Friday, November 2, 2018

Digital Rights Management (DRM)

The National Association of
Government Archives and Records Administrators

444 N. Capitol Street, NW | Suite 237 | Washington, DC 20001 | (202) 508-3800 | info@nagara.org

TABLE OF CONTENTS

Executive Summary

In October 2017, the Board of Directors of the National Association of Government Archives and Records Administrators (NAGARA) voted to convene a working group to study digital rights management (DRM) technologies and their associated impacts on the legal, public policy, and functional aspects of public record keeping. The working group was charged with studying the history of DRM technology, and to make policy recommendations for the association and its members.

The vast majority of work in the public sector is performed on computers and aided by other electronic devices. Government workers rely on the increasingly complex relationships of hardware, software, contracts, and licenses to perform their jobs. Distribution of information through electronic means, especially over the web, has increased the complexity of workflows. In day-to-day work, a typical public servant could use software or hardware developed, owned, or licensed by dozens of individual rights holders. Government archivists and records managers have a duty to ensure this information is useable for its entire lifecycle.

DRM and associated technological protection measures serve as a tool to protect the rights of those creating, providing, or sharing information with other parties, including governmental entities. The use of DRM technologies has grown tremendously in the past two decades. DRM measures are routinely applied to wide-ranging items including audio, video, e-books, electronic documents, lightbulbs, refrigerators, tractors, automobiles, and all sorts of web-connected electronic devices. Beyond impacting public business, this technology is so widespread it impacts most American citizens, and thus deserves both careful study and a policy framework to protect rights-holders and allow legal use of devices and data to preserve the accessibility, authenticity, and reliability of publicly-owned information.

Electronic records of all kinds utilize DRM technologies. DRM measures often go unnoticed by users of technology, but archivists and records managers should be aware that virtually all software used by government entities is protected by DRM of some sort. This has the potential to impact electronic records already in archival holdings and certainly already impacts records in government custody. With the great expansion in government contracting of cloud-based products and services, vendors maintain control over products and data like never before.

It is the responsibility of NAGARA to inform and educate its members, both administrators and practitioners, of the nature of this technology, the legal implications of its presence and use, practical and legal methods for removing access barriers, and techniques for insulating public records and other public property against undue external influence or control.

This paper is the conclusion of the work performed by the working group and includes a high-level overview of DRM technology, the underlying legal framework, activities both permitted and prohibited under current law, and recommendations for the education and awareness of records administrators and archivists.

Legal Framework

A full review of copyright law, rights, licensure, and other matters is far beyond the scope of this paper, but a survey of existing law can provide some of the necessary background and understanding of both the limitations and the scope of activities that are permitted.

DRM is generally applied to protect intellectual property rights. Some specific examples of these rights include patents, trademarks, and copyrights. This paper will focus primarily on copyrights and trade secrets, as they are most relevant in the archives and records management context.

The 1967 treaty that created the World Intellectual Property Organization outlines the definition and scope of intellectual property:

> "Intellectual property shall include rights relating to:
> - literary, artistic and scientific works
> - performances of performing artists, phonograms and broadcasts
> - inventions in all fields of human endeavor
> - scientific discoveries
> - industrial designs
> - trademarks, service marks and commercial names and designations
> - protection against unfair competition
> - and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields."[1]

In the United States, the majority of relevant law comes from two sources: Title 17 of the US Code (and associated regulations), which deals primarily with copyright; and the Digital Millennium Copyright Act (DMCA), which made significant changes to the US Code and created additional protections for digital rights management technologies. In short, US copyright law protects the expression of original works of authorship fixed in any tangible medium.[2] One important distinction must be highlighted:

> "Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied.[3]

This typically means that software is a copyrightable work.

Typically, copyrighted material is distributed for a variety of commercial purposes: films, television programs, literature, and other ventures not concerning governmental records or record-keepers.

[1] Convention Establishing the World Intellectual Property Association, 1967 and amended in 1979. Found at: http://www.kipo.go.kr/upload/en/download/03.pdf
[2] 17 U.S.C. § 102 (2018)
[3] 17 U.S.C. § 101 (2018)

However, there are a multitude of ways copyrighted material can be a part of public records.[4] Often they are acquired through the submission of documents or data as a part of judicial proceedings and contracting and procurement activities. Records administrators and archivists are often unaware of the copyright status of the records in their custody, as protected and non-protected materials become intermixed in the course of business.

