

International Hellenic University

Digital Rights Management technologies versus end-user privacy

Ioannidis Nikolaos - 1104170010

**Master Thesis: LLM in Transnational and European Commercial Law,
Banking Law, Arbitration/Mediation**

Academic year: 2017-2018

Thesis Supervisor: Assistant Professor Komninos Komnios

Abstract

In examining the liaison between intellectual consumption and end-user autonomy through a digital lens, it proves rather disputable how privacy boundaries are determined. Over the course of the last four decades, the map of unregulated fields in cyberspace is shrinking, yet the intellectual property acquis has engaged in an enduring conflict with the privacy acquis. Rights and obligations had to be relocated into a networked arena, giving birth to Digital Rights Management technologies. Primary object of the latter has been the proper allocation of digital-content rights to their respective owners, additionally, such systems represent an effort to control unauthorized proliferation of copyrighted material.

Not only broadband speeds, but also societal values have been subjected to technology advancements. By managing digital rights, these protective systems' objective has altered, since their data accumulation scope exceeds the most advanced copyright interests. Both data subjects are eventually exposed, and information gathered concerning them is vulnerable to ungoverned dissemination. Instead of being reassured for the exclusive purpose collected, it has been evidenced that personal data are spread into secondary markets. Via an evaluative analysis, it is assuredly demonstrated that data collection principles have been regularly disrespected.

Lucid explanations and specifications have only recently been provided, through a weighty legislative instrument, directly effective across the European Union, affecting copyright-safeguarding technologies among others. A variety of concepts have been introduced, most prominently the one of privacy by default and by design, a promising provision for future developments. Implementation of digital rights management systems should then reserve to be reversed and serve legitimate purposes, in contrast to today's defiance.

Table of Contents

List of Abbreviations 5

Chapter I

1. Introduction6

Chapter II

2. Re-conceptualization in the fullness of time8

2.1 Digitization of an erst analogue world 8

2.2 Restrictions in effective protection of rights 9

Chapter III

3. Digital Rights Management systems.....12

3.1 The subject: DRM technology, definition and scope..... 12

3.2 The object: Channeling the intellectual creations..... 14

3.3 DRM and peer to peer file sharing networks 18

3.4 Shielding intellectual products, the legal regime 23

Chapter IV

4. Privacy and Digital Rights Management29

4.1 General remarks – the right to privacy..... 29

4.2 Digital Rights Management systems categorized by pervasiveness 31

4.3 The new era DRMs: incessant “omniveillance” in a data-driven economy 35

4.4 Types of privacy; informational privacy 37

4.5 European Union privacy legislation..... 40

4.5.1 General Data Protection Regulation, an overview and new entries..... 41

4.5.2 Personal data: criteria for lawfulness of processing 45

4.5.3 Underlying principles of data processing 48

4.6 Critical evaluation of surveillance DRM systems..... 52

Chapter V

5. Alternative suggestions.....59

5.1 Nascent insights in practice 59

5.2 Privacy by design 63

Chapter VI

6. Conclusion.....66

Bibliography

Case Law	68
Literature	68
Legislation and Official Documents	74
Websites and Online sources	76

List of Abbreviations

A2K	Access to Knowledge
Art. 29 WP	Article 29 Working Party
DMCA	Digital Millennium Copyright Act
DRM	Digital Rights Management
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
EU	European Union
GDPR	General Data Protection Regulation
INFOSOC	Information Society Directive
IP	Internet Protocol Address
IPRs	Intellectual Property Rights
OECD	Organization for Economic Co-operation and Development
P2P	Peer to peer networks
PbD	Privacy by Design
PET	Privacy Enhancing Technologies
PRM	Privacy Rights Management
RMI	Rights Management Information
TPM	Technological Protection Measure(s)
TRIPs	Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WPPT	WIPO Performances and Phonograms Treaty
WTO	World Trade Organization

Chapter I

1. Introduction

Reckoning the evolution of digital communications, over the course of the last half century, one would constantly feel a state of exceptionalism, since every single stance of this span, one major technological invention followed the other. Referring to the overarching one, the Internet, it has facilitated variously individuals' life, as much as it complicated them. In terms of intellectual property as an activity and fundamental social institution¹, authors uneasily saw their works being exponentially disseminated through unregulated digital networks. A response to this undesirable phenomenon was proposed through mechanisms, as antibodies to intellectual products appropriation, namely Digital Rights Management systems (hereinafter: DRM).

An established system to almost every device today, its purpose corresponding to its name indeed, DRM systems' installation and rationale of existence, ranges from controlling digital licenses to indiscriminately absorbing information. The latter issue, being the principal subject of this thesis, has highly concerned legislators, technologists, activists, engineers and certainly end users. The re-purposing of information collected by DRM, whose entrance into society was initially mandated for intellectual property protection, poses threats and shakes the ground in the already agitated privacy field. Information power maximization² is achieved by an alternative usage of DRM, that of collecting personal data for marketing purposes, such as differential pricing, as it will be examined further. A competition tool, a strategic resource, a new form of social control, treating consumers like crooks instead of customers³.

The legitimacy of such actions shall be assessed taking into consideration current legal instruments, the categorization of DRM systems, and the technological context. The thesis introduction is followed by five chapters. In the second, a socio-legal approach

¹ Oleksandr Stovpets, Social-Philosophic View of the Intellectual Property Institution: Contemporary Features, Main Problems & Development Prospects, 9 Cogito: Multidisciplinary Res. J. 49 (2017) 49

² Nye, Jr. J.S., Owens, W.A., America's Information Edge // Foreign Affairs. Vol. 75. - No. 2, March-April (1996) 20-36

³ Doctorow, C.: Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future. San Francisco: Tachyon Publications (2008) 4

to the notion of intellectual property in the digital era is deemed necessary, while on the third chapter, DRM technology's function will be examined. Parallely, the evolution of integrated protection and management framework, deployed for diminution of inappropriate usage⁴, will demonstrate their multifaceted role. Subsequently, in the fourth chapter, after delimiting digital (informational) privacy as a concept, DRM mechanisms will be scrutinized through their interrelation with privacy, in theoretical and practical level, whereas it seems indispensable to recognize the threats and the methods of intrusion. Adequate legal protection will be discussed, if offered, by current legal instruments, in the territory of Europe. Next, the fifth chapter introduces recommendations in DRM architecture and functionality, focusing on privacy enhancement patterns. The thesis is concluded in the sixth chapter, with the main points being summarized.

⁴ Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 33

Chapter II

2. Re-conceptualization in the fullness of time

By what the American philosopher Thomas Kuhn names as “paradigm shift”, it is implied a fundamental change in the basic concepts and experimental practices of a scientific discipline⁵. An emanant revolution particularly in the advancement of information and communication technologies, has fertilized the ground for flourishing, unprecedented expansion in human knowledge. The networked information society⁶, still evolving and augmenting the technological intergenerational gap, had never been experienced by humanity.

A gateway to variant activities in cyberworld has bifurcated the underlying conflicting currents⁷, on the one side control of intellectual products, on the other side booming demand for access to them. Since the Statute of Anne in 1710⁸, copyright, merely has altered⁹, the last decades nevertheless, Internet has crucially inflicted damage to its core, copyright is under siege¹⁰. The world is passing from “elite creativity for a mass market” to “mass creativity for elite markets”¹¹.

2.1 Digitization of a former analogue world

An exposition and explication of the origins of existing digitality would be important, for an analysis of the pro-copyright and anti-privacy DRM technology. Intellectual property as a notion was not always synonymous with reproduction of an intelligible

⁵ Thomas Kuhn, *The Structure of Scientific Revolutions* (1970 ed.)

⁶ Antonios Broumas, *Code, Access to Knowledge and the Law: The Governance of Knowledge in the Digital Age*, 5 U. Ottawa L. & Tech. J. 221 (2008) 223

⁷ Id. at 225

⁸ Also known as the Copyright Act 1710, this was the first full-fledged copyright statute in the Kingdom of Great Britain and in the world.

⁹ Nick Rose and Michael Sweeney, 'The Hargreaves Report' (2011) 22(7) Ent LR 201, 201.

¹⁰ Alan Royle, *Pirates Ahoy: Copyright and Internet File-Sharing*, 1 N.E. L. Rev. 51 (2013) 51

¹¹ Alfredo M. Ronchi, Politecnico di Milano in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, *Digital Rights Management for e-Commerce systems* (Information Science Reference 2009, Hershey New York) 21

good residing inside a fixed means. A century ago, in Acoustic Era¹² dissemination of intellectual products was unfeasible, unless one appropriated the physical copy, by buying, borrowing or stealing it. Phonographs reached the limits of their usefulness and adaptability¹³. In contrast, the fashion of content distribution dramatically transitioned to the origins of what we perceive today as dissemination, via the Magnetic Era's means (e.g. tape, disks) which bloomed from mid-1900s to 1980s¹⁴, ending with the famous Sony Walkman¹⁵, the portable cassette player in 1979. It was not until the Digital Era that the specter of piracy began to loom above the media industry's head¹⁶, when the copied material wouldn't deteriorate, resulting in a non-destructive reproduction. The entire content, now piracy-receptive, alienated from the traditional copyright basis, the laborious authorship and the industriousness¹⁷, and was reduced to a single click.

2.2 Restrictions in effective protection of rights

While the introductory, rudimentary, conceptualization of intellectual property is traced back to around 557 A.D.¹⁸, the modern definition demarcates the deriving rights as a *“category of intangible rights protecting commercially valuable products of the human intellect,”* or a *“commercially valuable product of the human intellect, in a concrete or abstract form”*¹⁹. From an author's perspective, what substantially affects her exercise of rights, is the efficient licensing to subsequent acquirers, the licensees. What is

¹² Nicholas C. Butland; Justin J. Sullivan, Pirate Tales from the Deep [Web]: An Exploration of Online Copyright Infringement in the Digital Age, 13 U. Mass. L. Rev. 50 (2018) 55

¹³ Andre Millard, America on record 37-64 (1995) 136-157

¹⁴ Nicholas C. Butland; Justin J. Sullivan, Pirate Tales from the Deep [Web]: An Exploration of Online Copyright Infringement in the Digital Age, 13 U. Mass. L. Rev. 50 (2018) 55

¹⁵ History.com Staff, “The first Sony Walkman goes on sale” (2009) available at <https://www.history.com/this-day-in-history/the-first-sony-walkman-goes-on-sale> accessed 12 June 2018

¹⁶ Nicholas C. Butland; Justin J. Sullivan, Pirate Tales from the Deep [Web]: An Exploration of Online Copyright Infringement in the Digital Age, 13 U. Mass. L. Rev. 50 (2018) 57

¹⁷ George Ticknor Curtis, Treatise on the Law of Copyright 169 n.1 (Boston 1847) 171

¹⁸ Colmcille, the protagonist, did not infringe anyone's copyright in copying Finnian's book. The legal construct of copyright didn't exist yet. The first copyright act was arguably the UK's Statute of Anne in 1710 but copyright had existed as a monopoly and state (or crown) censorship device in that country and others for more than 150 years before that.

For more see: Ray Corrigan, Colmcille and the Battle of the Book: Technology, Law and Access in 6th Century Ireland, OPEN U. 1-2 (2007) available at http://oro.open.ac.uk/10332/1/GIKII_Colmcille_final.pdf, accessed 12 June 2018

¹⁹ Intellectual Property, Black's Law Dictionary (10th ed. 2014) available at http://www.chori.org/About_CHORI/Downloadables/FAQs.pdf accessed 12 June 2018

valuable and lucrative, following the fixation of the idea, is the application of the quid-pro-quo^{20,21} principle. An author today, communicating the work to the public either by digital means or not, is helpless as to who may illegally take advantage of her intellectual products.

As a state of the art, users have abandoned traditional distribution channels²², at a marginal cost. Non-professional users would make sure that the Internet community's interconnectedness would assure at least one purchased digitized copy for free download²³ *"Once an unprotected copy is generated it can then be shared freely on Internet file-sharing networks that run on generative PCs at the behest of their content-hungry users"*²⁴. Massive distribution, handiness in search, peer to peer networks, easiness of photographing, scanning, registering, high quality reproduction, along with the TCP/IP²⁵, rendering the Internet an agnostic tool in terms of transferring, altogether have secluded the original author.

A free culture²⁶, often contrasted with the permission culture, describes a social movement where freedom in distribution in the form of free content promotes

²⁰ Meaning "something for something" in Latin.

Merriam-Webster, the American Heritage Dictionary of the English Language (Fourth Edition)

²¹ Pesses, Elizabeth "Patent and Contribution: Bringing The Quid Pro Quo Into Ebay V. Mercexchange," Yale Journal of Law and Technology: Vol. 11: Iss. 1, Article 10 (2009)

Available at <http://digitalcommons.law.yale.edu/yjolt/vol11/iss1/10>, accessed 12 June 2018

²² Vagelis Papakonstantinou: Legal Issues for DRM: The Future in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 314

²³ See also Petrick Paul, Why DRM Should be Cause for Concern: An Economic and Legal Analysis of the Effect of Digital Technology on the Music Industry (November 2004), Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-09. Available at SSRN: <http://ssrn.com/abstract=618065>, accessed 12 June 2018

²⁴ Stuart Haber et al., If Piracy Is the Problem, Is DRM the Answer? in DIGITAL RIGHTS MANAGEMENT, (Eberhard Becker et al. eds., 2003) 224, and Jonathan Zittrain, The Generative Internet (119 Harvard Law Review 1974 Berkman Center Research Publication No 2006/1 University of Oxford Faculty of Law Legal Studies Research Paper Series Working Paper No 28/2006 June 2006) 2000

²⁵ Solum, Lawrence B. and Chung, Minn, The Layers Principle: Internet Architecture and the Law. U San Diego Public Law Research Paper No. 55 (2003) 5

Available at SSRN: <https://ssrn.com/abstract=416263>, accessed 12 June 2018

²⁶ See also: Lawrence Lessig, Free culture (2004)

creativity. Alternatively, it is argued²⁷ that Access to Knowledge²⁸ (A2K) “*envision[s] knowledge as central to human growth*” and “*aims at enhancing the production of information, knowledge and culture in the network by encouraging new models of non-market and decentralized, peer and collaborative research and information production*”. Rights over creations have to be productively enforced, in a protective manner, paving the way for mechanisms in the digital arena, those of DRM, as a response on behalf of legislators. “*The answer to the machine is in the machine*”²⁹.

²⁷ Most prominent are the Free Libre Open Source Software (FLOSS) movement in software, the Open Access Publishing initiative in science, the Bloggers movement in the media sphere, the Wikipedia project in the field of collective Knowledge, and the Creative Commons project in the field of law, to name but a few.

Antonios Broumas, Code, Access to Knowledge and the Law: The Governance of Knowledge in the Digital Age, 5 U. Ottawa L. & Tech. J. 221 (2008) 234

²⁸ Access to Knowledge (A2K), a movement with a loose collection of civil society groups, governments, and individuals converging on the idea that access to knowledge should be linked to fundamental principles of justice, freedom, and economic development.

See also: https://en.wikipedia.org/wiki/Access_to_Knowledge_movement, accessed 13 June 2018

²⁹ Charles Clark, "The Answer to the Machine in the Machine" in P. Bernt Hugenholtz, ed., The future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium organized by the Royal Netherlands Academy of Sciences INAW) and the institute for Information Law 139-145 (Amsterdam 6-7 July 1995) (Kluwer Law International, 1996) 139

Chapter III

3. Digital Rights Management systems

In this chapter, an overview of Digital Rights Management systems will be provided, commencing from a descriptive definition, enumerating their characteristics and delimiting their purpose. Furthermore, an introductory interrelation between DRM and peer to peer should clarify the reason why these technologies were implemented. Finally, their legal foundation will be analyzed, focusing on the EU legislation.

3.1 The subject: DRM technology, definition and scope

An overarching, fully inclusive definition of DRM has not been articulated³⁰. A generic umbrella term would “*cover the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets*”³¹. Or “*a system, comprising technological tools and a usage policy, that is designed to securely manage access to and use of digital information*”^{32,33,34} Even though the average user detects the “digital lock”³⁵ idea behind DRM, as a set of access-control technologies for restricting the use of proprietary hardware and copyrighted works, the latter comprises a series of functions, which could be summarized in two major subgroups, albeit interrelated³⁶. Both their roles are related to intellectual property rights.

³⁰ See also: Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003) 4

³¹ Renato Iannella, Digital Rights Management (DRM) Architectures (2001), D-Lib Magazine June 2001 Volume 7 Number 6 available at <http://www.dlib.org/dlib/june01/iannella/06iannella.html>, accessed 14 June 2018

³² Ian R Kerr, Alana Maurushat and Christian S Tacit, “Technological Protection Measures: Part I—Trends in Technical Protection Measures and Circumvention Technologies” (2003) at s. 5.2.2

³³ INDICARE, Natali Helberger (ed.), State-of-the-Art Report: Digital Rights Management and Consumer Acceptability. A Multidisciplinary Discussion of Consumer Concerns and Expectations (INDICARE, 2004), 126-134

³⁴ Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 4

³⁵ Rebecca Wexler, The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates, 17 Yale J.L. & Tech. 368 (2015) 369

³⁶ A similar identification is represented through the following concepts: first, the *Management of Digital Rights* (MDR), relating to Intellectual Property Rights (IPRs), issuing digital permissions,

Firstly, they serve as Rights Management Systems (or Rights Management Information, “RMI”), which provide identification of rights related to that work, either directly or indirectly³⁷. A consolidation of property in the work, a binding connection between the author and the intellectual product, in digital context. Expressed by the means of a sui generis language, the “Right Expression Language”, by which code is translated in the natural language of access rights to assets³⁸.

