Requirements for Privacy – Enhancing Electronic Copyright Management Systems

V. ZORKADIS[1], D. A. KARRAS[2]

[1]Data Protection Authority, Omirou 8, 10564 Athens, Greece,
e-mail: zorkadis@dpa.gr

[2]Hellenic Aerospace Industry, Rodou 2, Ano Ilioupoli, 16342 Athens

Abstract
Digital watermarks and signatures allow the insertion of rights management information in multimedia content or digital works, required in electronic copyright management systems. However, part of this information may be personal, enabling thus its collection and processing for other purposes as well, such as profiling and direct marketing. Recognizing the contradicting interests of the copyright holders and the multimedia content users, we aim at privacy – friendly protection of intellectual property, since it is essential and decisive for the development of global electronic commerce applications. Therefore, in this paper, we underline privacy related issues regarding copyright protection and define requirements to support designing privacy-enhancing copyright management schemes.

Key words: Electronic Copyright Management Systems, Privacy Protection, Watermarking Techniques, Digital Signatures, Privacy-Enhancing Technologies.

1 Introduction

The deployment of electronic copyright management systems leads to the creation of a technological and organizational infrastructure that enables automatic rights clearance in the information commerce world, allowing digital work creators to enforce their rights when their creations are accessed by other parties. As an example of such a system, we will discuss the IMPRIMATUR Business Model [11] (Fig 1). The components and their interactions in this model are as follows: the creator (C) of a digital work cooperates with a creation provider (CP), whose role is similar to the role of a publisher (offers editorial and marketing services), i.e., it packages the original work into a market-mature one. The media distributor (MD) has the role of a retailer, i.e.; it sells product usage rights. The monitoring service provider monitors, on behalf of creators and right holders, what is acquired from media distributors. The unique number issuer has a role analogous to the role of ISBN issuers, the certification authority or trusted third party supports the authentication between the involved entities in an electronic copyright management system. There are further entities that might play a role in the electronic transactions such as a license broker, (Internet) service provider, Internet access provider or network operators, etc.

Digital watermarking and digital signatures comprise the base of multimedia copyright protection techniques, proposed and applied so far. Extensive research has been carried out in the last two decades regarding digital signatures and since the middle of the 90's regarding watermarking techniques. Digital signature schemes reached a mature phase and are widely standardized and corresponding interoperability issues are investigated. On the contrary, such issues are still open in relation to watermarking systems.

A large variety of watermarking techniques has been proposed in the literature [1, 2, 3, 4, 5, 6, 7], which are appropriate to address several application requirements, such as copyright protection, data authentication and ownership identification. Though, there are some commonly required watermark characteristics by different applications, there are also application dependent characteristic requirements. To the former belong robustness, tampering resistance and low error probability and to the latter

unperceivability, invertibility, non-(quasi-) invertibility, watermark entropy and extraction speed. Watermarking techniques may be classified, from the point of view of detection, into blind or non-blind, private or public and readable or detectable. Blind watermarks, as opposed to non-blind watermarks, do not rely for reading or detection on the comparison of the original (non-marked) digital work (image or text or audio). Private watermarks allow only authorized users to detect them. In this case, the knowledge of some secret information is needed. In contrast, public watermarks allow anyone to read them. Especially, the public or private nature of the watermark significantly affects the way it can be applied in applications domains with contradictory functional requirements. Readable watermarks are the public ones, which allow anyone to read the marks. On the other hand, the detectable watermarks that are the private ones permit only the authorized users to check if given marks are present or not. The above classification proves to be useful to guiding the watermark selection according to the application requirements and the privacy-related goals.

