements and interoperable technologies are needed to enable broader distribution and use of geodata while protecting the rights of producers and users.

In or e-commerce models for dissemination and use of Intellectual Property (IP) assets, geodata are treated as commodities to be priced, ordered, traded and licensed. Direct monetary reward, however, is often not the motivation or is only secondary behind the desire for more rigorous control of IP assets. Harlan Onsrud of the GeoData Alliance argues that the incentive structures implicit in "library systems" are an appropriate model for motivating data producers, collectors and traders to document, share and otherwise disseminate their geodata. Onsrud observes that the library system is a "chaordic" framework of seemingly ad hoc agreements among stakeholders that strikes a balance supporting "…strong public goods, access and equity principles while fully protecting the intellectual property rights of authors and publishers."[14]

Rapid technological advances have tipped the balance of laws that establish incentives for producers to make their content available while maintaining the access, use and equity rights of users. Onsrud envisions the establishment of a framework of operating agreements, similar to that in which libraries develop and share resources, as one way to reestablish a way for geodata to be more accessible and useful to a larger numbers of users.

---

[13] Reprinted directly from the OGC web site at http://www.opengeospatial.org/groups/?iid=129

[14] Harlan Onsrud, "Exploring the Library Metaphor in Developing a More Inclusive NSDI." http://www.geoall.net/library_harlanonsrud.html

The specific requirements for protecting IP rights by controlling geodata distribution and use, however, are extremely complex and vary widely depending heavily on factors such as:

* The “business” of the organization (i.e., the motivations of commercial, public-sector, and academic organizations to make their geodata available)
* The type of data and media formats (e.g., physical, electronic, text, graphic, audio, video, vector, raster, observation, etc.)
* The content distribution channels (e.g., size of content, network bandwidth, types of end devices)
* The types and granularity of intellectual property rights to be protected and the contractual obligations for its use (e.g., unlimited distribution, license to use, license to reuse parts, limited distribution, sensitive/classified, etc).

Just as the requirements vary, so does the enabling technology. Digital Rights Management (DRM) is a popular term for a field that emerged in the mid-1990s when content providers, technology firms and policymakers began to confront the imbalance of technology and laws caused by the effect of ubiquitous computer networks on the distribution of copyrighted material in digital form. DRM is about creating, packaging, distributing, controlling and tracking content based on rights and licensing information. DRM is closely integrated with Content Management System (CMS) technology for creating metadata, storing and organizing digital content in support of workflow, search, browse, access and retrieval processes by users in workgroups, enterprises and information communities. It is also dependent on Information Security technologies to provide the trusted infrastructure for DRM and E-commerce to address the financial transactions necessary to procure rights to geospatial content.

Objectives

The objectives for the GeoDRM Working Group are:

· Enable business models for web-based geospatial services by identifying or developing a trusted infrastructure for purchasing and protecting rights to digital content,

· Guide the development of OGC specifications and best practices recommendations to permit the exploitation of mainstream DRM approaches, technologies and standards wherever possible

· Test, verify and mature as necessary the technologies required for geospatial DRM including electronic commerce and information security,

· Develop specifications for geospatial DRM that build on the OGC technical baseline.

[1] Harlan Onsrud, “Exploring the Library Metaphor in Developing a More Inclusive NSDI.” http://www.geoall.net/library_harlanonsrud.html

Appendix E: Geospatial DRM Policy Forum

December 9, 2004
8:30 AM to 12:30 PM
Diplomat Room, State Plaza Hotel, 2117 E St. N.W., Washington, DC.

Individuals from the public, private and non-profit sectors were invited to identify and begin to address the policy challenges presented by implementation of an interoperable digital rights management framework for geographic data and services.

Kathy Covert, FGDC, opened the session by referring to a statement made by Harlan Cleveland: it is important to put a policy wrapper around new technology before it goes running naked in the world. She described this forum as part of an ongoing project that started in 2002.

Everyone around the room gave a brief self-introduction before the formal program got underway. Joe Cardinale (OGC) and Tim Case (GDA) presented an overview of technology, policy implications and the status of initiatives of the Open Geospatial Consortium (OGC) and the GeoData Alliance (GDA).

Tim talked about digital rights management in the context of the recording industry. The November 2004 issue of *Wired* magazine introduces the opposing perspectives of Hilary Rosen, former CEO of the Recording Industry Association of America, and Lawrence Lessig, Stanford Law Professor and chair of the Creative Commons. (www.wired.com/wired/archive/12.11/larry.html)

Tim also cited Bruce Joffe's article in the Fall 2004 issue of *ArcNews*: "Open Data Consortium Proposes Geodata Portal Requirements." The article provides, in Tim's words, a "holistic perspective of licenses." The article is available on the web site of the Open Data Consortium. (www.opendataconsortium.org/documents/AN_OpenData.pdf)

Participants brought up various topics:

- Identity management (Steve Marley)
- Community access to regional analyses is one needed use case; inter-government data sharing is another one (Bruce Cahan)
- Interest in GeoDRM is amplified by access issues and privacy issues (Mark Reichardt)
- Though access and DRM initially sound like opposites, it appears they are **not** (Chuck Heazel)

Joe Cardinale presented information about the activities of the OGC Working Group (WG). The purpose of the WG is **not** to develop technology; it is to **use** existing technology.

He included a figure developed by Graham Vowles that shows interrelationships and the DRM playing field. It includes five user profiles or areas that each need use cases.

Participant Steve Marley raised the importance of goals in clarifying the completeness of the work.

Joe invited anyone who wants to participate in the weekly OGC WG calls to send him an email for the information about the calls. OGC has a use case framework, he encouraged participants to submit use cases.

Then six panelists had an opportunity to present remarks for about five minutes each. The panelists:

- Hari Reddy, ContentGuard Inc., Virginia
- Elaine L. Westbrooks, Cornell University; New York
- Marilyn Otto, MapInfo Corporation, New York
- Randall Johnson, Metropolitan Council, Minnesota
- Jeff Labonte, Geoconnections, Canada
- William G. Miller, U.S. Geological Survey, Virginia

The panelists were given nine questions in advance and were requested to select any one to be the focus of their remarks.