Secondly, A DRM may be employed as a Technological protection measure (“TPM”), which is a subset of DRM. Particularly, a DRM system may incorporate TPM, the purpose of which is to prevent unauthorized usage of protected content “*by limiting access, copying or other unauthorized actions by end users conditional on compliance with licensing conditions applied by the owner of rights*”³⁹. Their character may be punishing too, (self-enforcement tools) empowering the right holder to (remotely) terminate access^{40,41}. Most frequently, TPMs are used as copy-control mechanisms, to interdict unauthorized duplication of digital content (e.g. password protection, read-only usage).

Limitation of interoperability is a prevalent typicality of DRM systems. Apple products, for instance, through the infamous DRM technology *FairPlay*, were not available to be

communicating between platforms in code, and *Digital Management of Rights* (DMR), consisting of the TPM. One managing element and one enforcing element.

Antonios Broumas, Code, Access to Knowledge and the Law: The Governance of Knowledge in the Digital Age, 5 U. Ottawa L. & Tech. J. 221 (2008) 232

³⁷ To illustrate, one could add copyright notices, publishers’ information, dates, disclaimers, permissions, ISBN, acknowledgements, and so forth, typically inserted on the verso of the title page inside the work in printed volumes.

Perry Mark, Rights Management Information in the Public Interest: The Future of Canadian Copyright Law, Michael Geist, (2005). Available at SSRN: <https://ssrn.com/abstract=1622462>, accessed 14 June 2018

³⁸ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003), 101

³⁹ Strykowski, P. and D. Scorpecci Piracy of Digital Content, OECD Publishing, Paris(2009) 57 available at https://read.oecd-ilibrary.org/science-and-technology/piracy-of-digital-content/drivers-of-digital-piracy_9789264065437-4-en#page15 accessed 14 June 2018

⁴⁰ Rebecca Wexler, The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates, 17 Yale J.L. & Tech. 368 (2015) 374

⁴¹ Brad Stone, Amazon Erases Orwell Books from Kindle (17 July 2009) available at <https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html> accessed 14 June 2018

streamed by devices with a different operating system from Apple's, a case which raised controversies in terms of consumer rights⁴².

Furthermore, hardware DRM technologies refer to the part of the equipment or hardware which is used to play digital content⁴³ such as the region-exclusive DVD DRM, implementing region-coding technology. These kind of DRM systems are considered obsolete today and are progressively substituted by robust ones. Extensively, nowadays content distributors employ software restrictions⁴⁴, since digitized rich media is encapsulated in multipurpose devices.

Among the most essential evaluation criteria of DRM systems, one pinpoints user-friendliness, trust, security, extensibility, flexibility, implementability, openness and cost⁴⁵. Legally, which feature matters most, is the extent to which DRM middleware allow the intrusion of automated systems in users' privacy and undisclosed, undesirable and unlawful processing of personal data. By an exposition in the next section of how the standard DRM model operates, it will be assessed to what extend certain functions permeate privacy.

3.2 The object: Channeling the intellectual creations

Intellectual goods⁴⁶ to be distributed by content providers, are entrusted in software platforms, where DRM systems are embedded. Software⁴⁷, in general, comprises the programs and other operating information used by a computer. Whenever a consumer

⁴² Apple DRM is illegal in Norway, says Ombudsman (24 Jan 2007) <https://www.outlaw.com/en/articles/2007/january/apple-drm-is-illegal-in-norway-says-ombudsman/>, accessed 15 June 2018

⁴³ Hofman Julien.: *Introducing Copyright, A plain language guide to copyright in the 21st century*. Vancouver: Commonwealth of Learning. (2009) 112

⁴⁴ Id. at 112

⁴⁵ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: *Digital Rights Management, Technological, Economic, Legal and Political Aspects*. Berlin: Springer-Verlag Berlin Heidelberg (2003) 10-14

⁴⁶ An exceptionally great percentage of these goods concern copyright infringement, and do not relate to other intellectual property rights such as trademarks, patents or designs.

⁴⁷ Another definition for a (DRM) software is "A computer program, combined with all the information with regard to the installation, operation, repair and enhancement".

Watts S. Humphrey, 'The Software Engineering Process: Definition and Scope, Software Engineering Notes (1989) 82

buys digital content, in fact they purchase a certain license⁴⁸, which grants them a bundle of rights associated with the copy of that product. Not exhaustively, a license may translate into number of views, expiration date, copy control in transferring to other devices, compatibility with specific programs, subscription or rental.

Absent any license, merely scrambled bits are what the software recognizes⁴⁹. A DRM constructs these bits and provides a framework for digital licensing. Although there is no standardized business model, some common characteristics could outline a typical DRM⁵⁰ exemplar, in which an intellectual creation is enclosed. In that, four parties are involved, the content provider, the distributor, the clearing house and the consumer/end user⁵¹, without that meaning that the in-between agreement is quadripartite⁵².

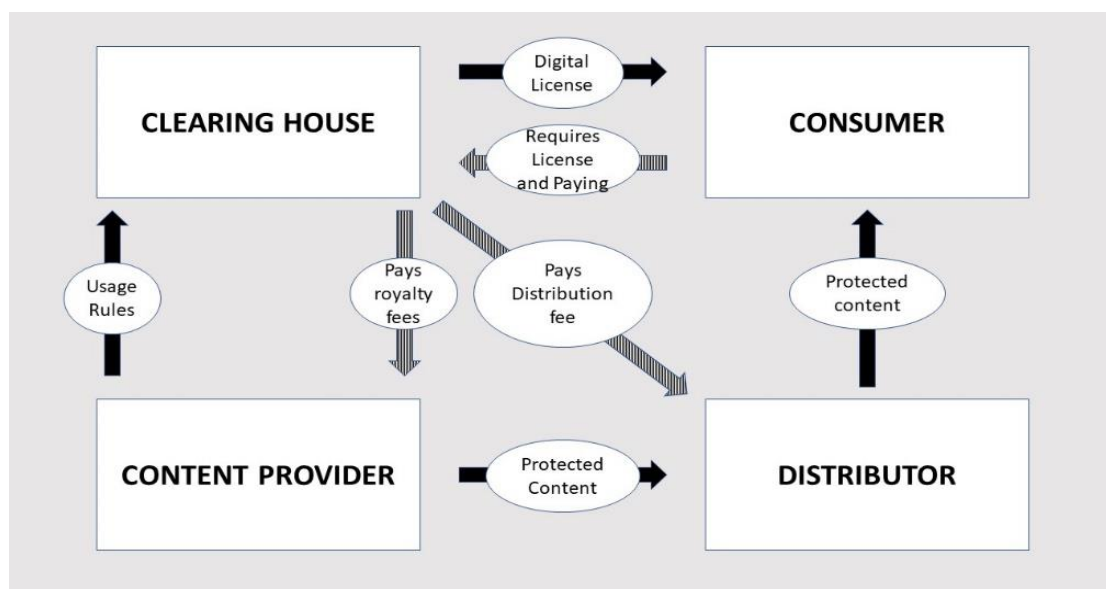


Figure 1: Typical DRM model⁵³

⁴⁸ Qioung Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, 'Digital Rights Management for Digital Distribution' 21 Research and Practice in Information Technology, (2003) 1

⁴⁹ Id. at 1

⁵⁰ As an exclusion tool, with no intrinsic value rather than the enforcement of copyright laws, DRM system could be characterized as shells, enclosing the creation.

See also: Giuseppe Mazziotti "EU Digital Copyright Law and the End-User", Springer-Verlag Berlin Heidelberg (2008) 20

⁵¹ Id. at 2

⁵² Whereas the content provider and the consumer are transmitter and receiver respectively, the content provider and the distributor are merely intermediaries to this process.

⁵³ The model is based on the illustration of Qioung Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, 'Digital Rights Management for Digital Distribution' 21 Research and Practice in Information

Initially, the information good, is created by the content provider, encoded in digital form and entrusted to the distributor to be commodified and exploited⁵⁴. Watermarking⁵⁵, steganography⁵⁶, cryptography⁵⁷ or digital fingerprinting⁵⁸ apply here, either by the content provider or by the distributor, if they undertake packaging⁵⁹ actions. In addition, the information good gets encrypted⁶⁰, and the keys for deciphering are held by the DRM. At the same time, to the clearing house are communicated the decryption keys for the digital license, as well as the usage rules⁶¹, which are normally the restrictions that the consumer confronts in their experience with the product.

A distributor's role in this scheme is to provide an aggregator platform (usually a content distribution network) where content is showcased and made available for downloading (purchasing of digital licensing). What a distribution channel does, is relieve the content providers, representing them in the financial markets, promoting and

Technology, (2003). The black arrows express the flow of intellectual content, while the stripped arrows signal the movement of money.

⁵⁴ Danielsén, D. James Boyle, Shamans, Software, and Spleens: Law and the Construction of the Information Society, Cambridge, MA, Harvard University Press, 1996, ISBN 0674805224, 288 pp., \$43.00 (hb), \$18.50 (pb). Leiden Journal of International Law, 16(2), 399-416 (2003) 403 available at <https://repository.library.northeastern.edu/files/neu:332338/fulltext.pdf>, accessed 16 June 2018

⁵⁵ Watermark as a technique, is an invisible signature embedded inside an image to show authenticity or proof of ownership, in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 57

⁵⁶ Steganography lies in devising astute and undetectable methods of concealing the message themselves.

Id. at 58

⁵⁷ Cryptography is about protecting the content of a message with the use of disguise.

Id. at 58

⁵⁸ Digital fingerprinting is the technique that embeds unique information into multimedia content and traces the usage of the corresponding multimedia content.

Id. at 180

⁵⁹ Pasi Tyrväinen, Concepts and a Design for Fair Use and Privacy in DRM (D-Lib Magazine February 2005 Volume 11 Number 2) 2

⁶⁰ To be encrypted means that "a user securely shares data over an insecure network or storage site, by transforming data into a scrambled form, a hash, which can only be translated by the one, owning the decrypting key."

See also: Dan Boneh and others, 'Functional Encryption: Definitions and Challenges' 6597 Lecture Notes in Computer Science (2011) 253

⁶¹ Usage rules often refer to copyrighted content's regulation as well as payment methods.

See also: Bogdan Popescu, Bruno Crispo, Adrew Tanenbaum and Frank Kamperman, 'A DRM Security Architecture for Home Networks' DRM (2004) 3

managing their works. Such defining examples are Netflix⁶² for video broadcasting, Hulu⁶³ for television and movies, Spotify⁶⁴, an equivalent for the music industry.

On the other hand, a clearing house assumes a carry-through, transactional role. As a holder of digital licenses, by delivering them to end users, along with the encryption keys, and by accepting payments, a clearing house credits the distributor and the content provider for shares on sales⁶⁵.

In contrast to the three parties, who act for economic interest in the respective industry, the end user, who financially supports the functioning of such mechanism, is the one encumbered with selling off part of their privacy, by submitting a series of personal data to platforms, to identify⁶⁶ themselves.

In this part, the consumer requests⁶⁷ a digital license from the clearing house, and depending on the properties of their existing account, a license is granted, accompanied with the rights embedded in the usage rules. Examples⁶⁸ include *demonstration license* (neither user nor hardware authentication needed), *educational/library license*

⁶² Netflix, Inc., incorporated on August 29, 1997, is a provider an Internet television network. The Company operates through three segments: Domestic streaming, International streaming and Domestic DVD, available at <https://www.reuters.com/finance/stocks/company-profile/NFLX.O> accessed 20 June 2018

⁶³ Hulu is a leading premium streaming service that offers instant access to live and on demand channels, original series and films, and a premium library of TV and movies to more than 20 million subscribers in the U.S, available at <https://www.hulu.com/press/about/> accessed 20 June 2018

⁶⁴ Spotify is a music streaming service developed by Swedish company Spotify Technology. The service that launched on 7 October 2008 is available in 65 regions and is headquartered in Stockholm, Sweden. It provides DRM-protected content from record labels and media companies, available at <https://en.wikipedia.org/wiki/Spotify> accessed 20 June 2018

⁶⁵ Pasi Tyrväinen, Concepts and a Design for Fair Use and Privacy in DRM (D-Lib Magazine February 2005 Volume 11 Number 2) 2, available at <http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html#20> accessed 20 June 2018

⁶⁶ These days, most DRM function online, as the Internet has been transformed into an accessible, inexpensive, yet hazardous tool. The interrelation between waiving privacy and request for digital licenses will be discussed further below. As a rule, the system asks for credentials, through a digital certificate to the consumer's user account who uses the e-commerce system to transact. This way, the content is decrypted and reachable by the end user.

See also: Qioung Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, 'Digital Rights Management for Digital Distribution' 21 Research and Practice in Information Technology, (2003) 2

⁶⁷ Such an action is performed in diverse ways, depending on the services or products merchandized. To illustrate, clicking a download button is one of them, permitting the user to keep a copy for offline use, alternatively the function "watch online" or listen online" for video or music files, only *streams* the content without it being available after disconnection.

⁶⁸ Professor Tyrväinen provides a descriptive list of licenses and templates employed in the designing and engineering of DRM, intended to conform with the fair use principle.

Pasi Tyrväinen, Concepts and a Design for Fair Use and Privacy in DRM (D-Lib Magazine February 2005 Volume 11 Number 2) 6, available at <http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html#20> accessed at 20 June 2018

(regularly personal or group student authentication is needed), *distribution license* (personal authentication for crediting sales requirement) or simply the *personal license/copy license* (either with personal authentication or not). In all these cases, the DRM certifies that the intellectual good is safely accessed, in order for the end user not to deviate from the determined set of allowed actions to them.

This approach is what the information industry has devised over the course of decades to protect digital content. Despite rising figures in piracy, it has been justifiably supported⁶⁹ that not all illegal copies would result in economic benefit through sales, in other words, if the content was disproportionately accessible (in contrast of today's situation) consumer behavior would be extremely unpredictable. Indeed, file-sharing had "*an effect on sales which is statistically indistinguishable from zero*"⁷⁰. In the following section, the interconnection between peer to peer and DRM systems will be discussed, associating it to the legal foundations of intellectual content.

3.3 DRM and peer to peer file sharing networks

Contrary to the imperfection of our physical world, one digital copy may perfectly and instantaneously be created and shared through peer to peer networks (hereinafter: P2P). Intolerable as it was for the entertainment industry, this extraordinary technique marked the counter-attack, the birth and implementation of DRM, whose principal aim was to confine the user to act as the ultimate consumer⁷¹. In this part it will be examined how P2P provoked the emergence of anti-copyright measures, which gradually evolved into a massive installation of embedded surveillance systems. Furthermore, three landmark cases will be noted.

⁶⁹ Alan Royle, *Pirates Ahoy: Copyright and Internet File-Sharing*, 1 N.E. L. Rev. 51 (2013) 55

⁷⁰ Felix Oberholzer and Koleman Strumpf, abstract of "The Effect of File Sharing on Record Sales, an Empirical Analysis" (UNC.edu, March 2004), available at <http://www.its.caltech.edu/~mshum/ec106/strumpf.pdf>, accessed 21 June 2018

⁷¹ Giuseppe Mazziotti "EU Digital Copyright Law and the End-User", Springer-Verlag Berlin Heidelberg (2008) 5

A decisive timing for P2P success, is owed to the rise of the Internet, considering the vast interconnectedness and the minimum cost⁷² that it offered. Although content was already digitized⁷³ through software, hardly could it be duplicated, except for when individuals physically transferred their fixed content. Otherwise, possessors were substantially isolated, as potential distribution was hindered by material factors⁷⁴. As a result, content and information industries were not particularly discomforted⁷⁵.

A P2P file sharing network is considered to be a decentralized application architecture of connected nodes, depending on each other, instead of a central server⁷⁶. Simply put, one end user has access to another end user's hard disk drive, and all are simultaneously both suppliers and consumers. That constitutes the baseline, where free Internet is structured, according to the proponents of DRM-free content⁷⁷, who envisioned a ubiquitous digital world without constraints. Although the piracy argumentation is not examined in this thesis, one major incentive for DRM installation was the anti-piracy regulation.

Even before the wide spread of P2P, in Betamax⁷⁸ case in 1984, the Supreme Court of the United States reasoned that *"if one records at home for noncommercial ends television broadcasts for the purpose of "time-shifting"⁷⁹, that was fair use"*. Particularly, Universal City Studios and Walt Disney Productions, brought an action against Sony Corporation of America, alleging that marketing Betamax devices,

⁷² Vagelis Papakonstantinou: Legal Issues for DRM: The Future in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 315

⁷³ *Digitization* of content refers to the process of changing from analog to digital form, also known as digital enablement. *Digitalization* is a term employed for the use of digital technologies to change a business model and provide new revenue and value-producing opportunities.