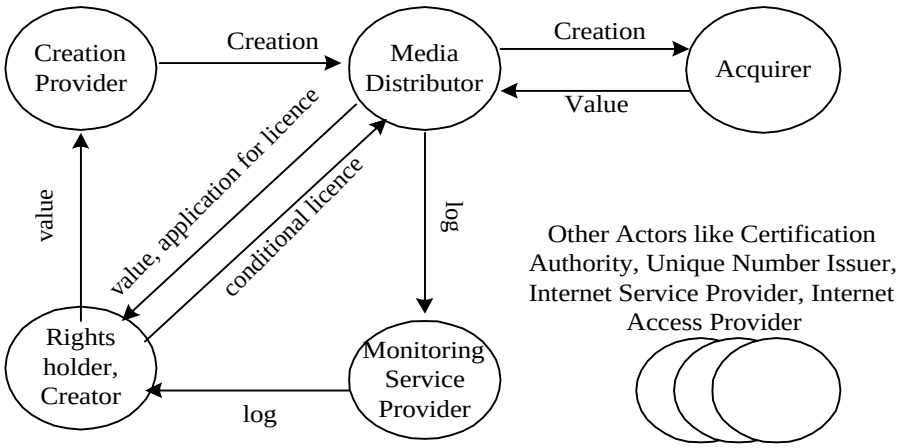

Fig. 1. IMPRIMATUR Business Model (simplified)

Digital signature schemes are primarily asymmetric cryptographic techniques [8, 9, 10], which can be used to provide entity and data origin authentication, data integrity and non-repudiation services. According to the related standards [9, 10], there are two types of digital signatures, the mechanisms with message recovery and the mechanisms with appendix. Asymmetric cryptography requires a public key infrastructure to exist, so that the associated algorithms can be proven and accepted to be used in global information commerce environment. The participants in this structure, such as the Certification Authorities, provide their services in a trustworthy (tamper-resistant) environment.

2 Copyright Protection and Privacy Issues

It is expected that copyright management information will play an important role in the future on-line trade in content and the administration of rights [12]. Copyright management information refers to the work, the author and the owner of any right in the work, to the terms and conditions of use and to related numbers and codes. There is legal protection against removal or manipulation of copyright management information. Various areas of law offer partial protection, such as copyright law, unfair competition law, trademark law and liability and criminal law.

Specific national laws based on the WIPO Treaties and the EU Directives may

provide better legal protection. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty contain provisions requiring the integrity protection of the complete copyright management information. In particular, according to article 12 of the WIPO Copyright Treaty, contracting parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by the Copyright Treaty or the Berne Convention: (i) to remove or alter any electronic rights management information without authority; (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority. Similar provisions are contained in the EU Directive on Copyright Protection and in US Digital Millenium Copyright Act.

However, the development of on-line trade in digital works lead to the processing of vast quantities of personal data. Privacy protection laws were enacted in many countries in the last three decades. They have been introduced to regulate the processing of personal data and to prevent what are considered to be privacy violations, such as unlawful storage or storage of inaccurate personal data and abuse or unauthorized disclosure of personal data. In the international legal instruments related to privacy protection are included the EU Directives 95/46/EC and 97/66/EC, the Council of Europe's Convention of the Protection of individuals with regard to Automatic Processing of Personal Data, and the OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [3,4]. Among the main principles, which comprise the basis of the legal framework related to data protection, are the following [13]:

- Personal data should be gathered by fair and lawful means,
- The amount of personal data collected should be adequate, relevant and not excessive in relation to the purposes for which they are processed,
- Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- Personal data should be accurate and up to date. Inaccurate or incomplete data should be erased or rectified,
- Personal data should be preserved in a form, which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored,
- Security measures should be taken to protect personal data from unintended or unauthorized disclosure, destruction or modification,
- Entities responsible for processing of personal data (data controllers) should be accountable for complying with the above principles.

3 Requirements for Privacy-Friendly Copyright Protection

From the discussion in Section 2, we recognize the contradicting requirements concerning copyright management systems and privacy protection, since the former rely on the use of copyright management information including data that can be regarded as personal and the latter relies on the possible absence of such data. To cope with these problems techniques should be devised, that enable balancing copyright and privacy protection. In this section, we attempt to define requirements for such techniques.

Though, it is not to exclude that entities involved in electronic transactions such as media distributors may collect and process personal data for other processing purposes than copyright protection, we focus on personal data in the context of electronic copyright management systems. The private use of digital works seems to be brought within the copyright-owners' sphere [14]. Techniques such as monitoring and blocking used in management systems enable copyright-holders and media distributors to enforce legal provisions against individual users.

Monitoring techniques enable to detect copyright infringements and violations of license terms during the private use of digital works. For instance, subscribers of pay-per-view television are charged for each actual service received. Some monitoring bases on specific hardware and/or software modules, which allow the recording and communication of usage information related to the copyrighted digital works. Thus, the copyright-holders can be provided with an audit trail regarding the private usage of their products and be able to accordingly bill the users or spot copyright violations.