1. What does GeoDRM mean to your organization?
2. What organizations will benefit most from GeoDRM?
3. What job functions will benefit most from GeoDRM?
4. What do you see as the biggest benefit of GeoDRM?
5. What price do we have to pay to realize the benefits of GeoDRM?
6. What is the biggest technical challenge to successful implementation of GeoDRM?
7. What is the biggest policy challenge to widespread use of GeoDRM?
8. When do you think the challenges will be met and we'll see widespread use of GeoDRM?
9. What next step can any motivated individual take to help move GeoDRM forward?

Hari Reddy, ContentGuard Inc., spoke about "Demystifying DRM." He started with an "atomic model." He noted that trust must be bilateral. DRM is following the classical technology advancement S-curve—architectures are being disaggregated.

Elaine Westbrooks, Cornell Library and Chair of the ODRL (Open Digital Rights Language) WG, said the library is scanning 20,000 pages per week; universities are concerned with access and also with preservation. She is interested in ODRL, not XRML or MPEG21, especially because Open is the first word. She noted that the subject is digital rights management, not management of digital rights. ODRL is a plug-in, not a technology. It provides the semantics of language. ODRL is immature and limited today. Development of ODRL needs more support, one can't see today how it will work out. Museums and libraries are interested.

Discussion points:

- Rights expressions can be associated with data, users and applications, what is the focus? Elaine said the focus is on data and users, not applications.
- There is a primitive notion of applications—view-only versus more.

Marilyn Otto, MapInfo, identified three ways MapInfo comes at data: 1) creator, 2) supplier and 3) integrator. She mentioned that for click-through licensing, it was explicitly set up so that the user had to move the cursor to yes. Use of data varies, examples include the touch-it model, server model, value and transaction. Each use and price is another license. (In-car navigation is a separate subject.) They need multiple API[15] strategies; relationship with the end user does NOT scale. Hari agrees on the need for multiple APIs.

Discussion points:

- Distinction between data and information. Marilyn clarified that if you cannot represent your intellectual property without their data, the data must be licensed for a fee.
- use of the transaction model is increasing and cannot be monitored manually.
- Is trust really two-way? The provider has a trust problem, what user has a trust problem? Consider the FEMA flood hazard data online. The user has to trust that the provider will stand behind the data. The user also has to trust that the software is trustworthy!

Randy Johnson, Metropolitan Council, described the experience of his organization. The initial stance was that all data are free, no licenses. Now, parcels and one other layer have licensed. Beginning six years ago, government to government access is free. Effort is underway to automate licensing and standardize licenses. Data sharing is the norm now.

Jeff Labonté, Geoconnections, pointed out that the Canadian experience is different. There, government licensing data is the norm. Public and private interests are on a collision path. The idea of "use cases" does not make sense to a Canadian elected official.

Discussion points:

- Do we need "DRM for Dummies?" Are we trying to automate what people do now? Where will guidance come from?
- The mechanisms have to be flexible, data transfers are not a national matter, are international.
- We need a "starter kit."
- The American Bar Association has a Subcommittee on Intellectual Property[16]. Maybe we need to get them to the table.
- Elected officials don't see this as important.

[15] Application Program Interface

[16] See http://www.buslaw.org/cgi-bin/controlpanel.cgi?committee=CL320010&info=Mission, accessed 31 March 2005.

Bill Miller, USGS, introduced himself as a scientist (not a lawyer or policymaker). He reviewed the scientific method, which includes the concept that experiments need to be repeatable. Thus geospatial data used to reach scientific conclusions today would ideally be available 200 years from now. GeoDRM could potentially hinder the scientific method and therefore science.

Discussion points:

- Migrating digital data to new media to be read by new operating systems is a big cost (already).
- Digital preservation is not proven.

Attendee List

Todd Bacastow
Penn State University
State College, Pennsylvania

Cristina Bories
Raytheon
Maryland

Don Buhler
Bureau of Land Management
Washington, D. C.

Joe Cardinale
Boeing Corporation
Springfield, Virginia

Tina Cary
Cary and Associates
Longmont, Colorado

Tim Case
Parsons Brinckerhoff
Boston, Massachusetts

Kathy Covert
Federal Geographic Data Committee
Reston, Virginia

Michael Domaratz
U.S. Geological Survey
Reston, Virginia

Travis Hardy
ESRI
Vienna, Virginia

Randall Johnson
MetroGIS
Minneapolis, Minnesota

Dennis Klein
Boundary Solutions, Inc.
Mill Valley, California

Jeff Labonte
Geoconnections
Ottawa, Canada

Tony Lupien
TeleAtlas
Baltimore, Maryland

Stephen R. Marley
Raytheon
Maryland

Susan Marlow
Smart Data Strategies, Inc

William Miller
U.S. Geological Survey
Reston, Virginia

Marilyn Otto
MapInfo Corporation
Troy, New York

Jim Plasker
American Society for Photogrammetry and Remote Sensing
Washington, D.C.