See Gartner IT Glossary, available at <https://www.gartner.com/it-glossary/d> accessed 21 June 2018

⁷⁴ For a content processor to surpass these boundaries, they had to physically move to a place where the infrastructure was installed, produce copies (usually homemade ones resulted in deteriorated form) and manually distribute them by advertisements or subscriptions e.g. by way of newspapers.

⁷⁵ Vagelis Papakonstantinou: Legal Issues for DRM: The Future in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 331

⁷⁶ A definition by Cambridge Dictionary <https://dictionary.cambridge.org/dictionary/english/peer-to-peer>, accessed 21 June 2018

⁷⁷ See also: Chapter "Piracy" in Lawrence Lessig, Free culture (2004) 62-66

⁷⁸ Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984), a one-page summary of the case can be retrieved at <https://copyright.gov/fair-use/summaries/sonycorp-universal-1984.pdf>, accessed 21 June 2018

⁷⁹ Time-shifting, as a broadcasting term, refers to the method of recording the live performance to a storage medium, for viewing afterwards. See also: "podcast"

promoted copyright infringement and thus they should be held contributorily liable, along with the consumers, who themselves committed copyright infringement by recording content. With a decision in favor of Sony, the components of the ruling included inability of the plaintiffs to prove substantial economic damage and additionally that the shows were broadcasted for free to spectators. The Sony technology provided for non-infringing uses, too. Such a decision was later interpreted as broadening the scope of fair use and domestic use of copyrighted material, since content could legally be individually produced.

The same argument did not prevail, however, in terms of “space-shifting”⁸⁰. In the milestone Napster⁸¹ case, P2P file sharing networks, were not that innocent⁸². A ruling, whose aftermath is to be extended worldwide, shaking from consumers to legislators. Not only vicarious⁸³ but also contributory infringement was the decision for Napster. The latter, although end users were connected via P2P, had a quasi-centralized⁸⁴ database and indexing search engine in servers, facilitating the diffusion of MP3 songs. Such organized, albeit non-commercial, exposition of end users’ hard disks, would not be justified by the defendants, claiming a sampling distributive function of content, approved from artists. Prior knowledge of constructive infringement was a given, rendering the platform contrary to the fair use principle. Nonetheless, dissenting opinions were prominent as well, in favor of the latest promising technology. “*Existing*

⁸⁰ That term involves the access of intellectual content from multiple devices, it allows media that originates in one place to be accessed from another place without changing the device on which it is stored.

Jamerich Parsons, June; Oja, Dan. New perspectives on Computer Concepts 2012: Introductory. Computers. Dengang Learning (2009) 465

⁸¹ A&M Records, Inc. v Napster Inc. (2001), a four-page summary can be retrieved at https://www.dcs.k12.oh.us/site/handlers/filedownload.ashx?moduleinstanceid=1862&dataid=1923&FileName=Napster_Case_Summary.pdf, accessed 22 June 2018

⁸² The scalability of P2P is demonstrated by the ever-increasing number of users who offer added value to the service. A massive number of 70 million users were knowingly involved in illegal file sharing, violating copyright law.

See also: Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003) 282

⁸³ Definition provided by Cornell Law School, Legal Information Institute, “Vicarious infringement is a form of secondary liability for direct infringement based on the common law principle of respondeat superior, if such acts occur within the scope of the employment or agency”, available at https://www.law.cornell.edu/wex/vicarious_infringement, accessed 22 June 2018

⁸⁴ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003) 350

business models may not be fully safeguarded, however invoking copyright rules merely stifles innovation and shall not be extended to disable modern technologies”⁸⁵.

A third legal technological breakthrough was achieved in the Grokster⁸⁶ case, in which the criteria applied in Sony Corp. of Am. v. Universal City Studios were revised. Notably, the intermediary software⁸⁷, even if it is technologically neutral, may render its user an infringer. Although the District Court and the Ninth Circuit both vindicated the defendants, the Supreme Court stated that it seems improbable to accuse every copyright infringer separately (referring to the end users), consequently, the secondary liabilities doctrine will be applied. American authorities adjudicated that P2P intermediaries are held liable.

Yet every node in the file sharing network although suspicious, was free to act unmanageably. Two of the features of P2P, are the non-rivalrous and non-exclusive character of the bit-to-bit copies⁸⁸. Intellectual products are not consumed by the end user in a way that vanishes them. After a short, profitable for the industry, campaign against unlawful copyright usage, DRM systems gradually populated digital content, securing and reassuring the content producers’ works.

Music files, video files, entire video games⁸⁹, software applications, got secured, while at the same time, digital copyright presumably regained its prestige. Consumers were persuaded at their majority to conform with anti-piracy schemes, expressing disaffection after all. Content industries, following the jurisprudence’s decisions, instead of exploiting the P2P conspicuous network technology, engaged in lawsuits and in the development of more robust systems, which repulsed consumers. As a matter of fact, even ad-wares or spywares encapsulated in online material would not intimidate

⁸⁵ Amended Brief Amicus Curiae of Copyright Law Professors in Support of Reversal, Consortium of 18 Copyright Law Professors, available at <http://www-personal.umich.edu/~jdlitman/briefs/Amicus.pdf> accessed 22 June 2018

⁸⁶ Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), a summary of the case exists in <https://www.casebriefs.com/blog/law/property/property-law-keyed-to-singer/intellectual-property/metro-goldwyn-mayer-studios-inc-mgm-v-grokster-ltd/>, accessed 22 June 2018

⁸⁷ The P2P platform could be characterized neutral, since a considerable number of files shared conform to copyright rules. Whether a service provider takes affirmative steps to prevent infringement or not, will substantially influence judges’ opinion.

⁸⁸ Eric Diehl, Securing Digital Video, Techniques for DRM and Content Protection (2012) 10

⁸⁹ John Kuehl, Video Games and Intellectual Property: Similarities, Differences, and a New Approach to Protection, 7 Cybaris Intell. Prop. L. Rev. 313 (2016) 321

the average user in accessing copyright protected content, so long as it was free of charge.

It is a fact that DRM systems have never been proven neither rigid, nor inviolable, and the truthfulness of this statement is validated in everyday life^{90,91}. Not a single DRM system (at least offline) has survived to raise considerable barriers, all of them have been compromised⁹². Their vulnerability lies in their structure, and the principles of reverse engineering. Distribution of digital content is always performed in encrypted form, access rights are provided only to authorized users, and after decryption, intellectual property rights (RMI) are erased. Traceability of content is lost⁹³. Ubiquity of Internet facilitates the passing of deciphered and unprotected code from sophisticated users, to less skilled ones⁹⁴

Subsequently, by the time Internet, as a good, grew accessible with bandwidth requirements being reduced to minimum⁹⁵, internet speeds permitted the deployment of a triumphing for the industry weapon. That of online DRM mechanisms (functioning

⁹⁰ A promising example of DRM for video games is "Denuvo", whose operation remains a trade secret. However, innovative encryption algorithms with periodical online authentication methods, that would reassure it a long life, have been "cracked" within some weeks. Yet, the mere fact that it endured more than 30 days (a critical time point when most DRMs do not withstand), made it a success. The same company that produced it, confessed the expiration date of DRMs, sooner or later all DRM systems are subject to tampering. "Don't call it DRM: what's Denuvo Anti-Tamper?", published at 19 June 2014, available at <https://www.eurogamer.net/articles/2014-12-19-denuvo-anti-tamper-drm> accessed 22 June 2018.

A recent version of Denuvo, 3 years after its first release indicates that *"best-in-class service can't even provide a full day of protection these days."* "Denuvo's DRM now being cracked within hours of release", Kyle Orland, 19 October 2017, available at Ars Technica, <https://arstechnica.com/gaming/2017/10/denuvos-drm-ins-now-being-cracked-within-hours-of-release/> accessed 22 June 2018

⁹¹ Regarding video games, which involve an immense computational power investment and years of designing by well-paid staff, a news reporting site about circumventing copyrighted material is hosted in <https://crackwatch.com/> accessed 22 June 2018

⁹² Managing Rights Management. Since 2005, Covering the Copyright and Consumer Electronics Industries, Including DRM, Digital Watermarking, Digital Fingerprinting and Related Technologies and Topics. "Disingenuous DRM Scoreboard", published on Tuesday, August 07, 2007 in The Rising Tide of Anti-DRM, available at <http://www.managingrights.com/2007/08/drm-scorecard.html>, accessed 23 June 2018

⁹³ Antonius Cahya, Prihandokoa, Bruce Litowa, Hossein Ghodosi, "DRM's rights protection capability: a review", The Proceeding of 2012 the First International Conference on Computational Science and Information Management, Volume 1 (2012) 14

⁹⁴ Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan "If Piracy Is the Problem, Is DRM the Answer?" (Springer-Verlag Berlin Heidelberg 2003) 224

⁹⁵ Jonathan Zittrain, The Generative Internet (119 Harvard Law Review 1974 Berkman Center Research Publication No 2006/1 University of Oxford Faculty of Law Legal Studies Research Paper Series Working Paper No 28/2006 June 2006) 1994

with online authentication and credentials), the ones which raise the most substantial privacy concerns.

3.4 Shielding intellectual products, the legal regime

There is no legal framework for Digital Rights Management systems, or rather, the provisions fostering their existence are diffused in various legal instruments. As previously mentioned, historically, the principal role of DRM implementation, originates from protection of copyrighted intellectual content. Nevertheless, hacked DRM systems was a discouraging result⁹⁶. Therefore, equivalent measures provided for in legislation, are those which deter and/or prohibit circumvention of defensive technology. In this subchapter, an overview of enacted measures will be provided, initiating from international treaties, and ending to the European legal framework.

Primordial conscientiousness regarding copyright⁹⁷, internationally, was firstly attested in 1886, in the Berne Convention⁹⁸ under the World Intellectual Property Organization (WIPO)⁹⁹, and set the grounds for any subsequent treaty and directive. An omnilateral agreement by the then industrial world, supported two more treaties in 1996, that of WIPO Copyright Treaty (WCT)¹⁰⁰ and that of WIPO Performances and Phonograms Treaty (WPPT)¹⁰¹.

⁹⁶ Matej Myska, "The True Story of DRM" Masaryk University Journal of Law and Technology (2009) 270

⁹⁷ The Paris Convention for the Protection of Industrial Property, three years ago, had already created the framework for patents, industrial designs and trademarks

⁹⁸ Berne Convention for the Protection of Literary and Artistic Works (as amended in Paris on September 28, 1979), available at http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693 accessed 23 June 2018

⁹⁹ Guarded under the UN, WIPO (World Intellectual Property Organization) was founded in 1967 and its mission is to provide a global forum for discussions pertaining to intellectual property issues, promoting innovation and creativity. Available at http://www.wipo.int/treaties/en/text.jsp?file_id=283854 accessed 23 June 2018

¹⁰⁰ The WIPO Copyright Treaty deals with the digital environment's rights of authors, and introduced a plethora of economic rights to authors, such as those of distribution, rental, and communication to the public, naturally falling within the scope of the three-step test. Furthermore, databases and software programs were classified as intellectual creations, whatever their form may be.

http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295157 accessed 24 June 2018

¹⁰¹ By the WIPO Performances and Phonograms Treaty, adequate safeguard is granted to performers and producers of phonograms in the digital environment, including economic and moral rights, available at http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295477 accessed 24 June 2018

In Article 11¹⁰² of the WTC, a stress was put on *Technological Measures* while Article 12¹⁰³ guarantees *Rights Management Information*, both of them engaging anti-circumvention behaviors relating to software. DRM systems belong to computer-code software, which falls within the scope of such protection, consequently anti-circumvention systems' legal protection for the first time is sealed in WTC. The latter smoothed the way for EU Copyright Directive's implementation in 2001¹⁰⁴.

Article 18 and Article 19¹⁰⁵ of the WPPT, provide for the same obligations pertaining to Technological Protection Measures and Rights Management Information. Indeed, this Treaty supplements WCT, as far as producers of phonograms and performers is concerned.

Entertainment, computer, information, mass media, and telecommunications industries also achieved integration of anti-circumvention and copyright strengthening schemes during the negotiations of TRIPs Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). Inasmuch as intellectual property appertains to economic and trade policies, the World Trade Organization¹⁰⁶ (WTO) could not but include a

¹⁰² Article 11: Obligations concerning *Technological Measures*:

"Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

¹⁰³ Article 12: Obligations concerning *Rights Management Information*:

"(1) 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 this 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.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public"

¹⁰⁴ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, also known as the Information Society Directive or the InfoSoc Directive, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN> accessed 24 June 2018

¹⁰⁵ These articles' phrasing is almost identical to the ones of WIPO Copyright Treaty.

See also: Becker, E., Buhse, W., Gunnewig, D., Rump, N.: *Digital Rights Management, Technological, Economic, Legal and Political Aspects*. Berlin: Springer-Verlag Berlin Heidelberg (2003) 411

¹⁰⁶ The World Trade Organization commenced its activities in 1995 by virtue of the Marrakesh Agreement and replaced the General Agreement on Tariffs and Trade (GATT, since 1948). A synopsis of its mission for world economic prosperity is summarized in: https://www.wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm accessed 24 June 2018

relevant provision for computer programs. Truly, in the first paragraph of Article 10¹⁰⁷, Digital Rights Management programs are protected as software computer programs, since the provision from Berne Convention in Paris is reiterated. Therefore, once more, minimum legal protection for copyright and not only¹⁰⁸, was consolidated.

EU, as a full member of WTO¹⁰⁹, on the grounds of TRIPs legislated its own enforceable copyright Directive¹¹⁰, entered into force in May 2001. By that steep legislative wave, almost two-thirds of national copyright laws had to be altered¹¹¹, while no other previous reform was that aspiring to intervene both in the digital and the analogue world¹¹². At the same time, reprioritization of objectives did not permit the incorporation of all measures drafted in the Green Paper^{113,114}.

Reflecting technological changes and implementing the international obligations, in the InfoSoc Directive lies Article 6(1), which states that:

“Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.”

Whereas immediately on the next paragraph the *mere promotion* of anti-circumvention tools shall be prevented:

“Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which: (a) are promoted, advertised or marketed for the purpose of circumvention of, or (b) have only a

¹⁰⁷ Article 10(1) states that “Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).”

¹⁰⁸ Intellectual property law was at first inserted in world trade by the TRIPS Agreement, systematizing legal obligation for members to enact or reinforce their national legal instruments in terms of trademarks, patents, copyright, geographical indications, industrial designs, appellations of origin etc.

¹⁰⁹ EU Member States are dually represented. All WTO members are available at https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm#collapseE accessed 24 June 2018

¹¹⁰ Directive 2001/29/EC supra note 104

¹¹¹ Giuseppe Mazziotti “EU Digital Copyright Law and the End-User”, Springer-Verlag Berlin Heidelberg (2008) 51

¹¹² Cohen Jehoram, ‘European Copyright Law – Even More Horizontal’, 32 IIC p. 532 (2001) 545

¹¹³ Commission of the European Communities, Green Paper. Copyright and Related Rights in the Information Society, Brussels, 19 July 1995, COM (95) 382 final 49. Available at <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1995:0382:FIN:EN:PDF> accessed 25 June 2018

¹¹⁴ Johannes Schönning, “The legitimacy of the InfoSoc Directive” Faculty of Law University of Lund, Master’s Programme in European Business Law (Creative Commons Attribution 2.5 Sweden License 2010) 18

limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.”¹¹⁵

It is evident that escalating options between rightholders and Member States will take place in the first section of paragraph 6(4)¹¹⁶, the most controversial one, regarding DRM and possible exceptions. Under the initiative of Member States, in combination with the absence of voluntary technological measures from rightholders, seven special exceptions bestow the right to the legal acquirer of a copyrighted work to individually access it, even if rightholders did not provide for that. However, the fourth subparagraph¹¹⁷ revokes *de facto* that possibility, given that most content on cyberspace is on demand¹¹⁸. A conclusion that could be drawn here, is that a pro-DRM policy restricts end users in terms of true benefit of legitimately acquired material, because of public policy issues¹¹⁹. An inflexible solution, which considers formalities and ignores

¹¹⁵ Article 3 of the Directive 2001/29/EC continues by explaining the scope of effective technological measures, meaning “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorized by the rightsholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed “effective” where the use of a protected work or other subject matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

¹¹⁶ Article 6(4) of the Directive 2001/29/EC underlines that “[n]otwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), L 167/18 EN Official Journal of the European Communities 22.6.2001 (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.”

¹¹⁷ In article 6(4)(d) it is mentioned that “the provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time *individually chosen* by them.”

¹¹⁸ Giuseppe Mazziotti “EU Digital Copyright Law and the End-User”, Springer-Verlag Berlin Heidelberg (2008) 98

¹¹⁹ Gasser, Urs and Girsberger, Michael, Transposing the Copyright Directive: Legal Protection of Technological Measures in Eu-Member States - a Genie Stuck in the Bottle? (November 2004 - Berkman Working Paper No. 2004-10) 10. Available at SSRN: <https://ssrn.com/abstract=628007> accessed 25 June 2018

utilization of content, open to Member States implementation purposes¹²⁰. Others simply call it a political compromise.¹²¹

In terms of protecting Rights Management Information¹²², the other side of the coin of DRM, article 7(1)¹²³ includes provisions against alteration and distribution of such information, if done in willful misconduct.