Blocking techniques allow copyright-owners to prevent access to their works, or certain uses of them, except the users acquire some special means, such as access keys in the case of encrypted works. As opposed to monitoring techniques, blocking techniques don't rely on the processing of data related to the actual use that is made of a work. Though blocking constricts user autonomy, from a strictly privacy perspective, however, it seems preferable to the monitoring of private usage.

Electronic copyright management systems make use of monitoring techniques based on special hardware and software modules, watermarks and signatures and of blocking techniques based on cryptography. From the above discussion we may define the following requirements - constraints with regard to privacy – friendly copyright protection:

- Blocking (or other alternative, less privacy-invasive solutions) is to prefer compared with monitoring, since it leads to essentially less processing of personal data.
- Electronic copyright management systems should inform end users of the measures used to enforce copyright as well as of the privacy policy followed.
- Monitoring techniques if applied should fulfill the principles of lawfulness and fairness, minimality, accuracy, anonymity, security, individual participation and accountability.
- Electronic copyright management systems should facilitate the access of data subjects to their own data and of data protection authorities to personal data collected and processed.
- Electronic copyright management systems should enable end users to rectify data on them if inaccurate and misleading.
- Especially, regarding security, an appropriate security policy is to be followed by all entities involved in electronic copyright management systems. Regarding the organizational and technical measures taken by them, it should be possible to be evaluated by the data protection authorities or other trusted parties.
- Staff selection involved based on their skill and ethics and participation in appropriate training in security and privacy issues.

4 Conclusion

In this paper, we discussed the tradeoff between copyright and privacy protection and recognized corresponding requirements for privacy – friendly electronic copyright management systems. Technological measures like monitoring techniques base on the collection and processing of data related to use of the copyrighted works at the user side. Regarding such techniques, if they have to be applied, they should fulfil all the principles contained in the legal framework related to personal data protection, such as lawfulness, minimality, accuracy, anonymity, security and accountability. However, blocking or other alternative, less privacy-invasive solutions should be applied instead of monitoring.

References:

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A Secure, Robust, Watermark for Multimedia", Workshop in Information Hiding, vol. 1174 LNCS, Springer Verlag, pp. 185-206, 1996.

[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[3] I. Pitas, "A Method for Signature Casting on Digital Images", Proc. of Int.

Conf. on Image Processing, vol. III, pp. 215-218, 1996.
[4] F. A. P. Petitcolas and Ross J. Anderson, “Evaluation of copyright marking systmes”, Proc. of IEEE Multimedia Systems’ 99, vol. 1, pp. 574-579, 1999.
[5] F. A. P. Petitcolas, Ross J. Anderson and M. Kuhn, “Attacks on copyright marking systems”, Workshop in Information Hiding, vol. 1525 LNCS, Springer Verlag, pp. 218-238, 1998.
[6] IMPRIMATUR (IMP/I4062/A), “Watermarking Technology for Copyright Protection: General Requirements and Interoperability”, pp. 1-14, www.imprimatur.net.
[7] F. Mintzer, G. W. Braudaway and M. M. Young, “Effective and ineffective digital watermarks”, Proc. of Int. Conf. on Image Processing, vol. III, pp. 9-12, 1996.
[8] ISO/IEC 9796, Information technology – Security techniques – Digital signature schemes giving message recovery, (1991), and 1997.
[9] ISO/IEC 14888, Information technology – Security techniques – Digital signature schemes with appendix, 1998.
[10] W. J. Caeli, E. P. Dawson, S. A. Rea, “PKI, Elliptic Curve Cryptography, and Digital Signatures”, J. Computers & Security, 18 (1999), pp. 47-66.
[11] IMPRIMATUR (IMP/3-0021), “Business Modeling”, pp. 1-18, www.imprimatur.net.
[12] IMPRIMATUR (IMP/3-0021), “Protection of Copyright Management Information”, 1998, pp. 1-42, www.imprimatur.net.
[13] V. Zorkadis, E. Siougle, ‘Information Security and Privacy Audit Modeling’, Proc. .., 2001.
[14] Institute for Information Law, Amsterdam, “Privacy, Data Protection and Copyright: Their Interaction in the Context of Copyright Management Systems”, 1998, pp. 1-80, www.imprimatur.net.