Hari Reddy
Content Guard
Virginia

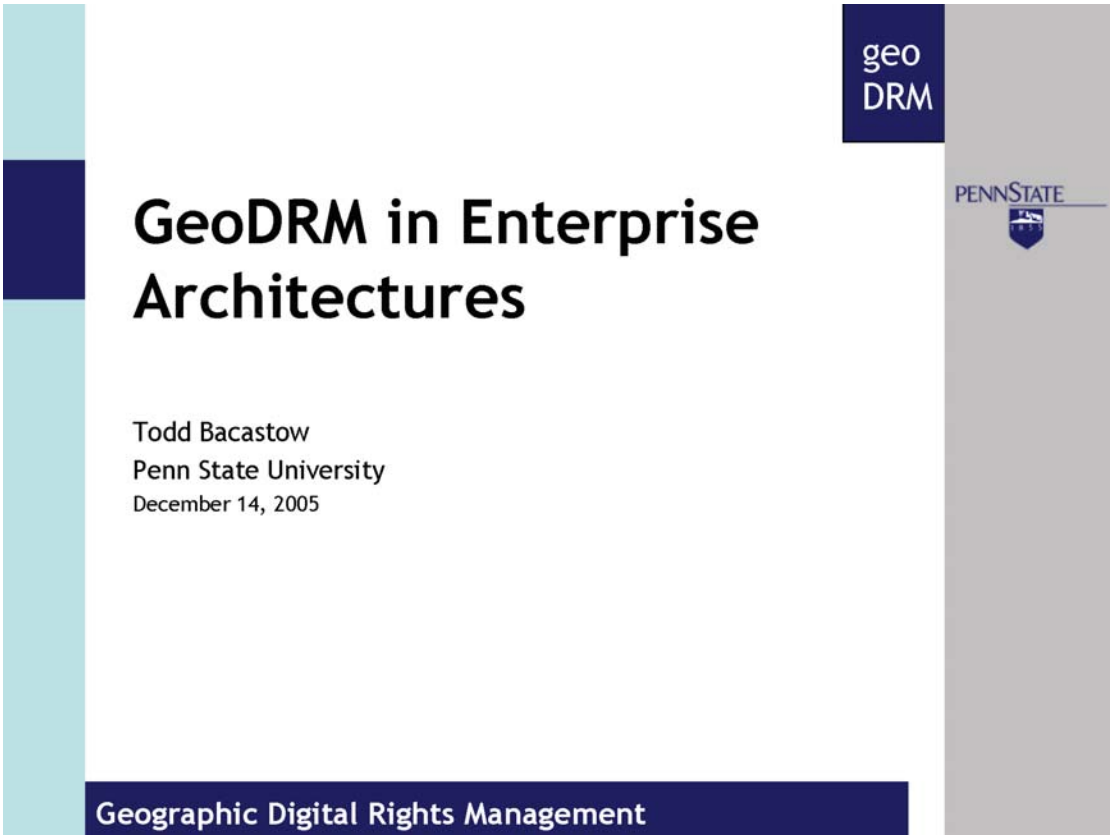
Mark Reichardt
Open Geospatial Consortium
Wayland, Massachusetts

Rebecca Somers
Somers-St. Clair
Fairfax, Virginia

Elaine Westbrooks
Cornell Library
Ithaca, New York

Appendix F. GeoDRM in Enterprise Architectures

Presentations by Todd Bacastow (Penn State University) and Graham Vowles (Ordnance Survey) to the DC Chapter of the Association of Enterprise Architects on 14 December 2005. Panelists for the event included Graham Vowles, Kevin Pomfret (OGC) and Joe Cardinale (Boeing).



geo DRM

PENNSTATE

GeoDRM Project

- Fundamental Project Goal:
  - Enable the intersection of attributes about user, content and usage to manage content and services
- Cooperative effort
  - GeoData Alliance
  - Open Geospatial Consortium
  - FGDC

geo DRM

PENNSTATE

Agenda

- Welcome and Introduction
- Introduction to Geospatial Digital Rights Management
- Panel
  - Graham Vowles (Ordnance Survey)
  - Kevin Pomfret (OGC)
  - Joe Cardinale (Boeing)
- Questions from the Audience
- Closing

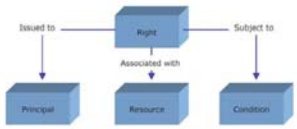
Geographic Digital Rights Management

geo DRM

PENNSTATE

"Almost" Indisputable Truisms

- The owner of a resource gives usage rights to a user
- These rights are associated with the use of a particular resource, e.g., a data set or service
- The rights can be subject to certain conditions, e.g., the right to copy



geo DRM

PENNSTATE

Session Purpose

- A system of interoperable standards are being developed to enable broader distribution and use of geodata while protecting the rights of producers and users.
- This session concerns the current Open Geospatial Consortium, Inc. (OGC) activities in addressing this issue.

Geographic Digital Rights Management

Geospatial Digital Rights Management (GeoDRM)

Graham Vowles (Graham.Vowles@ordnancesurvey.co.uk),
OGC Technical Representative, Ordnance Survey, and Co-chair of OGC GeoDRM WG

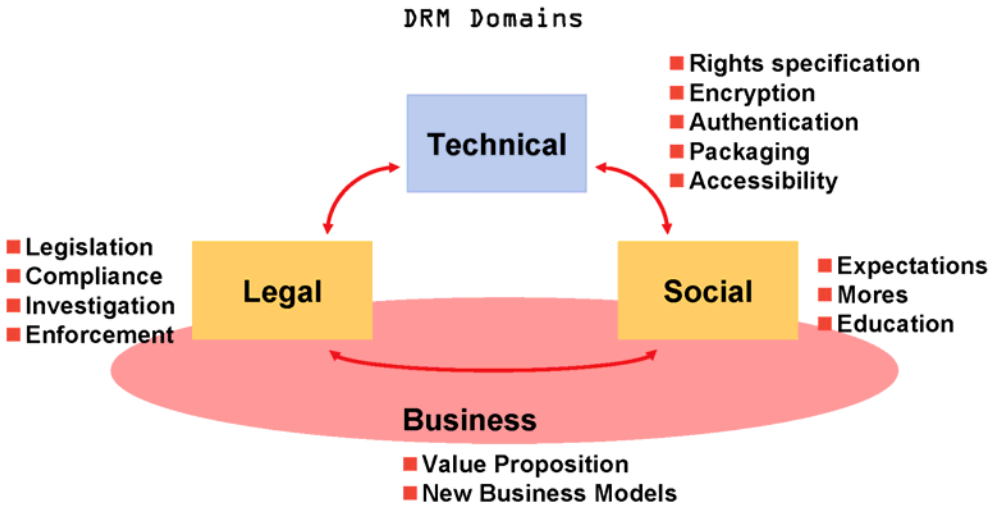
Stream 3 Technology (with Technology SIG)

C01: Foundations and futures

AGI2005 8-10 November, 2005

Chelsea Village, London

DRM consists of a number of technical elements which should be balanced with initiatives in other areas to increase the protection DRM provides.