Apart from the Copyright Directive, DRM systems' legal usage is also unambiguously enshrined in the Software Directive¹²⁴, in which computer programs and software are protected as such, under the Berne Convention. In article 7(1) of the Directive, a Member State shall act on mandate of EU to provide for:

“appropriate remedies against a person committing any of the following acts: (a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy; (b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy; (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

¹²⁰ Id. at 10

¹²¹ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003) 409

¹²² Article 7(2) of the Directive 2001/29/EC defines the expression “Rights Management Information” as “any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightsholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.”

¹²³ In this article it is affirmed that “Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.”

¹²⁴ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 On the Legal Protection of Computer Programs, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN> accessed 25 June 2018

Lastly, Directive 98/84/EC¹²⁵ employs anti-circumvention measures concerning utilization of *illicit devices* in article 4¹²⁶.

Clearly, neither international institutions nor EU have dedicated till today a legislative instrument exclusively on DRM systems, rather both opted for their incorporation in legislation under the name Technology Protection Measures or Rights Management Information. As a priority for the Community's digital agenda reformation¹²⁷, the Directive endeavors to harmonize substantive law, in order to achieve more efficient enforcement. Yet, no genuine "European copyright"¹²⁸ exists.

As a summary, it is evidenced that intense effort was put to safeguard copyright material in cyberspace. Rights Management systems embedded in digital content highly contributed to controlling the intellectual creation located inside. But DRM systems are rights agnostic¹²⁹ - what they control is streams of bits and associated meta-data. Circumvention is not forgiven, and that is the first step of techno-regulation's¹³⁰ success, since copyright shall be protected. What seems a nuisance, however, is the pervasive character of copyright-protection measures towards end-user's privacy. During the last decade, a repurposing of DRM took place, by far extending their legal basis beyond copyright safeguarding, augmenting their surveillance potential¹³¹ by amassing a huge, torrential deluge of data from consumers. A topic which will be the pivot of the second part of this thesis.

¹²⁵ Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0084&from=EN>, accessed 25 June 2018

¹²⁶ In Article 4, "Member States shall prohibit on their territory all of the following activities: (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices; (b) the installation, maintenance or replacement for commercial purposes of an illicit device; (c) the use of commercial communications to promote illicit devices."

¹²⁷ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: Digital Rights Management, Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag Berlin Heidelberg (2003) 411

¹²⁸ Id. at 417

¹²⁹ Viktor Mayer-Schonberger, Beyond Copyright: Managing Information Rights with DRM, 84 Denv. U. L. Rev. 181 (2006) 189

¹³⁰ Techno-regulation is a neologism referring to the "intentional influencing of individuals' behavior by building norms into technological devices".

See: Mireille Hildebrandt, Jeanne Gaakeer, "Human Law and Computer Law: Comparative Perspectives" (Springer Netherlands 2013) 69

¹³¹ Lee A. Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests" (Published in European Intellectual Property Review, 2002, vol. 24, no. 2, pp. 51–57) 3

Chapter IV

4. Privacy and Digital Rights Management

While a variety of implications stem from the installation of DRM systems, such as competition, consumer and interoperability issues, the most noteworthy veiled threat exists against privacy and data protection, due to uncontrolled usage in conjunction with the absence of a legal framework. Introductorily, on the basis of an elaboration on the generic DRM model, their breakdown is attempted, and afterwards, the logic why Europe is so significantly motivated in securing personal data is demonstrated. Furthermore, how rights over information are guaranteed by personal data protection legislation is examined in a thorough study (principles, grounds, latest modifications). The chapter concludes by an evaluative assessment on DRM legitimacy, through a legal, social and moral prism.

4.1 General remarks – the right to privacy

To disambiguate the term “privacy” is to resolve an expert-level legal riddle. Permanently and eternally, at least, to fix this notion into words seems unrealistic. An interrelation between privacy and social context, as an independent variable¹³², should ceaselessly bother any legislator, court or commentator¹³³. In addition to being so elusive a concept, modern capabilities of technology have intensified its ambiguities¹³⁴.

In one of the most influential articles in law history, a proclamation for privacy by Samuel D. Warren and Louis D. Brandeis, privacy is roughly translated as “*the right to be let alone*”¹³⁵, while it is considered that the authors added a chapter in the long-living

¹³² An argument by the author sets three principles (1) limiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal, whenever information travels between social spheres.

See also: Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. REV. 119, 137-38, 155 (2004) 107

¹³³ Rebecca Wexler, The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates, 17 Yale J.L. & Tech. 368 (2015) 370

¹³⁴ Id. at 370

¹³⁵ Samuel D. Warren and Louis D. Brandeis “The Right to Privacy” Harvard Law Review Vol. 4, No. 5 pp. 193-220 (Dec. 15, 1890) 193

legal scholarship¹³⁶. In a thorough taxonomy by Daniel J. Solove, privacy is defined as an umbrella term, “*encompassing a series of distinct harms that share mere family resemblance*”, that is “*dignitary injuries, power imbalances, and the chilling effects caused by the risk of future injury*”¹³⁷. Alan Westin perceived privacy as the “*claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*”¹³⁸. Plus, Richard Posner resorted “*that one aspect of privacy is the withholding or concealment of information*”¹³⁹.

As a fundamental right, a general privacy right is enshrined in various legal texts, from declaration documents to strictly binding and enforceable ones. In EU, indicatively, in OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data¹⁴⁰, in article 12 of the Universal Declaration of Human Rights¹⁴¹, in the seminal article 8 of the European Convention of Human Rights (Right to respect for private and family life)¹⁴², in articles 7¹⁴³ and 8¹⁴⁴ of the Charter of Fundamental Rights of the

¹³⁶ Letter from Roscoe Pound to William Chilton (1916) quoted in Brandeis Mason: A free man's life 70 (1956), in Dorothy J. Glancy “The Invention of the Right to Privacy” (Santa Clara Law Santa Clara Law Digital Commons 1979) 1 available at <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1318&context=facpubs> accessed 1 July 2018

¹³⁷ Daniel J. Solove, “A Taxonomy of Privacy”, 154 U. PA. L REV. 477 (2006) 487

¹³⁸ Alan Westin, “Privacy and Freedom” (New York: Atheneum 1967) 7

¹³⁹ Richard A. Posner, “The Right of Privacy” (Georgia Law Review Vol. 12, No. 3. 1978) 393

¹⁴⁰ Since 1980, these principles continue to represent international consensus on general guidance concerning the collection and management of personal information, available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#part2> accessed 1 July 2018

¹⁴¹ Article 12 of UDHR in 1948 mentions: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”, available at http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf accessed 2 July 2018

¹⁴² It is concisely referred that (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

¹⁴³ Article 7: Respect for private and family life

“Everyone has the right to respect for his or her private and family life, home and communications.”

¹⁴⁴ Article 8: Protection of personal data

“(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.

European Union, and lastly in the Convention of the Council of Europe Nr. 108 for the protection of individuals with regard to automatic processing of personal data¹⁴⁵. Most significantly, though, privacy in terms of end-users' usage of DRM systems, is safeguarded by the newborn General Data Protection Regulation¹⁴⁶ (hereinafter GDPR), which repealed Directive 95/46/EC (Data Protection Directive). While further analysis will follow regarding freshly-uncovered dimensions in data protection, a crucial priority is that DRM systems are assorted, according to their function.

4.2 Digital Rights Management systems categorized by pervasiveness

As the new business models, all software packages managing digital rights, are not identical apropos operation and data collection. They could be roughly summarized in the following distinct categories. What is the relevant criterion for classification, could be illustrated in a scale of intrusiveness, ranging from innocent DRM systems spectating anti-circumvention behavior to the ones monitoring (and influencing) our online activity.

Firstly, in order to constrain further reproduction of the work, a software developer may install a *constraining* DRM application. Predominantly selected to protect unauthorized usage, this type is truly correlated to copyright protection and rarely exceeds its purpose. What is meant to exist for, is keeping the content intact, while industries and consumers embrace its presence. Protection is supposed to be “for the user”, yet it is “from the user”¹⁴⁷. In quantifying its contraposition to privacy, no unapproved data accumulation takes place, due to its defensive leverage.

¹⁴⁵ Available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> accessed 2 July 2018

¹⁴⁶ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EL> accessed 2 July 2018

¹⁴⁷ These kind of DRM mechanisms are generally considered legitimate, since the decrease in users' autonomy level and freedom of expression is proportional to the right protected, that of copyright. Not a privacy invasion is observed, however, purpose misrepresentation is a fact. Chapman & Hall/CRC Computer and Information Science Series, “The practical handbook of Internet computing (2005) 212

One different construction of the DRM system *links* content permanently to a finite number of devices, in other words, software is trapped in hardware¹⁴⁸. Apart from lack of interoperability, any producer constantly oversees device swapping¹⁴⁹ keeping a customer record¹⁵⁰, a state which ensues privacy tampering.

Another category of DRM mechanisms associated principally with copyright and secondarily with data collection, are the ones *controlling user access* to tied content. Metadata¹⁵¹ specify the scope of actions available¹⁵², for instance the aforementioned encryption technique (passwords) requires user authentication¹⁵³ in order to release the rights related to the copy of that work. If this is the case, no violation of privacy is recognized, as long as authentication is materialized offline, nevertheless, to persistently identify yourself online, engenders serious concerns.

¹⁴⁸ In a tie-in scenario, where copyrighted content (computer programs) are in a particular storage device, happens in Sony Aibo Dog robot. In order to prevent secondary market competition, producers manufacture incompatible services. Whoever attempted to distribute online functionality-enhancing software for that robot, under the fair use doctrine, would receive a cease and desist letter from Sony.

¹⁴⁹ In consumer sociology, the term "*planned obsolescence*" implies a strategy by which planning or designing a product with an artificially and uneconomically short useful life, impels customers to make repeated purchases. Typical trait of mainstream technology products, such as mobile phones, portable devices and computers. DRM systems are designed to track consumers' purchasing habits as well, along with exclusivity of the content (for instance Apple Inc. products)

See also: Jeremy Bulow, An Economic Theory of Planned Obsolescence The Quarterly Journal of Economics, Volume 101, Issue 4, 1 November 1986, Pages 729–749, available at <https://academic.oup.com/qje/article-abstract/101/4/729/1840176?redirectedFrom=fulltext> accessed 5 July 2018

¹⁵⁰ Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 5

¹⁵¹ Metadata is in a very real sense data which describe, explain or refer to other data. Another definition, "data that provides information about other data", is available at Merriam-Webster dictionary <https://www.merriam-webster.com/dictionary/metadata> accessed 5 July 2018

¹⁵² Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 4

¹⁵³ Indistinguishable words in everyday semantics, are the following totally distant concepts: *identification*, *authentication* and *authorization*. In further delving into privacy points in question, they should be clarified, as their roles are distinct steps in DRM architecture.

-*Identification*, in information security signifies the claim of an individual to be somebody. By internet terms, that is equal with typing a username, while in non-digital life one equivalent would be for one to be introduced by their name. Also, this commences an activity, e.g. requesting the exercise of rights connected with DRM protected content. In this dialogue, probably the software will demand further authentication.

-*Authentication* is called the process by which one validates the information which had provided by identifying themselves. As a double-check, it varies from password typing to retina scanning in biometrics, or it could take the form of one's ID check in real life. The essence of authentication is for the DRM system to be persuaded that rights are to be legitimately accorded to the authenticated user, who has revealed a secret nobody else holds.

-*Authorization* is to be determined by the system now, as the third step. Collecting attributes about one's identity, it accredits them with privileges. An access or denial are the most frequent outcomes in connection to DRM systems.

It shall be stressed once more that, although Data Protection Regulation exists, no legal framework governs the architecture and functionality of DRM systems¹⁵⁴, therefore only practical advice for the engineering process¹⁵⁵ are available to developers. If identification and authentication are required, then initially they serve in confirming that users hold the appropriate keys, in a broad sense, to unlock the content, forestalling copyright infringement. On behalf of the rights holder, the claim of ownership has to be associated with the content and the consumer to be named¹⁵⁶. In contrast to authentication, which could be performed in an anonymous way¹⁵⁷, sometimes consumers have no other choice but to uniquely identify themselves in an online environment, furnishing personal minable data¹⁵⁸, which is not always deemed necessary. *Identification* systems are the firsts to handily permeate into users' personal information, in a manner which the singled out evades being the center of attention by

¹⁵⁴ Up until now in EU, only anti-circumvention provisions for digital content have been enacted, an instance which favors malevolent DRM developers and companies.

Jens Eckhardt, Martin Lundborg & Claudia Schlipp, "Digital Rights Management (DRM) and the development of mobile content in Europe" *Computer, Law & Security* (2007) 545

¹⁵⁵ Apparently, law is not the only discipline to be involved in privacy issues. Recently, an emerging field in engineering assumes a stand-alone existence as "Privacy Engineering". Pursuant to the definition articulated by the National Institute of Standards and Technology, "[Privacy engineering] focuses on providing guidance that can be used to decrease privacy risks and enable organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems". It could be called a derivative scientific field concerned with the practical implementation of privacy laws into IT systems.

See also "Privacy Engineering Program", available at <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering>, accessed 5 July 2018 and "IPEN - Internet Privacy Engineering Network" available at https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en accessed 5 July 2018

¹⁵⁶ Becker, E., Buhse, W., Gunnewig, D., Rump, N.: *Digital Rights Management, Technological, Economic, Legal and Political Aspects*. Berlin: Springer-Verlag Berlin Heidelberg (2003) 8

¹⁵⁷ To depict, an end user may be required to type the serial key number in a software product (e.g. Microsoft Office) without being needed to explicitly state who they are, whereas a considerable number of online products demand personal user identification prior to usage.

¹⁵⁸ Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 5

In the term "minable data" lies the uttermost foundation of why data is so valuable. It suggests information that could be extracted by certain programming techniques so that thought-provoking patterns are discovered by statisticians. Public institutions or private corporations store data in warehouses to identify association rules, mainly for marketing reasons.

See also: Morgan D., Kang J.W., Kang J.M., *Minable Data Warehouse*. In: Filipe J., Cordeiro J. (eds) *International Conference on Enterprise Information Systems. ICEIS (2009). Lecture Notes in Business Information Processing*, vol 24. Springer, Berlin, Heidelberg

other users; in principle, subject attention and user anonymity may harmonically coexist¹⁵⁹.

Weighting the identification and authentication schemes, a reasonable threat towards users' right to privacy is raised by contemporary, newfangled DRM middleware, the ones incessantly *monitoring* (and manipulating) consumer behavior. Contrary to the above-mentioned autonomous DRM systems¹⁶⁰, markets have imposed the utilization of *net-dependent* DRM systems¹⁶¹, also called *always-on* DRM¹⁶². Whenever mechanisms as these are employed, permanent surveillance is actualized in the online environment and not only, in a sense that not only metadata are processed, but images, fingerprints, voices and human faces¹⁶³. An unprecedented phenomenon for humanity, in an automated way and usually surreptitiously, software programs meter and quantify humans in terms of activity, preferences and choices, prescribing 24/7 instructions for close examination¹⁶⁴. Whether initially the objective was any guarding of copyrighted-content or managing digital licenses, nowadays the DRM evolution standard has displaced the belief that "*one's home is one's castle*"¹⁶⁵, by straightforwardly controlling intellectual consumption. Traditionally, a two-tiered surveillance could be

¹⁵⁹ Julie E. Cohen, DRM and Privacy, Georgetown Law Faculty Publications and Other Works, Berkeley Technology Law Journal. Vol. 18. (2003) 587, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed at 5 July 2018

¹⁶⁰ Autonomy is the state of a DRM which requires no extra outside interaction in fulfilling its purpose.

¹⁶¹ Net-dependence in computing is named the state by which a DRM software constantly communicates with external parties via Internet. In other terms, it cannot function properly without internet connection.

See also: Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York) 285 and

Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) executive summary iii

¹⁶² In case of video games, which are normally protected as computer software (code), intense criticism and pressure have been exerted against players' persistent authentication, through always-on DRM systems. Distinguished franchises have adopted this strategy, such as Diablo III, Starcraft II, SimCity, Darkspore, The Settlers VII, Assassin's Creed II, The Crew, The Division, Need for Speed and Hitman. Developer companies argue in favor of cloud computing and copyright infringement, while lawful buyers complain against slow servers and pirate copies.

Wikipedia (aggregate article), "Always-on DRM" available at https://en.wikipedia.org/wiki/Always-on_DRM#cite_note-13 accessed 5 July 2018

¹⁶³ For instance, a camera may itself operate as a hardware DRM system, where it proceeds in face control, or iris scanning. Equally, when a fingerprint sensor identifies a uniqueness is a persons' finger, allows access to the associated content.

¹⁶⁴ Ian Kerr and Jane Bailey, The Implications of Digital Rights Management for Privacy and Freedom of Expression, Faculty of Law, University of Ottawa, Ontario, Canada, Info, Comm & Ethics in Society (2004) 89

¹⁶⁵ Id. at 90

performed either by the phone-home¹⁶⁶ approach, or through a subscription service¹⁶⁷. One way or another, processing of data by third parties which do not always act as legitimate data processors or controllers, is an unfortunate reality.

As a summary, interference with one's right to privacy and self-determination is principally encountered during the surveillance DRM systems' performance, while it is evident that all perils are accumulated in this category. In the following subchapter, it will be discussed why machine-readable data proves to be of so high value, in an extent that industries shifted their priorities in DRM engineering¹⁶⁸, from safeguarding content, to amassing data.