Most states, in addition to the federal government, protect trade secrets[5] found in public records. Protections for information and data containing trade secrets are necessary for the proper functioning of government. Public officials need accurate and timely information from regulated entities and thus must protect this information when in the government's custody so as to not cause damage to those entities.

Many laws define records as information existing in a fixed medium, such as a paper document or electronic file. These laws often distinguish between the record itself and the information contained in the record. That distinction is essential to the nuanced implementation of digital rights management. Records in the custody of a public body may contain both *public information* and *non-public information*. For example, medical records held by governmental public health agencies may have information in the public domain (e.g. aggregations of public health statistics) but may also have information protected by the Health Insurance Portability and Accountability Act (HIPAA) and other privacy laws (e.g. personal health information). Additionally, government entities may acquire copyrighted material regularly but must endeavor not to redistribute it in violation of copyright protections.

The existing legal framework makes it challenging to provide for the public to both access and copy public records when those records contain protected information. Private organizations are well within their rights to apply technological protections for their information (such as their software and content). Copyright, patent, and trade secret laws explicitly protect *information* or *data*, whereas administrators and archivists of public records are primarily concerned with the protection of the record. However, DRM technologies often apply technological controls on the record rather than on the information, and they have the potential to pose a significant barrier to the long-term preservation and access to government records.

Digital Rights Management Technology

Digital rights management (DRM) refers to technological or legal controls designed to restrict the use of hardware, software, and content. These controls are meant to protect the intellectual property rights of the creator or legal owner of the technology. While these controls have become most associated with protections for copyrighted creative works, they are embedded in many hardware and software tools, especially those delivering information or data through the web. Many of these technologies are included in licensing agreements or other contractual arrangements, and these agreements challenge traditional

[4] Clarification note: copyrighted material included in written or recorded information (e.g. documents, files, etc.) that are public records does not mean the copyrighted information is part of the public domain. Recordkeeping activities are primarily concerned with the preservation, and provision of access to the records themselves, and those records include public information as well as many kinds of information whose rights may be held outside the public domain.

[5] 18 U.S.C. § 1839 (2018)

views of ownership or custodianship of data. Understanding how technological protection measures (TPMs) function can help government archivists and records managers avoid unintended loss of access to the information and records needed to perform essential functions and protect public information.

DRM is not a new technology. These types of controls have been used for decades and are prevalent in printed and electronic materials. For example, a common early protection technique was to print using colored paper with low contrast to make photocopying difficult. Additionally, much of the physical currency printed by governments includes a pattern of symbols, called a EURion constellation, to help imaging software identify and prevent the reproduction of banknotes. Most TPMs are rooted in the protection of appropriate legal rights, like ensuring the protection of copyright and counterfeit currency.

Other types of TPMs include using authentication of products, software encryption, activation codes, and other measures that allow an authorized user to gain access to information. Many software distribution and use models (for example, anything requiring a "subscription") rely on TPMs to ensure only those who purchased the software or license have the ability to use it. For example, most government employees are familiar with software installed on desktop or networked workstations which require a login and authentication. These software are using authentication information to ensure the person authenticated is properly licensed to use the software. If not, the system will not function. This protects the information stored or manipulated by the software or system against unauthorized access.

Another example of TPM is the "activation key," which relies on encryption. While it is becoming outdated, for decades software distributors have used this technology to restrict access to their offerings. Either the entire software package comes encrypted, and without the activation key is useless, or the software can be installed but will not function without first contacting an authentication server to ensure only a certain number of licenses are issued (and none is used more than once). These types of technologies can be used in physical media and written as code in downloadable material.

As more content and software distributors change their business models from outright sale to subscription-based models, the challenge of managing records in DRM-enabled environments becomes greater. Many subscription-based services use some degree of proprietary rights-management technology, and governments rely on these software and services. Without proper understanding of the nature of this technology and the corresponding use agreements, public records and information are at risk.