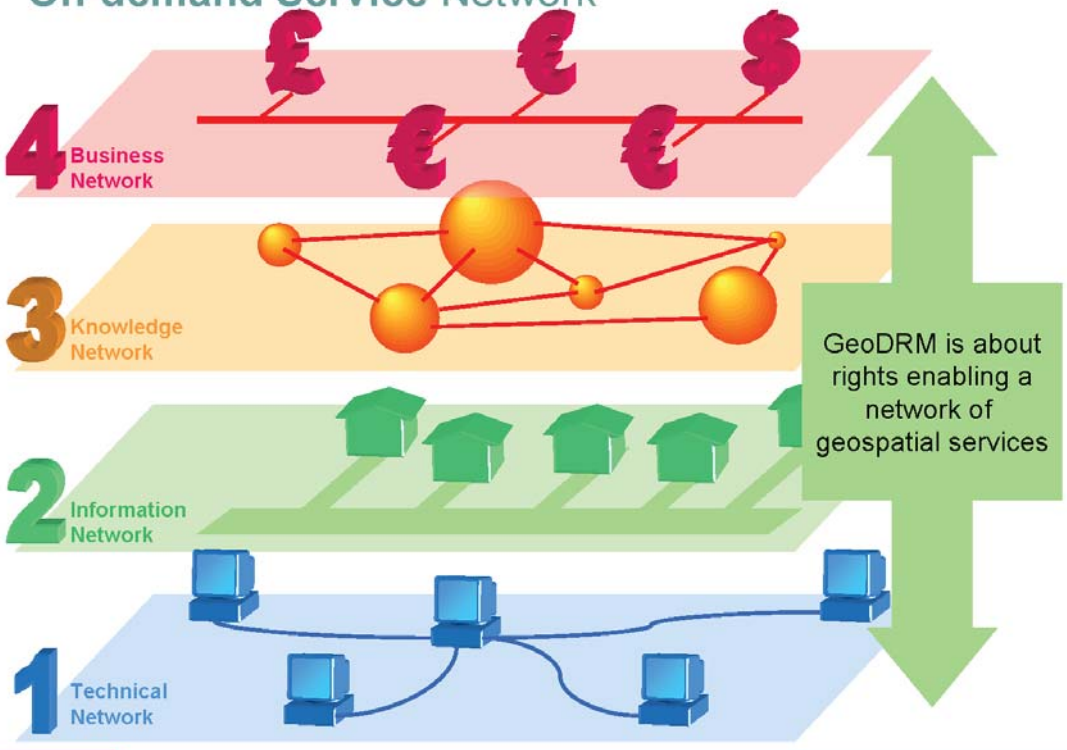
Source: Robert Bolick, McGraw-Hill, 2001

GeoDRM Working Group

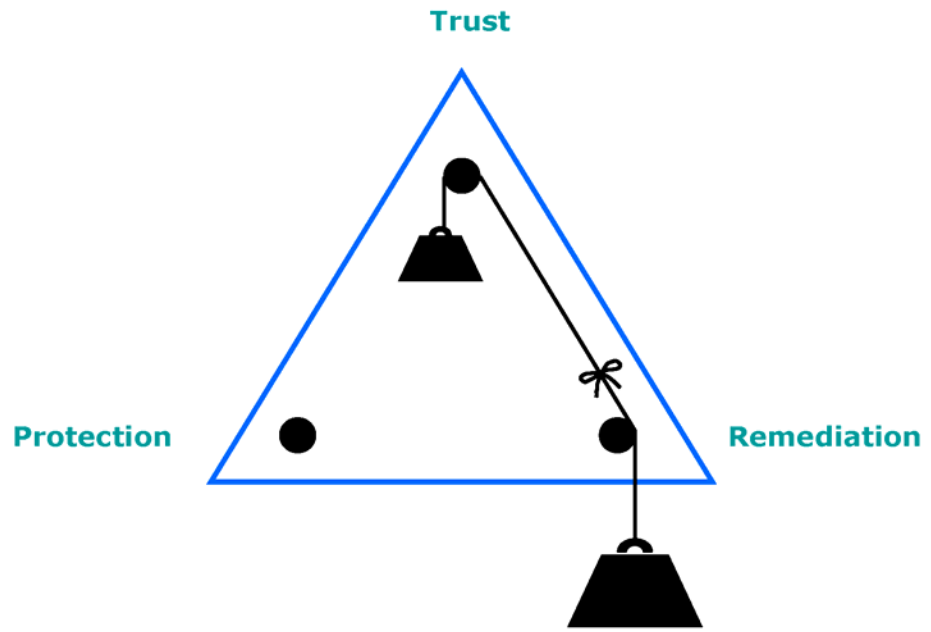
- Part of Open Geospatial Consortium (OGC) – where geospatial standards are defined
- GeoDRM Working Group – comprises of content providers and technology providers
- Charter is not to invent new digital rights technologies but to reuse and extend for geospatial data and services
- Formed in June 2004 – Graham Vowles, Roland Wagner, Joe Cardinale Co-chairs
- Last meeting November 7-11 2005, Bonn, Germany.