4.3 The new era DRMs: incessant "omniveillance" in a data-driven economy

Within the scope of the present thesis fits a general explanation of why the circumstance of data collection sacrifices private life. What makes data so valuable, and why has the EU invested unimaginable resources to establish an internal data space and network¹⁶⁹ will be briefly exposed in this part.

Unilateral personal-data sharing directed to massive corporations, although sounds an unbalanced recourse, may actually beget a series of favoring circumstances for end users, leveraging their online experience. In an impersonal life, internet individuality

¹⁶⁶ Phone home in computing and information security refers to that action by which streams of bits are reported back to the server by the client/user, naturally without the latter neither acknowledging these flows of information nor necessarily endorsing them. Normally it takes place after a product was downloaded or a service was used. Interestingly, data may be intentionally encrypted by malware software installed on users' computer, transmitting back usernames, location and other data. As displeasing and as this profiling may seem, it proves to be both unregulated and mostly triggered by the private sector.

¹⁶⁷ Presupposing an insertion of credentials, this technique ties a users' account with individual behavior, building fine-grained, digital-personality profiles, suppressing private space. See also: Lee A. Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests (Published in European Intellectual Property Review, 2002, vol. 24, no. 2, pp. 51–57) 5

¹⁶⁸ Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 2

¹⁶⁹ Elements of the European data economy strategy (Digital Single Market, Policy, 25 April 2018) available at <https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy> accessed 8 July 2018 and Communication (25 April 2018) "Towards a common European data space" available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN> accessed 8 July 2018

and “*profiling is used to cluster data in such way that information is inferred, and predictions or expectations can be proposed*”.¹⁷⁰ Based on probabilistic theories, aggregated data contribute in pattern drawing, and predictability in consumer behavior. Intriguingly, neither a novel notion nor a groundbreaking technique is applied. Yet crucial element in our times is the fashion of data collection; big data¹⁷¹ against informational privacy.

Among other pretexts, frequently vaguely described in companies’ privacy policy are the following: delivering of personalized entertainment, marketing and commercial purposes¹⁷², administrative and internal reasons, selling to third parties or improvement of products and services.¹⁷³ Especially within the frame of the latter, institutions seek to enhance their Quality of Service¹⁷⁴, via responsive feedback from customers. Piles of data are definitely processed proactively for combating piracy, imposing restrictions and controlling traffic. They enrich economies of scale and production by decreasing cost, while resolutely promote efficient decision making. Turning to sheer and direct economy, Big Data favor differential pricing¹⁷⁵ privileging the sellers to explore the demand curve and achieve targeted marketing, thus charging personalized fees for the exact same product. In a more abstract level, other legitimate reasons for data

¹⁷⁰ Serge Gutwirth, Yves Poullet, Paul De Hert, “Data Protection in a Profiled World”, Springer Netherlands (1st edition 2010) 32

¹⁷¹ Data sets which feature qualitative and quantitative massiveness and complexity are called Big Data. A term used since 1990s and coined by John Mashey, is demarcated by what is called the five V of Big Data: *Volume, Velocity, Variety, Variability* and *Value*
Anil Jain, The 5 Vs of Big Data (17 September 2016) available at <https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/> accessed 8 July 2018

¹⁷² Personalized advertisements more efficiently attract consumers than general and random content-based ones.

¹⁷³ Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 37

¹⁷⁴ Improving QoS With Big Data Analytics available at <https://tmt.knect365.com/telco-data-analytics-europe/improving-qos-with-big-data-analytics> accessed 8 July 2018

¹⁷⁵ Differential pricing is divided in three categories: first-degree price discrimination is applied when individual sellers charge dissimilar prices due to negotiation with buyers individually; second-degree occurs when quantity discounts reduce the per-unit price; lastly third-degree price differentiation takes place when economically vulnerable groups, such as students, possess a legal privilege for discount. One rationale behind behavior data accumulation is the correct profiling of customers, in order for the sellers to identify the maximum exact amount of money one is willing to pay, and subsequently adjust their prices marginally, to what each user may afford. Data precious to sellers are user location, browser and search history, streamed content, reviews and posts etc., information closely related to what a net-dependent DRM system may dexterously collect.

See also: Executive Office of the President of the United States, Big Data and Differential Pricing (February 2015) 4 available at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf accessed 10 July 2018

acquisition involve archiving or backup¹⁷⁶, traffic modeling, mining of depersonalized values for tendencies identification, statistical purposes, risk management¹⁷⁷, social sorting¹⁷⁸ etc.

Data multiplication is not a synonym to data significance. Bulks of information non-valuable at first sight do prove inestimable, in conjunction with today's originality; from a traditional collection, we move to automated compilations, after that to correlations, and finally detections, measurements and quantification. *"The detection of the correlation is the information"*¹⁷⁹ is one present-day motto, while *"[human] actions have become the resources of an extensive, if not unlimited, network of possible profiling devices generating knowledge affecting and impacting upon them"*¹⁸⁰.

As a concluding remark, an appeal to the technology neutrality principle would conclude that DRM functioning is legitimate, since policymakers should not push the market towards particular (subjectively optimal) structures¹⁸¹. Because of the topic's intricacy, to discern whether data controllers' purposes for collection are legitimate or illegitimate, would amount to a severe and arduous task in a technologically ever-evolving society.

4.4 Types of privacy; informational privacy

Ceaseless surveillance is not always the case. Within the DRM systems family, one notices a gradation in privacy rights encroachment. What part of the manifold right to private life is violated, shall be discussed in this passage.

¹⁷⁶ Data Archiving for Modern Business Big Data Initiatives available at <http://hortonworks.com/wp-content/uploads/2014/02/Cisco-and-Hortonworks-Data-Archiving-.pdf> accessed 10 July 2018

¹⁷⁷ Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 2

¹⁷⁸ Categorization of individuals in subsets by data manipulators. When consumers become personally identifiable subjects, they may as well be sorted by criteria as age, race, education, gender, ethnicity, etc.

¹⁷⁹ Serge Gutwirth, Yves Poullet, Paul De Hert, "Data Protection in a Profiled World", Springer Netherlands (1st edition 2010) 33

¹⁸⁰ Id. at 33

¹⁸¹ Maxwell, Winston and Bourreau, Marc, Technology Neutrality in Internet, Telecoms and Data Protection Regulation (November 23, 2014). Computer and Telecommunications L. Rev. (2014) 1, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529680 accessed 12 July 2018

A different aspect is menaced whenever technological products attain commercial circulation. According to a recent typology¹⁸², physical privacy is perceptibly distinguished by informational privacy. While the first one comprises types as bodily, spatial, communicational, proprietary, intellectual, decisional, associational and behavioral privacy, the overlapping layer of informational privacy resembles “*the other side of the coin*”¹⁸³ to each ideal¹⁸⁴ physical privacy type. Informational privacy is strictly interwoven to the entirety of physical privacy, as a positive and negative freedom¹⁸⁵. While physical privacy contains the substance and matter of one’s actions, informational privacy mostly adheres to the information emanating from such adoption, i.e. personal data. In a concomitant definition, *control*¹⁸⁶ remains a fundamental element, thus whoever possesses it, may simultaneously designate how to exclude access on the one hand and how to raise walls on the other, protecting their confidentiality, e.g. in communications.

¹⁸² Unlike previous attempts to demarcate the right to privacy, this typology highlights associations which were absent in other classifications or taxonomies. In a four-dimensional model, nine in total types of privacy are portrayed, with scales of *access – control*, *personal zone – public zone* and *freedom to be let alone – to be self-developed* being used.

“An analytic and evaluative tool to help assess the impact of new technologies, social practices and legal measures on broader privacy interests.”

Koops, Bert-Jaap and Newell, Bryce Clayton and Timan, Tjerk and Škorvánek, Ivan and Chokrevski, Tom and Galič, Maša, A Typology of Privacy (March 24, 2016). University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, 488, 566. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043 accessed 12 July 2018

¹⁸³ Id. at 568

¹⁸⁴ As long as technology flows, so will society and ethical norms. As of today, it is DRM systems that shape our privacy concerns, in the near future probably a way graver threat. No ideal type could exist eternally. As Cohen J. aptly note down, “...nor does privacy reduce to a fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic...privacy is fundamentally dynamic. In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination...an interest in breathing room to engage in socially situated processes of boundary management”

Julie E. Cohen, What Privacy is for, 126 HARV. L. REV. 1904, 1907 (2013) 3

¹⁸⁵ Freedom *to do* something demonstrates a positive action, whereas freedom *from* something expresses a negative aspect. Due to techno-regulation’s structure, frequently, end users need to defend their right to privacy rather than actively exercising it. Recent emerging concepts such as “privacy by design” and “privacy by default” have become enforceable by the General Data Protection Regulation.

¹⁸⁶ Moore, Adam D., Defining Privacy (2008). Journal of Social Philosophy, Vol. 39, No. 3, pp. 411-428, Fall 2008, 414. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1980849 accessed 12 July 2018

Without prejudice to communicational and behavioral¹⁸⁷ privacy, it is informational/intellectual and spatial privacy which are inflicted most damage. Compelling surveillance belittles exposed human dignity, reducing consumers to “*the sum of their profiles*”¹⁸⁸. Physical space, or spatial activity, concerns primarily home conduct, where individuals take it for granted that such privilege is to be enjoyed in an untethered fashion. Not an equivalent to property, though, a right which is normally inviolable.

Repercussions of a twofold character arise, in relation to DRM application and privacy, since confidential information diffuses rather exponentially. Firstly, *constraining* private conduct, secondly, *storing* (almost) permanent records of end-users’ activity.¹⁸⁹ A mere content protection (copy control) would not engage one’s personal sphere, even if it lessens autonomy. Only, it would provoke anti-competitive effects, if applied to its maximum. DRM embedded mechanisms, which limit accessibility, get the job done, manifestly preserving copyright integrity. Above designated as surveillance or monitoring DRM technologies, these software packages automatically compile data records, digitally exploring the victim’s devices, either online or offline. Informational privacy standards immediately diminish, and re-use or re-purposing of personal data for secondary reasons acts as the norm¹⁹⁰.

¹⁸⁷ “A person’s interest in restricting access to communications or controlling the use of information communicated to third-parties” and “typified by the privacy interests a person has while conducting publicly visible activities” respectively.

Koops, Bert-Jaap and Newell, Bryce Clayton and Timan, Tjerk and Škorvánek, Ivan and Chokrevski, Tom and Galič, Maša, A Typology of Privacy (March 24, 2016). University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, 568. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043 accessed 12 July 2018

¹⁸⁸ Julie E. Cohen, DRM and Privacy, Georgetown Law Faculty Publications and Other Works, Berkeley Technology Law Journal. Vol. 18. (2003) 578, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed 12 July 2018

¹⁸⁹ Id. at 580

¹⁹⁰ Typically, when informational privacy gets breached and personal data uncontrollably stream towards third parties, an annoyingly unsettling situation awaits the end user. A habitual example involves enforcement security (the pretext), while eventually the user discovers that marketing purposes and cross-selling of their information was the latent intention. Above all, lack of consent or surpassing the limits thereof by the data controller clashes with the data subject’s informational privacy.

See: Lee A. Bygrave, Digital Rights Management and Privacy, Legal Aspects in the European Union E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 422

In conclusion of this panorama pertaining to types of privacy, it should be underlined that it is the privacy right's core which is struck, that of spreading of information¹⁹¹. A comparable assault is effected by most cyberspace products, implemented for similar purposes. Strengthening and orientating the engineering process to usher privacy-friendly guidelines, is the intention of the General Data Protection Regulation, which will be discussed below, and the proposal for the EU ePrivacy Regulation.

4.5 European Union privacy legislation

Until recently, the role of an adamant reference frame to data protection in Europe played the now repealed Directive 95/46/EC¹⁹². As a regulatory point of departure, it included a prescriptive guidance across the totality of sectors¹⁹³, while possessed an imperative character. Since 25 May 2018, the Data Protection Directive, along with the national provisions transposing it, is substituted by the GDPR. Simultaneously with GDPR, the ePrivacy Regulation¹⁹⁴ was supposed to come in force and repeal Directive 2002/58/EC¹⁹⁵, but due to temporal miscalculations, it is expected around 2019¹⁹⁶.

¹⁹¹ Prevailing of informational privacy is once again stated by J. Cohen: "The body of constitutional privacy doctrine that defines unlawful "searches" regulates tools that enable law enforcement to "see" activities as they are taking place inside the home *more strictly* than tools for discovering information about those activities after they have occurred."

Julie E. Cohen, "Privacy, Visibility, Transparency, and Exposure", University of Chicago Law Review, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, 182. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1012068 accessed 12 July 2018

¹⁹² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, valid until 24 May 2018. Not only a European but also EEA extendible legal instrument. A one-of-a-kind law, no such omnibus legislation regulating personal data exists in US, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> accessed 13 July 2018

¹⁹³ Lee A. Bygrave, Digital Rights Management and Privacy, Legal Aspects in the European Union E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 424

¹⁹⁴ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN> accessed 15 July 2018

¹⁹⁵ DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> accessed 15 July 2018

¹⁹⁶ Dr Frank Eickmeier "What does the ePrivacy Regulation mean for the online industry?" (14.02.2018) available at

Constitutive aim of the latter is to supplement GDPR, functioning as *lex specialis*, enhancing privacy in electronic telecommunications.

To the privacy-defending trilogy¹⁹⁷ is added the relevant provision of the Copyright Directive, concerning users' initiative and possibility to circumvent DRM systems' privacy-intrusive operations. Notably, the legitimacy of DRM middleware activity is highly controversial, even more if they are subjected to the technological measures' scope, set by article 6(3) of the Copyright Directive. In a negative scenario, which is widely supported¹⁹⁸, end users could perfectly avail themselves of favorable self-help steps, that is to licitly circumvent the content-protecting technology¹⁹⁹. Though, that depends on the contextual definition of surveillance and monitoring as objectives per se. If panoptic²⁰⁰ DRM systems pertain to effective technological measures' ambit, protection shall be granted to them. Otherwise, if designed merely for malicious privacy meddling aims, the act of bypassing it should be recognized as a fully rightful defense.

4.5.1 General Data Protection Regulation, an overview and new entries

In order for a technological legislative instrument to be ensured survivability, it remains of quintessential importance to avoid overregulation, by adopting broader definitions. For an extended in time regulatory goal, over-inclusiveness or under-inclusiveness²⁰¹

<https://www.eprivacy.eu/en/about-us/news-press/news-detail/article/what-does-the-eprivacy-regulation-mean-for-the-online-industry/> accessed 15 July 2018

¹⁹⁷ Another legislative document with regard to data generated in communications platforms, was the Data Retention Directive, or Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=EN> accessed 15 July 2018. Due to the unconstitutionality of prolonged data occupation, the ECJ in April 2014 adjudicated against its legality.

¹⁹⁸ Lee A. Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests (Published in European Intellectual Property Review, 2002, vol. 24, no. 2, pp. 51–57) 7

¹⁹⁹ A typical self-help measure is the installation of external mod-chips in hardware, which are also covered by the ambit of the InfoSoc Directive's TPMs definition. Under certain circumstances, the European Court of Justice adjudicated in favor of these defensive steps, in Nintendo of Europe GmbH v. PC Box Srl, 9Net Sr C-355/12 (2014)

Marcella Favale; Neil McDonald; Christos Gatzidis, Human Aspects in Digital Rights Management: The Perspective of Content Developers, 13 SCRIPTed 289 (2016) 299

²⁰⁰ Id. at 7

²⁰¹ Solum, Lawrence B. and Chung, Minn, The Layers Principle: Internet Architecture and the Law. U San Diego Public Law Research Paper No. 55, 49

points should delimit legislators. Therefore, as an introductory remark, GDPR encircles “personal data” in the following (generalized) wording:

*“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”*²⁰²

Despite its overbreadth, data protection rules’ scope should neither be overstretched nor be construed in a restricting manner²⁰³. *Personal data* must be the object of a processing step for the Regulation to be applied. Of considerable significance is the identifiability of the natural person, either directly or indirectly, a term used to express the possibility of identification²⁰⁴, thus amplifying its reach. All DRM systems acquiring such data should fall inside the boundaries of the Regulation, even when ancillary data helps to particularize data subjects²⁰⁵. Furthermore, group data are excluded as non-personal, while data educed under pseudonymization or anonymization measures do not

²⁰² Article 4(1), encompassing the definitions for the purposes of GDPR.

It is worth mentioning that in the repealed Directive’s text, the definition was slightly less illuminative: ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

The terms *location data* and *online identifier*, explicitly stated in the renewed definition, are elements pertaining to novel technologies, such as modern DRM systems.

²⁰³ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (2007) 4 available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf accessed 1 August 2018

²⁰⁴ “[A] person may be identified *directly* by name or *indirectly* by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.

Id. at 12

²⁰⁵ The very first proposal on the Data Protection Directive explains the ambit of personal data and its implications.