Digital Rights Management, Records Management, and Digital Preservation

DRM is often designed to work behind the scenes and not be apparent to end-users, including information technology professionals, records administrators, and archivists. This creates situations in which users may not realize the software or hardware they are using has additional barriers to long-term management and preservation of their work. Some of the major challenges government archivists and records managers face with DRM include:

- Authentication controls breaking down and preventing an authorized user from gaining access to content, such as caused by connection issues or the company no longer maintaining those controls; for example, when a company closes.
- Ownership of data residing with the service provider, rather than the government agency, due to the terms of service.
- Licensing rather than outright ownership of tools used in government agencies, including "software-as-a-service" and other cloud-based solutions.
- Data reuse limitations from technological controls on accessing, copying, or sharing of information.
- Government reliance on commercial software with embedded DRM rather than in-house developed solutions.

Much of the difficulty with managing records in DRM-enabled technology comes in the intersection between the protection of legal rights and the technology used to do so. As discussed previously, many software environments in which government employees work involve DRM technology.

This creates challenges when the government contracts with a software solution. Most contractual relationships have fixed terms or need to be continually renewed until no longer needed. Conversely, DRM and associated TPMs are rarely time limited. The technological controls last longer than the contractual relationship, and in some cases last longer than the legal right in question.

Additionally, since software is considered a "work of authorship," many facets of the digital environments can include copyrighted or other proprietary material: operating systems, software, file systems, file formats, algorithms (including encryption and decryption algorithms), and more. When publicly-owned data is stored within proprietary systems or is gated in some other way by proprietary technology, this presents a significant obstacle to long-term preservation and access.

Many states already incorporate provisions regarding the ownership of data and the control thereof into standard licensing and contractual agreements. While the government is not able to give ownership and restriction of public information to private interests, seldom does the export of data from proprietary systems and formats go as smoothly as the import. Software vendors are heavily incentivized to get data into their systems, but far less so to assist with its extraction. Furthermore, vendors often cease operations unexpectedly, leaving numerous instances of government data trapped within obsolete, unsupported systems.

This is further complicated by the DMCA, which prohibits the circumvention of DRM controls, save for specific circumstances. While archives and libraries have some protections under Section 108 of the Copyright Act of 1976, these exceptions are tied to analog records, do not address DRM circumvention, and are "stuck in time."[6] Further, museums and other cultural heritage organizations possessing government records are not included in the Section 108 exceptions and must have permissions from the copyright holder or rely on fair use to make copies for preservation.

[6] Copyright.gov. *Revising Section 108: Copyright Exceptions for Libraries and Archives*. Found at: https://www.copyright.gov/policy/section108/

Protections in copyright law exist for libraries and archives to make reproductions for distribution and preservation, but these protections leave significant gaps for recordkeepers.[7] First, not all public records administrators and those engaged in digital preservation activities are employed in libraries and archives. Indeed, more and more public agencies need to consider their long-term digital preservation strategies at the point of records creation, and many content- and records-management systems are administered by agencies potentially not covered by the aforementioned protections. Furthermore, it is not clear that exemptions to reproduction apply to the circumvention of DRM. While the Librarian of Congress is authorized to grant temporary (renewable on a three-year basis) exemptions to restrictions on circumvention of copyright protection measures, there is no permanent or temporary exemption for long-term digital preservation or public information purposes.

DRM-specific issues such as these compound access challenges archivists and records managers already face from software and hardware obsolescence cycles and changing file formats. Typical digital preservation workflows include repeated copying and backing up of electronic records, as well as the migration of data from format to format in order to ensure data remains readable. Embedded DRM presents a significant obstacle to these activities, even if legal prohibitions for circumvention are not considered. It can be exceptionally difficult, if not impossible, to remove proprietary encryption from files without understanding the algorithm used to encrypt. Reverse-engineering and other DRM-circumvention techniques require specific technical expertise or are too costly for government agencies with limited budgets.

Because electronic information relies on many layers of abstraction to be human-readable (hardware, operating system, file system, file format, software, display, etc.), there are many avenues by which DRM can disrupt completely legal and authorized access. Indeed, a frequent complaint against DRM is that it broadly restricts legal access methods, and rights holders do not know (or are unable) to prevent this unintended restriction.

DRM and technological protection measures present a multi-faceted challenge to digital preservation specialists and any activity that seeks to prolong access to electronic information. The intent of TPMs is to restrict access to authorized users, which in a public recordkeeping context is a population that evolves over time, creating direct obstacles to the preservation and dissemination of records, and potentially the ability to fulfill statutory mandates.