OGC™ Technical Committee Member

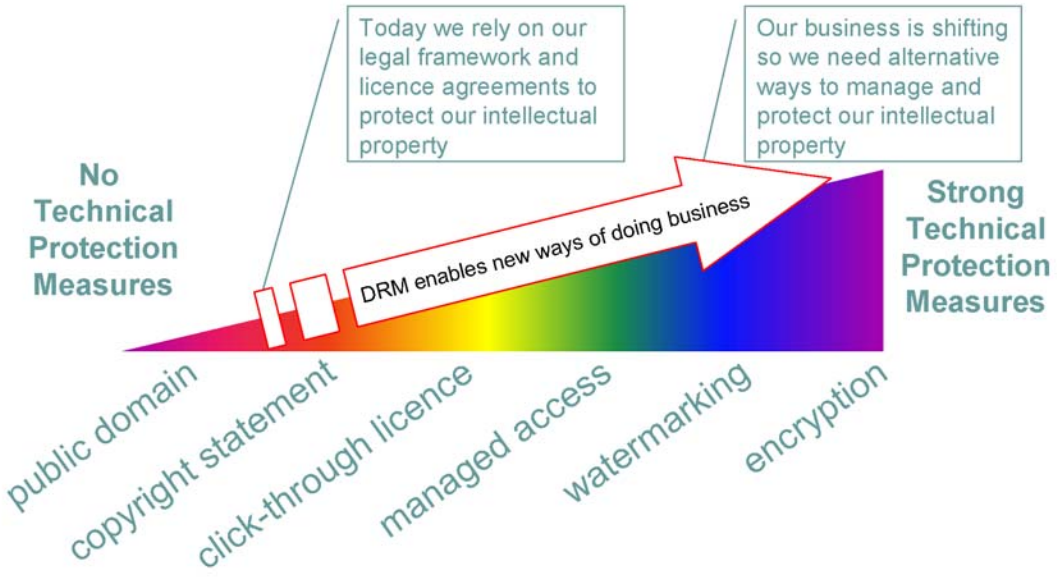
On-demand Service Network



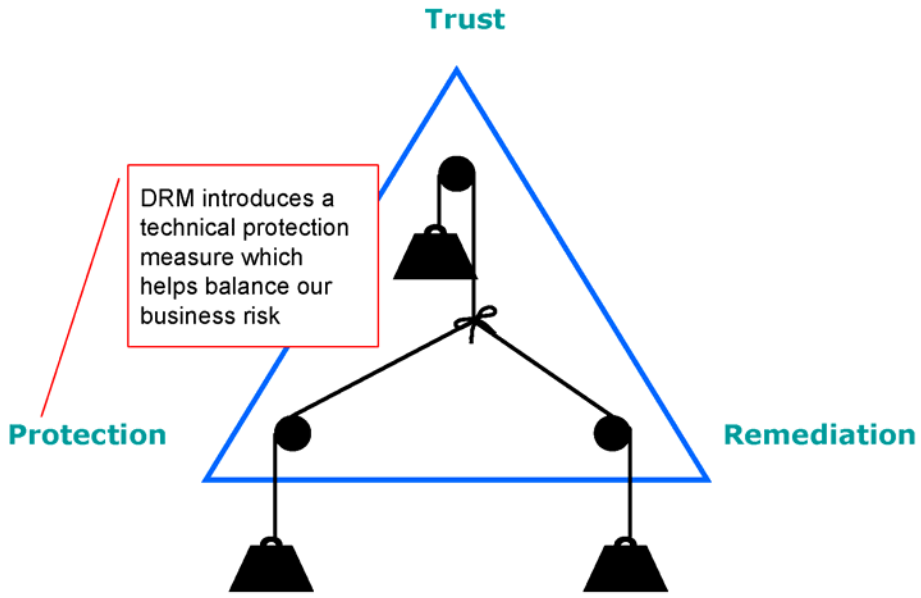
How we do business now…



Ways of managing and protecting Intellectual Property



Introducing technical protection measures into the way we do business…



Digital Media DRM vs Geospatial DRM

Digital Media DRM

•Trade the rights to a discrete object. For example the rights to listen to an audio file

•Business model is B2C and traditional supply chain. Limited number of parties involved in the transaction

•Similar in concept to buying property freehold

•No rights to resell or create derived works

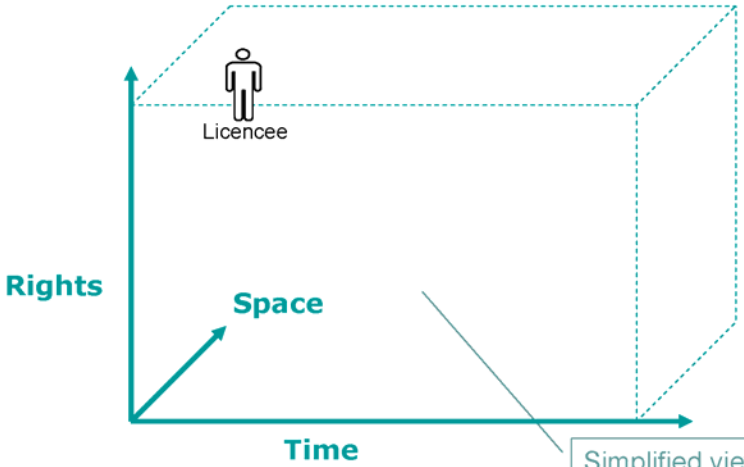
Static Products

Geospatial DRM

- Trade the rights to access a geospatial dataset for a given geographical space for a defined period of time
- Business model is B2B and networked. A number of intermediaries may be required, each playing a specific role within the GeoDRM network
- Similar in concept to renting a property or buying leasehold
- Possibly includes the rights to publishing derived works

Dynamic Services

GeoDRM Licence Extents

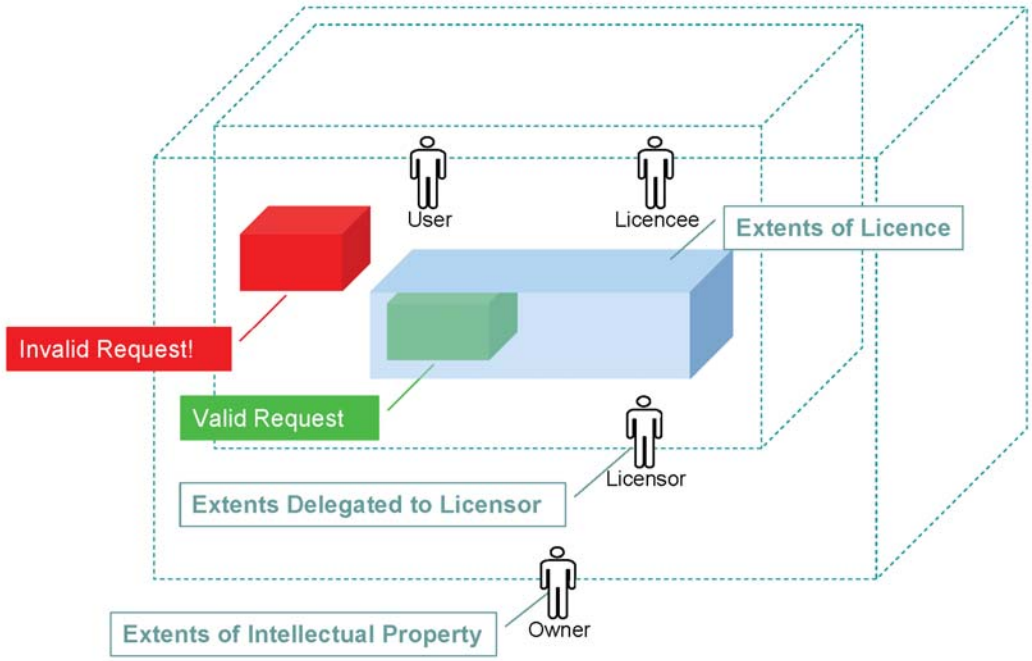


Simplified view of the extents of a GeoDRM Licence: three-dimensions of rights, space and time