Commission of the European Communities: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (15th October 1992) COM (92) 422 final – SYN 287, 9 available at the Archive of European Integration <http://aei.pitt.edu/10375/1/10375.pdf> accessed 1 August 2018

appertain to article 4(1). To this principle's assistance comes Recital (26)²⁰⁶, the phrasing of which clarifies the theoretical properties of an identifiable subject.²⁰⁷

Depending on which personal data the DRM system collects, its controller or processor in the event of a data breach may be accordingly held liable²⁰⁸, while the end user is accorded the right to lodge a complaint. At the same time, since DRM systems function in a multinational digital environment, Codes of Conduct (article 40 GDPR) are to be formulated and respected concerning transfer to third countries²⁰⁹. Lastly, article 32 GDPR²¹⁰ obliges DRM tool adopters to keep pace with the state of the art and incorporate corresponding measures, averting any risk of inconsistency with advancement in technology.

A general obligation subsection (articles 24-31 GDPR) enumerates responsibilities by processors and controllers with article 24²¹¹ stating their duty to embrace appropriate measures. A prominent place amidst these obligations occupies the obligation to maintain records under the controllers' responsibility²¹², which renders their position

²⁰⁶ Recital (26) GDPR: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

²⁰⁷ Lee A. Bygrave, *Digital Rights Management and Privacy, Legal Aspects in the European Union* E. Becker et al. (Eds.): *Digital Rights Management*, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 422

²⁰⁸ In articles 77-84 GDPR both the data controller and the processor are held liable for the entire damage caused to the data subject by processing that infringes the Regulation. The same applies for joint controllers and joint processors, while administrative fines are extremely high (article 83 GDPR). This extended liability was absent in Directive 95/46/EC.

New obligation of the controller is to notify the personal data breach to the relevant supervisory authority and the data subject, whereas the processor must report to the controller (articles 32-34).

²⁰⁹ Truly, in contrast to the Data Protection Directive where only the adequacy decision was provided for, the recent legislation introduces the appropriate safeguards, e.g. enforceable standard data protection clauses, approved certification mechanisms or Binding Corporate Rules.

²¹⁰ Article 32(1): "...the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

²¹¹ Article 24(1) regarding the responsibility of the controller: Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

²¹² Article 30(1)(2) for the controller and the processor respectively.

vulnerable regarding past unsolicited intrusions, and relocates the burden of proof. However, a data processing principle, acting as future cornerstone, has been introduced into the legal text rather than the Recitals²¹³, that of Privacy by Design²¹⁴. By the last mentioned, the controller must implement mechanisms that by default ensure a data minimization regime, in terms of storage, access, retention and processing, considering the cost and state of the art.

Operators of DRM mechanisms must comply with a series of specifications to the Directive, imported by the Regulation. Specifications in the right to rectification, erasure (*right to be forgotten*) and restriction in processing personal data (articles 16-18 GDPR) are put into effect. An economically meaningful right²¹⁵ for a digitally integrating Europe, the right to data portability enables user-centric interoperability²¹⁶, while benefiting the entire data sector²¹⁷. Especially, this right forces a defined level of functionality and semantic communication between devices, which discontinues any usage of stiff DRM systems. The modalities of exercising these rights by the data subject are extended. To comply with the Regulation, a manifest and comprehensible²¹⁸ summary must be delivered to the end user, including information about their processed data and how to access them (article 12 GDPR).

²¹³ Tikkinen-Piri, Christina & Rohunen, Anna & Markkula, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. The International Journal of technology Law and Practice (2017) 9

²¹⁴ Article 25 GDPR, regarding Data protection by design and by default, which will be discussed below.

²¹⁵ Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, Volume 34, Issue 2, Pages 193-203 (2018) 195

²¹⁶ Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, Digital Single Market REPORT / STUDY (25 April 2018) available at <https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and> accessed 2 August 2018

²¹⁷ Article 29 Data Protection Working Party reckons that: "data portability could enable businesses and data-subjects/consumers to maximize the benefits of big data in a more balanced and transparent way. It can also help minimize unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes, which would benefit both businesses and data-subjects/consumers." Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 47

²¹⁸ Article 12 GDPR: ... in a concise, transparent, intelligible and easily accessible form, using clear and plain language...

4.5.2 Personal data: criteria for lawfulness of processing

Without a legitimate ground for data processing, it is interdicted for DRM systems to access and process end users' data. Contrary to the Directive's scope, the Regulation noted remarkable developments with reference to the notion and conditions of consent (article 7 GDPR), which remains the nucleus of data processing. To assess the lawfulness of processing by DRM systems, the following criteria are applied²¹⁹:

- “(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Compared to other criteria, it is, by far, the *affirmation of consent* which normatively characterizes data protection. During the pre-GDPR era, DRM systems operators could less severely equivocate in relation to consent circumstances. Pre-ticked boxes, silence, inactivity and click-wrap agreements would be the rule, but henceforward the Regulation incapacitates these tactics²²⁰. Consent must be given on a voluntary basis, in a “free” manner²²¹, implying that no exogenous constraints affect the outcome of the

²¹⁹ Conditions (d) and (e) from article 6 GDPR are omitted due to irrelevance to DRM systems' application. [(d) processing is necessary in order to protect the *vital interests* of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller

See: Lee A. Bygrave, Digital Rights Management and Privacy, Legal Aspects in the European Union E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 430

²²⁰ Recital (32) GDPR, describing the conditions for consent, explains that: “consent should be given by a *clear affirmative act establishing a freely given, specific, informed and unambiguous indication* of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.”

²²¹ Intersoft Consulting services AG GDPR, available at <https://gdpr-info.eu/issues/consent/> accessed 3 August 2018

choice. Its character may be implicit or explicit, whenever needed [e.g. article 9(2)(a) GDPR]. Notification should always precede processing, so that data subjects are given the opportunity to consent or not (e.g. cookies in browsers, “clickstream” data²²²). Frequently an unethical limitation is observed in software, that of bundling processing purposes. Legitimacy could be achieved only by *granularity*²²³, in other words separating and obtaining consent individually for each purpose. Other voiding factors involve imbalance of power, conditionality clauses and detrimental instances, thus consent is not presumed to be freely given²²⁴. Withdrawal, lastly, shall be effected without detriment and as comfortably as the manner it was given²²⁵.

The second criterion stipulated in article 6, sets forth the *performance of a contract* at the request of the data subject as a legitimate basis. Usually, it is end users who externalize their interest in accessing DRM-protected content, thus it is only natural that prior processing by the operator is vital. Examining digital-content purchases from online stores, it goes questionless that personal data will be collected²²⁶. Two capital principles safely pave the way for legitimate processing, that of commercial need and proportionality to the aim of the contract²²⁷.

²²² “Clickstream analytics” is the process of collecting, analyzing and reporting aggregate data about which pages a website visitor visits -- and in what order. The path the visitor takes though a website is called the clickstream. Particularly beloved information for marketers, click paths reveal the customers’ entire online journey.

Available at <https://searchcrm.techtarget.com/definition/clickstream-analysis> accessed 3 August 2018

²²³ Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 17/EN WP259 rev.01 (April 2018) 9 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed 4 August 2018

²²⁴ Example [1] on the WP guidelines: “A mobile app for photo editing asks its users to have their GPS localization activated for the use of its services. The app also tells its users it will use the collected data for *behavioral advertising purposes*. Neither geolocation or online behavioral advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.”

The DRM of the mobile photo application surpasses the limits of freely acquired consent, coercing the end user to consent on conditions, unjustifiably limiting their privacy.

Id. at 5

²²⁵ Recital (42) GDPR stresses that: “...consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.”

²²⁶ Before DRM systems credit to the user a disseminated copy of the copyright protected content, access to personal details will be requested, typically identification details, billing address, date of transaction, credit card number etc. Limits in personal data processing should be applied decisively, in a standardized form.

²²⁷ To abstractly establish rules about what data should be retained is an unfeasible task, as far as online purchases is concerned. Nevertheless, examining the absolute necessity of processing in every particular contract, should fulfill article 6(b) GDPR. Pre-contractual obligations are included, while

Of mediocre importance is the third legitimate basis, *the compliance with a legal obligation*, particularly when joint controllers' roles are put together, contractually assuming obligations²²⁸. Again, non-orientation or omission to notify the data subject, results in non-compliance. Strict lawfulness is the outcome of the last provision, namely 6(1)(f). Although widely interpreted, between the enforcement of controllers' legitimate interests and end-users' *fundamental freedoms*, the last named must prevail. Being elusive and unintelligible meanings, fundamental freedoms²²⁹ should be particularized on a case by case basis, with factual events, for an effective equilibrium.

The Regulation addresses special categories of data in article 9, enumerating vague and nebulous rights²³⁰, yet being more up-to-date and extensive, in comparison with the Directive. In DRM context, sensitive data may be processed only in consonance with a justifying ground²³¹. By rights, the end-users' explicit consent should be granted duly, for instance when a consumer buys digital content pertaining to the healthcare industry, or media files concerning history, politics and ethnography, or possibly content disclosing sexual orientation and religious matters. Premises for legitimate processing are exhaustively itemized, but DRM operators must comply with data processing principles (e.g. data minimization), aside from the indispensability criterion, which denotes a stringent measure.²³²

monitoring post-contract performance through net-dependent surveilling DRM systems, seems fairly disproportional.

Lee A. Bygrave, *Digital Rights Management and Privacy, Legal Aspects in the European Union* E. Becker et al. (Eds.): *Digital Rights Management*, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 431

²²⁸ The term "legal obligation" shall be construed narrowly to exclude simple agreements concluded by the DRM operators, where the data subject is not a party.

Id. at 432

²²⁹ DRM systems engaging in automated processing may infringe fundamental freedoms due to algorithm misprogramming (e.g. generating sensitive information from non-sensitive data)

Article 19 (Human Rights Organization) "Privacy and Freedom of Expression In the Age of Artificial Intelligence" (April 2018) 17, available at <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf> accessed 4 August 2018

²³⁰ Article 9(1) GDPR: ... personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation...

²³¹ Article 9 paragraph 2, points (a-j) GDPR

²³² Lee A. Bygrave, *Digital Rights Management and Privacy, Legal Aspects in the European Union* E. Becker et al. (Eds.): *Digital Rights Management*, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003) 435

4.5.3 Underlying principles of data processing

In a thorough Canadian Report, assessing a wide spectrum of commercial DRM systems²³³, the findings were enlightening enough to verify the consumers' suspicion against the privacy-permeating character of embedded software in media. *"Content distribution organizations that in the past lacked direct access to consumers now, through the use of digital technologies, observe the behavior of consumers even though the consumers' dealings with associated content has not changed"*.²³⁴ In order for the act of processing to fulfill the criteria for legitimacy, a set of principles ought to govern the lawfully acquired data processing. Pursuant to the meticulous nature of Recital 39 and article 5 GDPR, a surrounding framework is formed. Specifications in principles²³⁵ are mandated due to technological advancements. The Regulation recognizes the following seven principles: (a) lawfulness, fairness and transparency, (b) purpose limitation, (c) data minimization, (d) accuracy, (e) storage limitation, (f) integrity and confidentiality and (g) accountability, as stipulated in article 5(1) and (2) GDPR.

The indefinite and hazy wording of article 5 is attributable to an attempt not to overregulate. Deductions should be shaped only on a particular basis. What privacy legal instruments normally struggle to do, is pave the way, align different strategies and set standards. Thus, in obedience to these principles, DRM systems are to be engineered²³⁶.

All along the time, the outcomes' overview proved categorically poor, and cooperation was nonexistent. A tiny percentage of DRM systems would comply with data

²³³ The Report summarized the outcome of an investigation in connection with the following technological products: Apple iTunes Music and Video Store, Azureus (Bittorrent client), eReader, Disney video game (Pirates of the Caribbean), Intuit Quicktax (tax software), Microsoft Office, Napster, Ottawa Public Library, Universal Studios Ray (DVD), Sony BMG, Symantec Norton (antivirus software), Telus Mobility (wireless services), Ubisoft video game (Prince of Persia), Valve video game (Half Life 2), Warner Music Group music albums. Although the research was conducted on 2007, the technological mechanisms have not considerably differentiated over the course of the last decade. In scrutinizing the results, PIPEDA (Personal Information Protection and Electronic Documents Act) was the reference point, an instrument legislated in 2000, in consonance with the European principles of data protection. Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007)

²³⁴ Id. at 48

²³⁵ In comparison to Directive 95/46/EC.

²³⁶ Other policies that are considered to achieve an appropriate balance, include: (i) the anonymity principle (ii) individual access and (iii) DRM licenses.

See: Ian R. Kerr, "If Left to Their Own Devices...How DRM and Anticircumvention Laws Can Be Used to Hack Privacy," in Michael Geist, ed., In the Public Interest 167-210 (Irwin Press, 2005) 181

processing principles²³⁷, while an even more minimal number conformed to the proportionality tests²³⁸. In the context of the Regulation, these principles shall be construed according to guidelines procured by authorities (e.g. Article 29 Working Party, now European Data Protection Board²³⁹), to ensure legal certainty. In the *transparency* principle, to cite an instance, the plain language has been interpreted as essential when defining purposes²⁴⁰. “Concise, transparent, intelligible, easily accessible and free of charge”²⁴¹ constitute critical components as well.

Under the definition of *data minimization* principle, the heart of data-processing rules lies. Personal data shall be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.²⁴² The *minimum possible* calculates the function between *purpose* and *processing*. Application developers, as an example, should conform, utilizing aggregated data, instead of raw data when

²³⁷ Sub-section 5(3) of PIPEDA, touching privacy and data collection issues, was employed in the Report to compose a relevant questionnaire, comprising topics such as: (i) Does the organization *identify* the purpose for which it collects personal information, and if so does it do so on or before collection? (ii) Has the organization made a “reasonable effort” to ensure that the individual is *advised* of the purposes for which the information will be used? (iii) Does the organization require “express” consent to its collection, use or disclosure of personal information? (iv) Is the collection of personal information *limited* (in both type and amount) to that which is necessary for the purposes identified by the organization? (v) Does the organization collect personal information by fair and lawful means? (vi) Does the organization specify the type of information it collects? (vii) Does the organization use or disclose personal information for purposes other than those for which it was collected? (viii) Does the organization have a “readily available” privacy policy? (ix) Is the organization’s privacy policy “generally understandable”? (x) Has the organization established procedures to receive and respond to complaints and inquiries? (xi) Has the organization provided a specific account of third parties to which it has (or may have) disclosed personal information about an individual?

See: Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 30-31

²³⁸ In case *Eastmond v. Canadian Pacific Railway*, FC 852 (2004), the Federal Court laid out a test for assessing sub-section 5(3) of PIPEDA: (a) Is the measure necessary to meet a specific need? (b) Is the measure likely to be effective in meeting that need? (c) Is the loss of privacy proportional to the benefit gained? (d) Is there a less privacy invasive way of achieving the same end?

Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 33

²³⁹ European Data Protection Board, available at <https://edpb.europa.eu/> accessed 10 August 2018

²⁴⁰ Insufficiency in wording has been identified in the following phrases: “We may use your personal data for research purposes”, “We may use your personal data to offer personalized services”, “We may use your personal data to develop new services”.

“Data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue.”

Article 29 Data Protection Working Party, 17/EN WP260, “Guidelines on transparency under Regulation 2016/679”, 9, available at https://iapp.org/media/pdf/resource_center/wp29-transparency-12-12-17.pdf accessed 10 August 2018

²⁴¹ Id. at 7

²⁴² Article 5(1)(c) GDPR

possible²⁴³. In gauging compliance, the proportionality is measured i.e. the legitimacy of the aim, the adequacy, the necessity, as well as how reasonable it is, in connection with different interests at stake (*stricto sensu*)²⁴⁴. DRM operators' policy scarcely corresponds because unjustified datasets were revealed to be generated²⁴⁵. Particularly, a misconception of what constitutes personal data or anonymized data, in reference to the IP address, let DRM policies amass disproportionate quantities of data concerning name, address, email, telephone, credit cards and demographic data, without informing the data subject²⁴⁶. Privacy enhancing technologies (PET) and Privacy by Design are inextricably correlated with data minimization²⁴⁷.

In the former Canadian survey, a network was configured in the technical investigation to ensure non-flaw of personal data to unauthorized third parties. Unfortunately, the results were rather displeasing, as *repurposing* of personal data turned up to be the rule²⁴⁸. Personal data was found to be communicated towards third parties (mostly advertisement sites), in such a manner that circumvented the *purpose limitation* principle. In the spirit of a teleological perspective, personal data shall be obtained "for specified, explicit and legitimate purposes and *not further* processed in a manner that is incompatible with those purposes"²⁴⁹. Yet, in absence of sufficient Internet literacy, both DRM systems administrators and consumers often consider personal data as disposable property, the first side exploiting end users for commercial purposes, the second ones neglecting the precariousness and fragility of digital identities.