<u>Conclusions and Recommendations</u>

First, we consider the conclusions and recommendations made by the Register of Copyrights in 2017 concerning section 1201:

> The basic framework of section 1201—including its treatment of circumvention as a standalone violation independent of copyright infringement and robust anti-trafficking provisions—remains sound, and the Copyright Office does not recommend broad changes to the statute's overall

[7] 17 U.S.C. § 108 (2018)

scope. Within this existing framework, however, it may be appropriate to recalibrate provisions in section 1201 to better reflect changes in technology since the DMCA's enactment nearly two decades ago. Specifically, the Office recommends amending section 1201 to permit third-party assistance for exemption beneficiaries, expand the scope of the security testing and encryption research exemptions, and establish new permanent exemptions to allow uses of assistive technology for e-books, certain repair, diagnosis, and maintenance activities, and cellphone unlocking.

These recommendations do not include any permanent exemption for activities related to the preservation of electronic records, and scant few of the comments submitted during the 2015 and 2018 rulemaking periods referred to electronic recordkeeping, or recordkeeping activities generally, as critical issues. It is unclear if these topics comprise any substantial party of the conversation around DRM technology.

Utilizing information security research and using third parties for removing unneeded DRM are existing recommendations that would greatly benefit governmental recordkeepers. Government networks and systems are frequent targets of malicious actors, and insulating government information and records against unauthorized access, change, or destruction is of the utmost importance. Similarly, it is unlikely governmental agencies (especially at the state and local level) will be able to develop the in-house expertise to circumvent DRM and unlock their data if the need arises. Allowing third-party assistance will be critically important for smaller governmental agencies.

The DRM working group has prepared two sets of recommendations. The first for policymakers and professional agencies:

- Collaborate with other professional associations of records administrators and archivists to thoroughly review existing statutes, regulations, and case law to determine what activities records professionals can perform legally.
- Articulate and advocate for a permanent exemption as part of the Library of Congress' copyright and intellectual property rulemaking, allowing for records managers (in some cases) and archivists (in most cases) to circumvent or remove DRM to support digital preservation or legally-authorized access purposes.
- Create and advocate for a policy framework restricting the implementation of DRM technology by non-rights holders on public data, documents, devices, and records which they distribute or otherwise have in temporary custody.
- Develop education for professionals and administrators to include contract requirements about the ownership of data and the removal of DRM and other proprietary protections on public information and data stored in digital formats.
- Work with leaders in office productivity, data transfer, cloud storage, digital preservation, and other industries to develop DRM-free implementations of software and hardware for those rights-holders. Support open-source destination formats, systems, and software allowing for long term preservation of information.

The working group also provides recommendations for practitioners to take immediately:

- Clearly articulate provisions regarding data and metadata ownership and control in contracts and agreements with vendors. Include whether the agency will have the ability to extract all data and metadata without restrictions or vendor intermediation, and whether the data will be within any sort of protected or proprietary format. This applies equally to software purchased or developed by government agencies and software-as-a-service arrangements.
- Inventory all programs, services, and storage environments within an agency to determine what, if any, control/access restrictions may be in place. This will provide a clear picture of the scope of the problem, and will be the first step in mitigation.
- Once DRM-restricted information (and the restrictive software containing the information) has been identified, develop specific mitigation strategies. Prioritize longer retention or high access volume records, as well as those residing within aging systems or those who lack support.
- Migrate (when contextually or technologically appropriate) to stable, DRM-free formats. In some cases, this may involve copying rather than moving record data to create retention outside of the live system. Also consider use of electronic records management software to maintain records..

Additional References

Digital Content Protection. *HDCP Specifications.* Found at: https://www.digital-cp.com/hdcp-specifications

IFPI. *The WIPO Treaties: Technological Measures.* March 2013. Found at: http://www.ifpi.org/content/library/wipo-treaties-technical-measures.pdf

Library of Congress Circular 92, Copyright Law of the United States https://www.copyright.gov/title17/title17.pdf

Section 1201 of Title 17: A Report of the Register of Copyrights United States Library of Congress

Title 37 of the Code of Federal Regulations Patents, Trademarks, and Copyrights https://www.copyright.gov/title37/

United States Copyright Office. *Section 1201 of Title 17.* Found at: https://www.copyright.gov/policy/1201/section-1201-full-report.pdf

Wikipedia. *List of copy protection schemes.* Found at: https://en.wikipedia.org/wiki/List_of_copy_protection_schemes