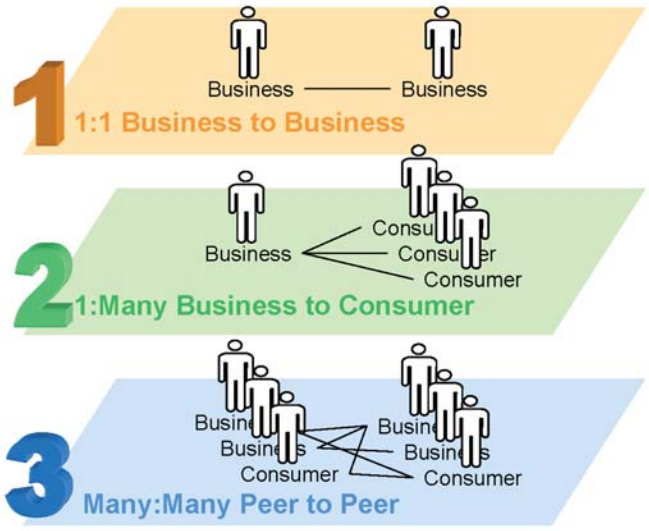
Imagine yourself transported into the GeoDRM universe

- No longer the normal three dimensions – but the intellectual property dimensions of rights, space and time…
- You are now an intellectual property magnate dealing in the rights to access information. A bit like rental agreements in the real world.
- You could directly licence individual users to access "blocks" of intellectual property, or it may be easier to delegate licensing responsibility to intermediaries
- Licence management is the process of ensuring a user's information request falls inside that user's licence extents

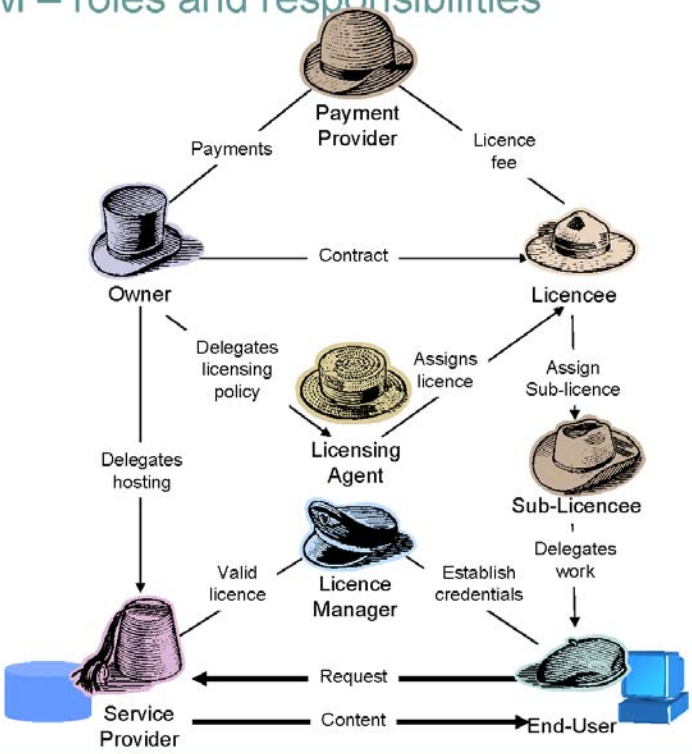
GeoDRM Abstract Rights Model (ARM)



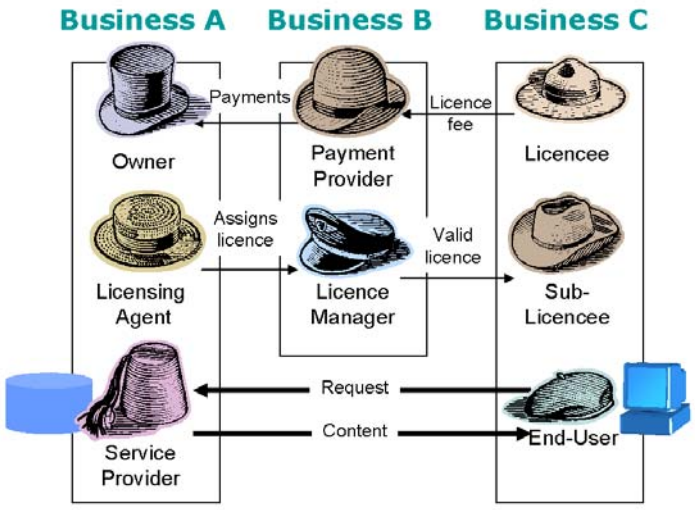
Evolution of Rights Managed Business Models



GeoDRM – roles and responsibilities



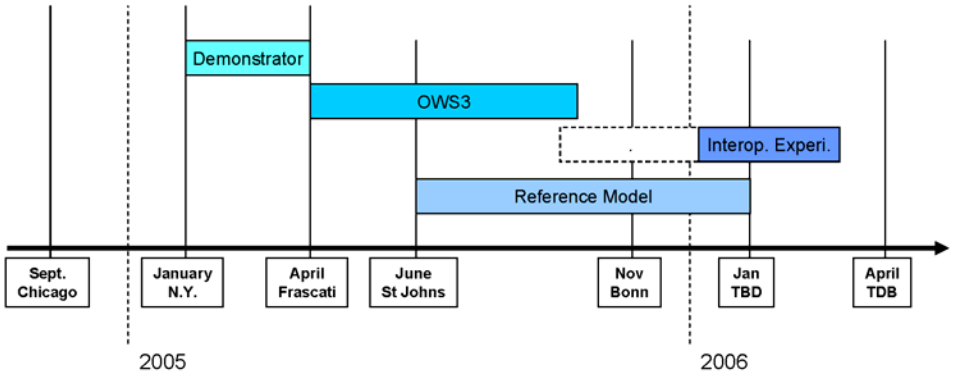
GeoDRM – example business model



GeoDRM Working Group Programme 2005

- Project 1: GeoDRM.Demonstrator
- Project 2: GeoDRM.OWS3 Testbed
- Project 3: GeoDRM.Interoperability Experiment
- Project 4: GeoDRM.Reference Model