²⁴³ Article 29 Data Protection Working Party, 14/EN WP 223, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 23, available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf accessed 11 August 2018

²⁴⁴ Juan Cianciardo, The Principle of Proportionality: The Challenges of Human Rights, 3 J. Civ. L. Stud. (2010) 179, available at: <http://digitalcommons.law.lsu.edu/jcls/vol3/iss1/11> accessed 11 August 2018

²⁴⁵ Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 49

²⁴⁶ *Id.* at 50

²⁴⁷ Privacy Enhancing Technologies – A Review of Tools and Techniques, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada (November 2017) available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#heading-0-0-5 accessed 11 August 2018

²⁴⁸ None of the 12 corporations examined would reconcile with the purpose limitation principle. Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 53

²⁴⁹ Article 5(1)(b) GDPR

Auspiciously, in improving enforceability and attentiveness²⁵⁰, a provision dedicated to compatibility assessment was inserted in the Regulation.²⁵¹

Provisions regarding *profiling*²⁵² and *automated decision-making*²⁵³ may gain importance in respect to contemporary personal data processing tools. Their philosophy is uttered by Art. 29 WP, in warning that these technologies could pose “*significant risks for individuals’ rights and freedoms*” and can “*perpetuate existing stereotypes and social segregation*” absent appropriate safeguards²⁵⁴. In article 22 GDPR, the right to object to fully automated individual decision-making, is manifestly conferred to data subjects.²⁵⁵ Especially whenever sensitive personal data are examined, stricter conditions apply, within the purview of article 22(4) and Recital 71 GDPR. Furthermore, along with the general right to object, that arrangement ultimately forces DRM administrators, as data controllers, to cease processing in case of direct marketing purposes, whenever data subjects oppose²⁵⁶. By virtue of data monetization projects, capitalizing on profile creation offers considerable incentives to investors,²⁵⁷ except that, on the other hand, end-users’ capability to henceforth disallow profiling, drastically overturns DRM operators’ strategies.

Finally, processing personal data must be in harmony with the secondary principles, albeit equally relevant to DRM systems. In order for them not to fall short and end up

²⁵⁰ Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, “The Principle of Purpose Limitation and Big Data”, Springer Nature Singapore Pte Ltd. (2017) 35

²⁵¹ Article 6(4) GDPR

²⁵² Article 4(4) specifies profiling as: “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements”.

²⁵³ Automated decision-making is defined as “the ability to make decisions by technological means without human involvement”.

Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (6 February 2018) 8, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 11 August 2018

²⁵⁴ Id. at 5

²⁵⁵ Article 22(1) GDPR affirms that in principle: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

²⁵⁶ The right to object is effectually perceived in a direct marketing shell, as per article 21(2) GDPR: “Where personal data are processed for *direct marketing purposes*, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.”

²⁵⁷ PricewaterhouseCoopers Legal LLP (London), “Profiling” available at <https://www.pwc.lu/en/general-data-protection/docs/pwc-gdpr-profiling.pdf> accessed 12 August 2018

in a corrupted mishandling outline, any personal data acquired, and which permits identification, must be retained in agreement with the *storage limitation* principle²⁵⁸. Hence, in privacy policies proportionate time limits should be declared²⁵⁹. Additionally, by continuing to assure the *accuracy* of personal data²⁶⁰, the legislator enhances the qualitative aspect. To consider the challenges and prevent misleading incidences, in DRM systems, data controllers must warrant accurate information and corresponding updates. On a final note, a security provision translated into the *integrity and confidentiality* principle prescribes technical measures²⁶¹ which afford refined certainty of personal data, while DRM systems implementers, supposing they breach any of the preceding rules, are held liable under the *accountability* principle²⁶². The responsibility of data controllers presents one positive-active feature (demonstration of compliance) and one negative-passive (responsibility for compliance).

4.6 Critical evaluation of surveillance DRM systems

As explained in previous chapters, precautionary steps were taken to attain copyright enforcement, by implementing and embedding constraining mechanisms into digital content. Developments in computing gradually led to a more sophisticated engineering process, a fact which rapidly culminated in DRM-watchdogs. Two of their central features involve surveillance acts and the “*ability to unbundle copyrights into discrete*

²⁵⁸ Article 5(1)(e) GDPR

²⁵⁹ Principles of the GDPR, “For how long can data be kept and is it necessary to update it?” available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en accessed 13 August 2018

²⁶⁰ Information Commissioner’s Office (UK), Principle (d): Accuracy, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/> accessed 18 August 2018

²⁶¹ The security principle, as a cornerstone to the Regulation, governs a considerable assortment of provisions (article 32 et seq.). Implementation of appropriate organizational and technical measures, risk policies and analysis, should be conducted in line with the state of the art and related costs. Under an empirical investigation, frequent measures are explicated in: Cision “Technical and Organizational Measures” available at <https://gdpr.cision.com/technicalorgmeasures> accessed 18 August 2018

²⁶² Article 5(2) GDPR: “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (the other data protection principles).”

and custom-made products”^{263,264}. The basal rationale of their use is now shifted from piracy combatting to privacy obstructing.

Despite the fact that a gamut of DRM systems’ aims, functions and operations has been identified, the most contentious illustration is depicted in DRM mechanisms which continually oversee end users²⁶⁵. In opining about the economics of privacy myopia, Froomkin stated that “consumers are in a poor legal position to complain about the sale of data concerning themselves” and “against privacy-destroying technologies”²⁶⁶. Indeed, the extent to which other categories comply with data protection and proportionality principles has not been a subject of ongoing dispute, since their legitimacy is based on sound grounds. Be it systems which limit interoperability, or establish copy-control, or identify persons via credentials, or manage end-user access to copyrighted material, their legitimacy is honestly upheld. Consequently, given that other classes of DRM platforms present less concerns for consumers, an observational evaluation should be conducted mainly for surveilling DRM structures.

The technological measures’ generic layout gravely collides with data protection rules, as a direct aftermath of the digital copyright against privacy current clash. To date, DRM systems in reference to the European market were loosely affected by the Directive, rendering the upgrade to Regulation an essential movement. Without prejudice to the DRM future design, up to this point, the *Fair Information Principles*²⁶⁷ set by OECD, which were encoded into law, only barely served as baseline. Although

²⁶³ Ian Kerr and Jane Bailey, The Implications of Digital Rights Management for Privacy and Freedom of Expression, Faculty of Law, University of Ottawa, Ontario, Canada, Info, Comm & Ethics in Society (2004) 88

²⁶⁴ The smaller the information pieces protected, the more comprehensive they become. Victor Mayer-Schonberger, “Beyond copyright: managing information rights with DRM” in Denver University Law Review, September (2006) 194

²⁶⁵ DRM technologies that monitor user behavior create records of intellectual consumption... records of intellectual exploration...records of behavior. Julie E. Cohen, DRM and Privacy, Georgetown Law Faculty Publications and Other Works, Berkeley Technology Law Journal. Vol. 18. (2003) 578, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed 18 August 2018

²⁶⁶ Froomkin, A. Michael, The Death of Privacy? 52 Stan. L. Rev. 1461 (2000) 1501 available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715617 accessed 18 August 2018

²⁶⁷ Mostly general goals, these principles include: collection limitation, data accuracy, purpose disclosure, use limits, security, openness, participation, and organizational accountability.

GDPR should be employed as the assessment tool for the present thesis, most DRM systems do not even comply with what the Directive dictates²⁶⁸.

Overall, multifaceted flows exist. Laboriously extracted information about DRM operators, and secrecy in their activities related to personal data, suggest a malfunctioning data protection approach. Repeatedly, surveys have revealed that personal data were open-endedly and indiscriminately collected, not adequately specified, there were enigmatic tracking behaviors, no opt-outs, no correspondence between privacy policies and reality, avoidance to respond to customers' inquiries, undisclosed communications, unrevealed purposes, and misstating of personal data²⁶⁹. As inferred above, such tactics do not conform in the least with data minimization, purpose limitation or transparency guidelines. GDPR, sets a framework where all these tricks will end, insomuch as *specifications* on provisions concerning data subjects' rights are instituted (e.g. to rectify data, to object to profiling/automated processing, to erase personal data, to restrict processing, to access to their own data). Put differently, in a hypothetical comparable present-day survey, the answers would prove fairly sincere and data controllers quite compliant and obedient²⁷⁰.

Unjustifiable actuality in data processing poses the repurposing²⁷¹ "game plan" that DRM data controllers have employed routinely. Standardly, users type their contact

²⁶⁸ A concession seems obligatory at this point: The Regulation has marginally been applicable, since 25 May 2018. This thesis examines DRM systems designed, programmed and manufactured long before, in an era when the Directive 95/46/EC split its coercive character into the European Member States' jurisdictions. Outcome of this instance is the perplexed transitional phase in between which the majority of these technologies are stuck. Precisely, GDPR has introduced various legal innovations, as mentioned, applying impact assessments, ridiculously astronomical fines and pragmatic compliance formalities apart from substantive law provisions. To be commercialized two decades ago means that DRM systems, although guidelines and laws existed, technology limits would not permit them to be designed in an effective pro-privacy manner, rather in a rudimentarily practical way. Thus, their assessment ought to be carried out both instructively and critically.

²⁶⁹ Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. The Canadian Internet Policy and Public Interest Clinic (2007) 65-67

²⁷⁰ Data breaches nowadays are unequally treated in comparison to the past, by the Directive. Not only exorbitant administrative fines are menacing, but also extension of liability to all responsible parties and for a considerable number of multiple data breaches (each data breach is counted separately) would amass huge sums to be paid as sanctions.

Paul Voigt, Axel von dem Bussche, "The EU General Data Protection Regulation (GDPR), A Practical Guide" Springer International Publishing (2017) 212

²⁷¹ Between "reuse" and "repurpose" in data governance, there is a prodigious gap: while data reuse signifies that a dataset has been exploited twice or more (reuse customer lists for a second market campaign), data repurpose is translated into classifying the same customers in accordance with other data (combining customers details with their sales transactions and their volume).

details or preferences in DRM platforms so as to gain access, under the excuse to be authorized to access copyright-sheltered content. Regardless of how personal data are extracted, once alienated by the data subject, they were fully marketable, without opposite, collective resistance on behalf of the consumers.

Addressing data minimization, storage limitation and accuracy principles, unquestionably the majority of DRM platforms misperform in these fields. Regrettably, to enforce the minimization of generation of personal data resembles a feat in ubiquitous computing environment, or a meaningless hope²⁷². Nevertheless, if digital rights management as a concept is to be considered authorized, legal deference is the least that must be demonstrated before these principles. *On the verge of unlawfulness*, it is either comply, or permanently abort the mission. By the fresh Regulation, a period of grace had been granted for all European or Europe-targeting data processing actors (extraterritorial applicability²⁷³); accordingly, thenceforth, in the short-term future what remains to emerge are well-planned and calibrated DRM systems dictated under Privacy by Design principle's command, which will be described underneath.

Undeniably, from a legal perspective, it is a matter of time (and sanctions) until most DRM structures alter their modus operandi. Be that as it may, is such balance viable from a social standpoint? Are anti-DRM advocacy campaigns' arguments²⁷⁴ well substantiated, towards an eradication of DRM systems? Both content industries and end users display decent justifications on their opinion. The evolutionary pattern of DRM architecture initiated merely in favor of copyright protection, and moving forward, privacy intrusion was a spillover, probably an unintentional side-effect. Industries acknowledge such issues, yet to flow against the stream of their interests seems impossible, provided that they are all intertwined businesses. What could be socially acceptable, are solely DRM systems which are strictly patterned after copy-control or

The Practitioner's Guide to Data Quality Improvement "Data Governance and Quality: Data Reuse vs. Data Repurposing" (February 2012) available at <http://dataqualitybook.com/?p=349> accessed 20 August 2018

²⁷² Serge Gutwirth, Yves Poullet, Paul de Hert, Ronald Leenes, "Computers, Privacy and Data Protection: An Element of Choice" Springer Netherlands (2011) 164

²⁷⁰ SLAUGHTER AND MAY, "New rules, wider reach: the extraterritorial scope of the GDPR" (June 2016) 3 available at <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf> accessed 20 August 2018

²⁷⁴ Rebecca Wexler, The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates, 17 Yale J.L. & Tech. 368 (2015) 378 and Electronic Frontier Foundation "Cory Doctorow Rejoins EFF to Eradicate DRM Everywhere" available at <https://www.eff.org/press/releases/cory-doctorow-rejoins-eff-eradicate-drm-everywhere> accessed 21 August 2018

access-control edifice. Consumers' personal identification *disproportionately* surpasses intellectual property rights preservation.

Other than elusive, legal, data processing dilemmas, which are to be scrutinized in particularized DRM models, one more widespread societal predicament arises. That of "Mass Surveillance", which nowadays has become a buzzword along with Big Data, Artificial Intelligence, Internet of Things and Blockchain. By their common denominator, one perceives them as bleeding edge technologies, namely, posing high risks and (social) costs. Following the premeditated plan, for DRM technologies not many choices were offered. As stated in the beginning, the paradigm shift this time involves the propertization of information privacy²⁷⁵.

Propertization of personal data is substantially reproved by individuals and collective organizations. By being commodified, informational privacy is conceived as a valuable trading asset not for consumers, but for markets²⁷⁶, upon where individuals are enabled to decide whether and to what extent their privacy interests are traded away²⁷⁷. Besides, privacy is inseparably affiliated with consumer considerations²⁷⁸. Societal implications like gender discrimination²⁷⁹ originate frequently from personal data management by third parties, an issue that must be tackled, in view of dignity and autonomy being damaged inconsiderately. Hence criticisms surveyed on the legal terrain are identically applied through the lens of society.

Without ignorance to legislators' talent to *normalize* social conduct and acceptance, morality debates obfuscate the discussion even more. For the shake of copyright

²⁷⁵ Victor Mayer Schonberger, "Beyond copyright: managing information rights with DRM" in *Denver University Law Review*, September 2006, 195

²⁷⁶ *Id.* at 195

²⁷⁷ Andrew Orlowski, "Lessig, Stallman on 'Open Source' DRM Best of all possible shaftings?" (April 2006) available at https://www.theregister.co.uk/2006/04/15/lessig_stallman_drm/ accessed 21 August 2018

²⁷⁸ DRM: Copy Protection vs. Consumer Frustration (Event summary, keynote speaker Richard Gooch, International Federation of the Phonographic Industry) available at <https://www.musicbank.co.uk/product/drm-copy-protection-vs-consumer-frustration-transcript/> accessed 21 August 2018

²⁷⁹ As an example, women-oriented sites tend to employ gimmicks to attract customers, who sometimes "unmindfully, docilely and passively share information and allow corporate entities to monitor their online efforts to educate and inform themselves" and at the same time "electronic entities then attempt to exploit this sharing and networking for commercial gain" See: Bartow Ann, "Our Data, Ourselves: Privacy, Propertization, and Gender". *University of San Francisco Law Review*, Vol. 34, p. 633, (Summer 2000) 2, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=374101 accessed 21 August 2018

interests, dataveillance²⁸⁰ should not be entirely justified. “*Dataveillance in the present moment is not simply descriptive (monitoring) but also predictive (conjecture) and prescriptive (enactment)*”²⁸¹. Towards the *objectification* of the *so-called data subjects*²⁸², DRM have so negatively contributed, if not being the leaders.

However, a qualitative evaluation is accomplished only after both parties’ claims are reviewed. As unexpected as it may seem, pro-DRM claims²⁸³ do not exclusively concern copyright protection, but additionally assist in end-users’ privacy-status amelioration. The foregoing hypothesis is well-supported by a mixture of arguments. From a privacy-as-property standpoint, to accord personal data to a digital rights management mechanism, simultaneously this act entails exclusivity for consumers, and communicative privacy for copyright holders²⁸⁴, who may select their audience. Furthermore, regarding spatial privacy, via an ex-ante intellectual consumption control, DRM systems operate as legal expansions²⁸⁵, rendering any additional law enforcement redundant. Thanks to DRM coordinated structures, also contextual privacy is safeguarded, since their mere existence successfully reduces data leakage and mitigate undesirable data disclosure, via measures as Privacy Rights Management (PRM) platforms²⁸⁶. Even more, intermediary software contributes to favorable data anonymization, and in a substantive way, decisional autonomy and cognitive integrity are secured, as akin facets to copyright protection, and ultimately rights of personality. Lastly, pro-DRM claims iterate a material interest, arguing that the more DRM systems

²⁸⁰ Dataveillance is called the increasingly preferred way of systematically monitoring citizens through social media and online communication technologies and of continuous surveillance through the use of (meta)data.

José van Dijk, “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology” *Surveillance & Society* 12(2): 197-208 (2014) available at <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication> accessed 22 August 2018

²⁸¹ Lisa Gitelman, “Raw Data” Is an Oxymoron, *The MIT Press Cambridge, Massachusetts London, England, Massachusetts Institute of Technology* (2013) 124

²⁸² See: Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*. Georgetown Public Law Research Paper No. 233597, (2000), available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=233597 accessed 22 August 2018

²⁸³ In the case *United States v. Reichart*, 747 F.3d 445, 456 (6th Cir. 2014) one dissenting judge characterized DRM systems as privacy enhancing.

²⁸⁴ Rebecca Wexler, *The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates*, 17 *Yale J.L. & Tech.* 368 (2015) 386

²⁸⁵ *Id.* at 387

²⁸⁶ Kang, Jerry and Shilton, Katie and Estrin, Deborah and Burke, Jeff and Hansen, Mark, *Self-Surveillance Privacy* (December 21, 2010). *UCLA School of Law Research Paper No. 11-01, Iowa Law Review*, Vol. 97, p. 809, (2012) 844, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729332 accessed at 22 August 2018

are strengthened, the more data protection, as a notion, is rooted, in a sense that as the time goes by, anti-circumvention laws do *sanitize* DRM technologies by ostracizing the malfunctioning ones²⁸⁷.