Identify
Develop
Consistency
Describe



Conclusions

- **Prepare for the evolution of rights-managed networks**: Ensure that you have assessed the strategic impact of digital rights management on your business, and use that to frame your long-term strategic and near-term operational goals.
- **Develop new business models**: Work closely with your suppliers, partners and customers to establish new ways of doing business over a rights-enabled network of trusted services.
- **Implement solutions based on your operational needs**: Start your current implementation based on your near-term operational needs, but prepare for the longer term through the adoption of emerging standards.
- **Contribute to the definition of emerging standards**: To make sure that standards will support your business model, engage and actively contribute to the standards process – for example, by submitting example use cases. Should your organisation be participating in the current activities of the GeoDRM WG?
- **Look for opportunities to reduce costs and grow revenues**: New channels present new opportunities to deliver more for less. How can you maximise the value you deliver while simultaneously reducing costs to both yourself and your customers?

Ordnance Survey

Thank you!

Graham Vowles
graham.vowles@ordnancesurvey.co.uk

Digital Rights Management – the new economic animal

Consumer Rights

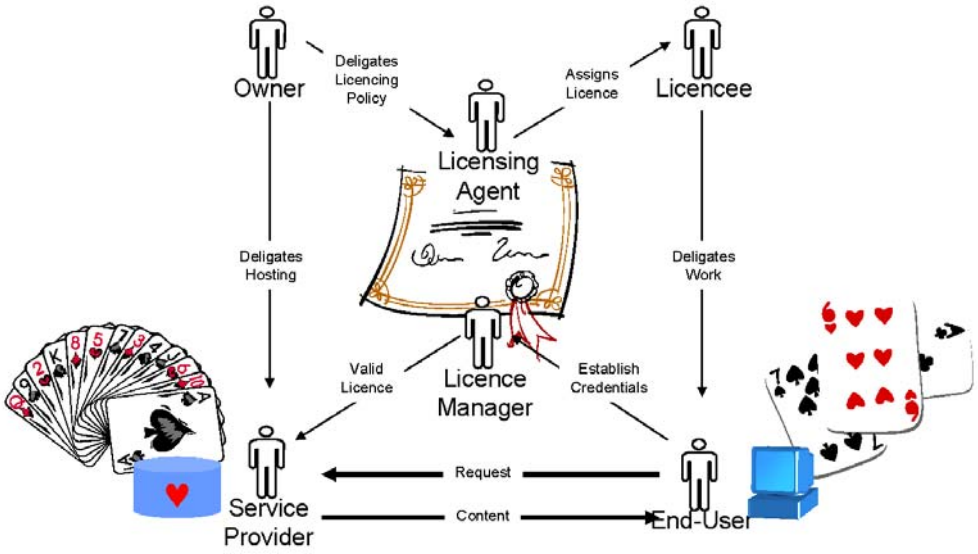
Community
Custodian
Data Sharing
Agreements
Commons

Producer Rights

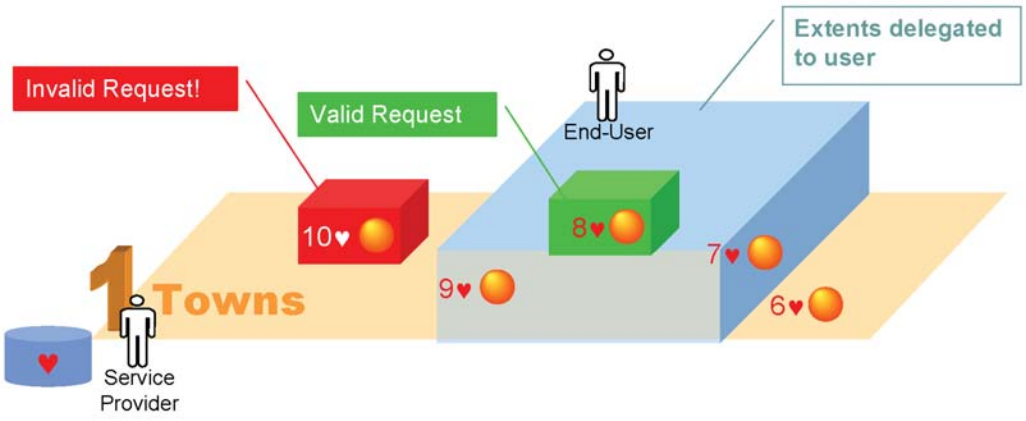
Market
Owner
Access Control
License
Intellectual Property

DRM is about enabling an information economy where the benefits flow both ways

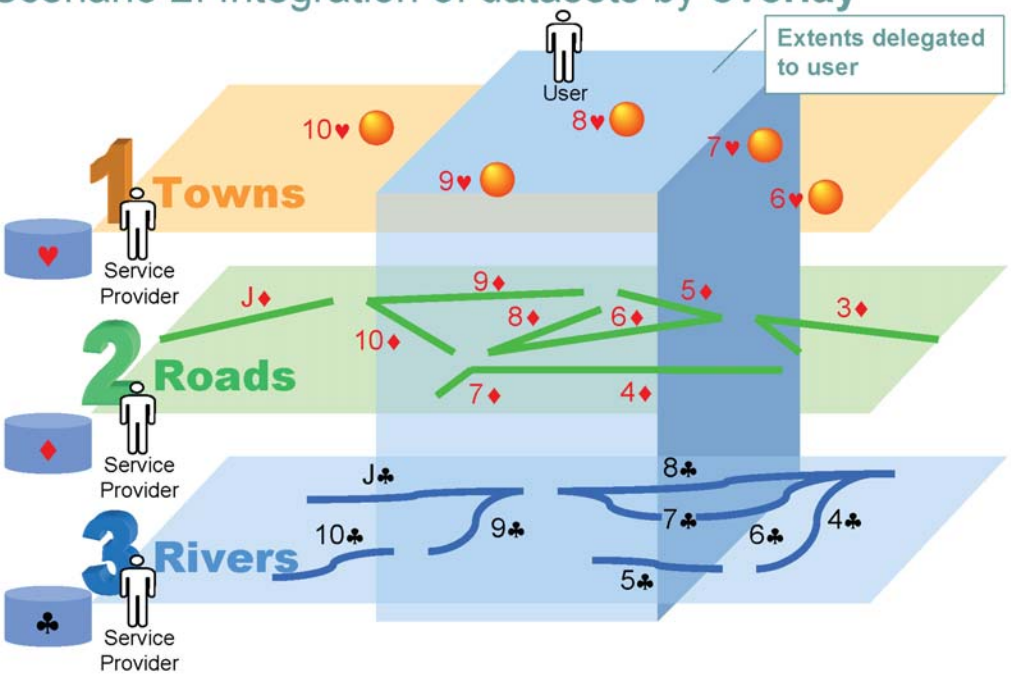
GeoDRM Game – Interactive Role Playing



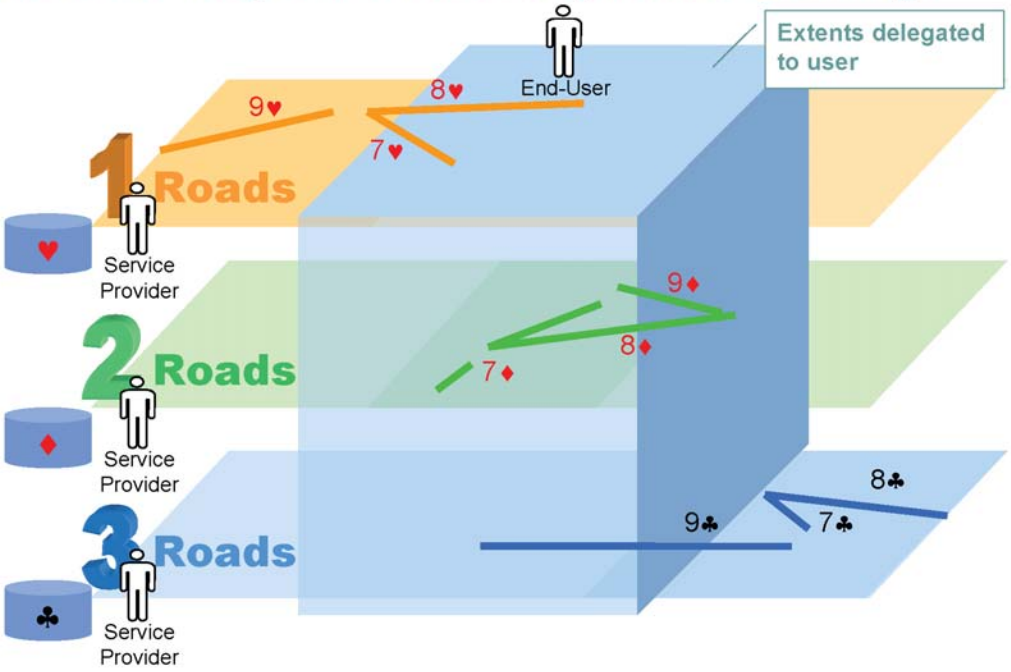
Scenario 1: User accesses content (8♥)



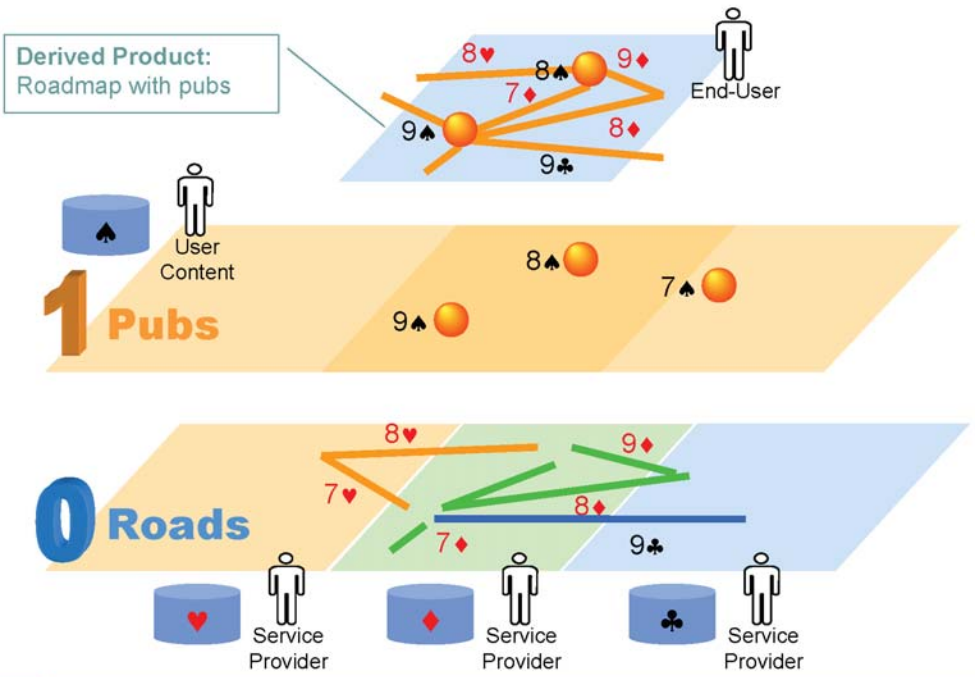
Scenario 2: Integration of datasets by **overlay**



Scenario 3: Integration of datasets by **mosaic – roaming?**



Scenario 4: Derived Product – Adding Content



GeoDRM WG Proposed Direction