To sum this paragraph up, it is evident that DRM systems were reviewed one-sidedly, since the scope of this thesis is not extended into consumer behavioral economics. End users are surely the ones victimized, still, in part, they should not be exempted of any ignorance and responsibility to share their data unconcernedly. Definitely, leeway for eventual improvements is reserved.

²⁸⁷ In "Protecting Personal Privacy Interests" chapter, an alternative rationale is expressed about anti-circumvention measures: "In fact, enactment of section 1201 should have a positive impact on the protection of personal privacy on the Internet. The *same* technologies that copyright owners use to control access to and use of their works can and will be used to protect the personal privacy...by outlawing the activities of those who make it their business to provide the tools for circumventing these protective technologies, this legislation will substantially enhance the degree to which individuals may protect their privacy as they work, play and communicate on the Internet."

S. Rept. 105-190 - The Digital Millennium Copyright Act Of 1998, 18 available at <https://www.congress.gov/105/crpt/srpt190/CRPT-105srpt190.pdf> accessed 22 August 2018

Chapter V

5. Alternative suggestions

Counterbalancing contradictory and irreconcilable interests amounts to one ambitious vision, that recent legislation brought one step closer. To accommodate both parties in this bet, scholarship and legal instruments have proposed a non-negligible number of recommendations, best practices and future developments, which will be discussed in the present chapter.

5.1 Nascent insights in practice

To deny that conscious deployment of technology²⁸⁸ does not covertly adjust people's behavior is an oversimplified approach. Legal certainty, if not *clarity*, are material components in an attempt to regulate efficiently, during an age where a whole new set of questions has opened. Notwithstanding the natural rigidity of technology-embedding rules, legal norms are characterized by flexibility and reasonableness, so as to incorporate technology progress, but in this interdisciplinary study of technology, science and society, value tradeoffs^{289,290} are a given.

Privacy-Enhancing Technologies (PET) were firstly implemented circa 1990 for consumer protection, and since then donated enough to the theoretical and practical repertoire of privacy protection substitutes. They are defined as “*a system of ICT that measures the protection of informational privacy by eliminating or minimizing personal*

²⁸⁸ Bert-Jaap Koops, The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding (November 1, 2011). *Legisprudence*, Vol. 5, No. 2, pp. 171-194, (2011) 3, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1953967 accessed 25 August 2018

²⁸⁹ Julie E. Cohen, DRM and Privacy, *Georgetown Law Faculty Publications and Other Works*, Berkeley Technology Law Journal. Vol. 18. (2003) 587, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed 25 August 2018

²⁹⁰ In reference to Privacy Economics, in public-opinion polls conducted among Americans, the conclusions drawn calculate that: the cost of selecting is not worth the offered benefits, that 69% of the respondents totally ignore how personal data flow in companies, and principally that whenever tangible benefits are involved, they deem privacy of lesser importance.

Yun Shen, Siani Pearson, “Privacy Enhancing Technologies: A Review” HP Laboratories HPL-2011-113 (2011) 17, available at <http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf> accessed 25 August 2018

data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system”²⁹¹. To aid DRM systems in ensuring privacy²⁹², these technologies envelop encryption, metadata schemes, application programming, system development governance, user interface, anonymous credentials²⁹³, identity management and architecture²⁹⁴. Informed consent, technical enforcement, remote audit, terms and conditions negotiation, policy checking, purpose-binding, data tracking, anonymization and pseudonymization paradigms, are all equally included in privacy enhancing packages. Unlike Directives on data protection and electronic communications²⁹⁵, the standing harmonizing Regulation dedicates directly article 25 on designing consumer-friendly and pro-privacy DRM systems.

Specifically, anonymity²⁹⁶, which is the less painfully discernible PET, is attained “*by unlinking the identity of the person from the traces that his/her digital activities leave behind in information systems*”²⁹⁷. When incorporated into DRM architecture, third observers are unable to identify subjects with certitude, unless multiple transactions are inspected, which however only probabilistic information will secure. Pseudonymity, as a replacement, is achieved by pseudonymization²⁹⁸, and is firmly encouraged by recitals 26, 28, 29 and 78 GDPR. Both maneuvers’ objective remains the concealment of personally identifiable information.

²⁹¹ G.W. van Blarckom, J.J. Borking, J.G.E. Olk, “Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents” The Hague (2003) 33

²⁹² As an example, for statistical purposes, personal data pertaining to birth date, full postal code and exact profession could be transformed in age category, residence region and industrial area respectively, enabling individuals to stay non-identifiable.

²⁹³ For instance, “*Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control (ReCRED)*” is an anonymous credentials EU project, leaded by Greece, to “promote the user’s personal mobile device to the role of a unified authentication and authorization proxy towards the digital world”, available at <https://www.recred.eu/> accessed 25 August 2018

²⁹⁴ Steve Kenny, “An Introduction to Privacy Enhancing Technologies” (May 2008) available at <https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/> accessed 25 August 2018

²⁹⁵ Limited direct command existed for privacy enhancing strategies, apart from the more general art. 17 and recital 46 in Directive 95/46/EC and art. 6 and recital 30 in Directive 2002/58/EC.

²⁹⁶ Not to be confused with anonymization. Anonymity describes the state or quality of being anonymous and is a precedent, whereas anonymization entails an information sanitization process which guarantees privacy.

²⁹⁷ Serge Gutwirth, Yves Poulet, Paul De Hert, “Data Protection in a Profiled World”, Springer Netherlands (1st edition 2010) 305

²⁹⁸ Article 4(5) GDPR explains that: pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

In privacy, as a contextual phenomenon, two variables participate, the willingness to pay and the willingness to accept. In spite of consumers' preparedness and incentives to adopt anti-encroachment measures, unfortunately it is merely online industries that unilaterally decide which PET may pass from the marketplace funnel²⁹⁹. Hardly any consumer resistance has been realized thus far, and absent true pressure, there is lack of high-priced investments³⁰⁰. Furthermore, despite this three-decade awareness, only recently EU proceeded to a decisive step, by adopting guidelines on PET readiness analysis³⁰¹ along with the largely propitious GDPR, so as to salvage any doomed to failure PET.

Mechanisms managing digital rights were, in their majority, designed before robust data protection regulatory interventions, such as today's Regulation. In addressing workable solutions regarding privacy concerns, it would be prudent to examine the privacy acquis up to now. Of conspicuous relevance is the harmonizing effect in the administrative sanctions sector. Discretion power of distinct supervisory authorities came to be centrally governed by the ubiquitously enforceable article 83 GDPR³⁰². Similarly, remedies are provided for in a determined context rather than in decentralized legislative instruments. Taking into consideration, additionally, the extraterritorial scope of the Regulation, (even non-EU) DRM implementers could not afford to neglect this *standardizing* austerity, in a sense that no DRM shall be masterminded the same anymore. On a final note, legal action is identified as the last resort for developers³⁰³,

²⁹⁹ Privacy enhancing technologies are summarized in two categories, the *substitute* PET and *complementary* PET. Within the scope of the first one fall technologies which steeply neutralize information leakage (avoidance of identification at all costs). In the second category, personal data are ineluctably extracted but technologies aid in its minimization.

See: Anna Romanou "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise" Computer Law and Security Review 34, 99-110 (2018) 102

³⁰⁰ Serge Gutwirth, Yves Poullet, Paul de Hert, Ronald Leenes, "Computers, Privacy and Data Protection: An Element of Choice" Springer Netherlands (2011) 338

³⁰¹ European Union Agency for Network and Information Security, "Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan", Approved Version 1.0 Public December 2015, available at <https://www.enisa.europa.eu/publications/pets> accessed 26 August 2018

³⁰² In contrast to the tremendously unadorned article 24 of the Directive 95/46/EC which voices the obligation of Member States "...to adopt suitable measures to ensure the full implementation of the provisions of this Directive....and lay down the sanctions to be imposed in case of infringement...", the Regulation devotes one and a half pages in specifying the conditions for imposing administrative fines.

³⁰³ Marcella Favale, Neil McDonald, Christos Gatzidis, "Human Aspects in Digital Rights Management: The Perspective of Content Developers", 13 SCRIPTed 289 (2016) 303

due to cost/benefit reflections, therefore, in case of non-professional infringements, human and cultural elements should be prioritized.

In an alternative pragmatic scenario where end users are independently involved, for someone to bypass a software which impinges on informational privacy constitutes a legitimate and benign act. Pursuant to the aforementioned article 6(3) of the Information Society Directive, to circumvent deceitful programs is permissible, albeit unworkable due to the fact that they are reserved mainly for experienced users. Concurrently, overseas, in Section 1201 of the DMCA³⁰⁴, which influences and governs most DRM systems worldwide, “*it is not a violation for a person to circumvent a technological measure that effectively controls access to a work protected*” when the latter targets personally identifying information, provided that some conditions fulfill³⁰⁵, and the doctrine of fair use is mirrored.

Ultimately, it is notable that DRM technologies, have shaped intellectual consumption markets in a style that copyright enforcement, has shifted from an ex-post to an ex-ante paradigm³⁰⁶. In other words, not that many sanctions are imposed afterwards, as many vouchers are purchased in advance to gain access to content, enabling the ascent of a “*pay-per-use society*”³⁰⁷. Parallely, the very structure of systems which practically replace digital copyright law, ought to be fittingly scrutinized through a license

³⁰⁴ The Digital Millennium Copyright Act is a United States law, enacted in 1998 aiming to incorporate the two 1996 WIPO copyright treaties, available at <https://www.copyright.gov/legislation/pl105-304.pdf> accessed 26 August 2018

³⁰⁵ Section 1201(i) stipulates the four conditions under which a DRM system could be lawfully circumvented: (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating *personally identifying information* reflecting the online activities of a natural person who seeks to gain access to the work protected; (B) in the normal course of its operation, the technological measure, or the work it protects, *collects or disseminates* personally identifying information about the person who seeks to gain access to the work protected, *without providing conspicuous notice* of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination; (C) the act of circumvention has the *sole effect of identifying* and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and (D) the act of circumvention is carried out *solely for the purpose of preventing* the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

³⁰⁶ Nicolo Zignales, “Digital Copyright, fair access and the problem of DRM misuse” Boston College Intellectual Property & Technology Forum (2012) 6

³⁰⁷ John R. Therien “Exorcising the Specter of a Pay-Per-Use Society: Toward Preserving Fair Use and the Public Domain in the Digital Age” Berkeley Technology Law Journal, Volume 16 Issue 4 Supplement Article 5 (2001) 984

procedure, so that the wide privacy engineering principles are reassured to be implemented a priori.

5.2 Privacy by design

Not a novel concept albeit highly fascinating, “Data Protection by design and by default”, also known as “Privacy by Design”, by its integration into the Regulation is transformed from a guideline into a legally binding provision, an obligation, since it is upgraded³⁰⁸ from mere recitals into a solid article³⁰⁹. From 1990 on, technological innovations compelled actors in this multidisciplinary domain to adopt privacy engineering principles as a countermeasure to mass surveillance, with Dr. Ann Cavoukian³¹⁰ being a prominent proponent. Since then, national data protection authorities have substantially endorsed these principles.

Emphasis is added on two pertinent points that form a variation between PET and PbD. In spite of both promoting privacy, PET are implemented indirectly and are addressed to skilled users, whilst PbD applies ex-ante during the internal process and is delivered to end users via consolidated products, obviating further active steps from the consumer side.

In an epitomized version, implementers should consider seven radical aspects³¹¹ in building end-user interactive software: (a) the *proactive* not reactive; preventative not

³⁰⁸ According to settled ECJ case law, no binding legal force emanates from the preamble to Community acts and “cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording”.

Case C-345/13 Karen Millen Fashions Ltd v Dunnes Stores Ltd [19.6.2014] ECJ, recital 31

³⁰⁹ Article 25 GDPR in the first paragraph states: “Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller *shall*, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures....” while in the second : “The controller *shall* implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed...”

³¹⁰ Dr. Ann Cavoukian, former Information and Privacy Commissioner for the Canadian province of Ontario, where she served for 17 years, has spread the notion of Privacy by Design through titles such as “Privacy and Digital Rights Management (DRM): An Oxymoron?”

³¹¹ Ann Cavoukian, “Privacy by Design, the 7 Foundational Principles Implementation and Mapping of Fair Information Practices” Information and Privacy Commissioner of Ontario (2011) available at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf accessed 27 August 2018

remedial character of software, (b) privacy shall be ensured as the *default* setting to safeguard non-proficient users (c) privacy as embedded into *design*, IT systems shall be empowered by holistic creativity (d) full functionality, positive-sum, not zero-sum, aims to accommodate all stakeholders' legitimate interests, a functional win-win (e) end-to-end security, lifecycle protection, related to storage limitation (f) visibility and transparency, entailing accountability, openness and compliance (g) respect for user-centric elements, such as consent and access.

Current DRM systems adopters shall not stay apathetic, adhering to a stoic perception and maximizing their benefits. Privacy by default and by design shall be transposed into their context, advocating an empirical "*value-sensitive design*"³¹² without unnecessary trade-offs. In building these principles into code, the technological literature mandates that an appropriate Rights Management Language³¹³ shall henceforth supervise information asymmetry and moral hazard between entities³¹⁴. To illustrate, a milestone European document examining PbD has been issued on RFID³¹⁵, conducting privacy impact assessments³¹⁶.

When deploying smart technologies³¹⁷ (to which DRM software progressively adheres), targeting European citizens, data protection by design and by default must as parameters be synchronized with them. Due to DRM technologies' globalized features,

³¹² Julie E. Cohen, DRM and Privacy, Georgetown Law Faculty Publications and Other Works, Berkeley Technology Law Journal. Vol. 18. (2003) 587, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed at 27 August 2018

³¹³ Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems" (2001) 12

³¹⁴ Because "*the overall privacy in a system is as strong as the privacy offered by the weakest link*", and additionally for Privacy by Design to dodge accusations of drawing fuzzy lines, each declaratory line must be translated in engineering structures. Examples: To limit personal data collection, credit card security could work with public keys. Databases architecture is optimal when data are segmented and erased automatically after transactions. Anonymous credentials help in online car rentals to prove only that the candidate driver is above 23 and has a license; nothing more is necessary. Personal data collection must be accompanied with due notice and real choice, not plausible. In client-side data aggregation, disclosure of personal data is again redundant. Besides, data could be processed in an earlier stage and be delivered in aggregate form (e.g. before distributing royalties to artists).

³¹⁵ Radio-Frequency Identification refers to an automatic identification and data capture technology, which automatically identifies and tracks tags attached/embedded on inanimate objects, using electromagnetic fields.

³¹⁶ European Commission, Digital Single Market, law, 12 January 2011 "Privacy and Data Protection Impact Assessment Framework for RFID Applications" available at <https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications> accessed 28 August 2018

³¹⁷ Among other implications, Privacy by Design affects also e-health, biometrics, and video surveillance. Anna Romanou "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise" Computer Law and Security Review 34, 99-110 (2018) 104

data portability to third countries shall be ascertained, while at the same time analogous international standards³¹⁸ should resonate, too.

On the other hand, by an only 2018 enforceable provision no market structure could instantly transform. Although not in experimental stage, PbD doctrines hardly have thrust digital-content industries to invest in implementing academic articles' reflections and soft-law agreements. Simply because the relevant market is not exclusively one of privacy standards, but also one for DRM-protected content³¹⁹. Put differently, developers demand tangible incentives. To this end, legislative actions by the Regulation come to rebalance this irregularity, also in view of the technical non-expertise, from what an average user of information goods suffers. If deep DRM system embeddedness is what markets pursue, then profound internalized pro-privacy patterns shall also by default institute a setting for end users to be prospectively edified.

In conclusion, to what extend the philosophy of user empowerment will be launched, is a matter of public policy, since the nebulosity of how fundamental the right to privacy is, does not allow a single defined status³²⁰.

³¹⁸ International Conference of Data Protection and Privacy Commissioners, Madrid Resolution, "International Standards on the Protection of Personal Data and Privacy", (2009) available at http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madr_id_en.pdf accessed 28 August 2018

³¹⁹ Julie E. Cohen, DRM and Privacy, Georgetown Law Faculty Publications and Other Works, Berkeley Technology Law Journal. Vol. 18. (2003) 612, available at <https://scholarship.law.georgetown.edu/facpub/60/> accessed 28 August 2018

³²⁰ Perpetual relinquishment of personal data for utilitarian purposes should be interdicted the same way as human organs selling in Europe, if privacy intrusion affects that much human dignity and autonomy.

See: Serge Gutwirth, Yves Poullet, Paul De Hert, "Data Protection in a Profiled World", Springer Netherlands (1st edition 2010) 329

Chapter VI

6. Conclusion

Data-oriented communities may represent an uncertain direction towards which present societies are guided. What humanity had been summoned to actualize centuries ago was to enact rudimentary analogue legislation codes, and nowadays is challenged to do the same, in a slightly dissimilar milieu. Rights and duties are transferred into digital environments³²¹, and from a sociological standpoint, they then define real-life values and further arrange human demeanor. This is why *managing digital rights* (and duties) is of utmost significance.

Along the chapters of this thesis, numerous discoveries were touched. Initiating with a brief exposition of digitalization's key components, in the second chapter, it has been clarified that the conventional copyright mechanism could not survive anymore. Following the then currents, authors' works would disseminate via the web, soliciting a proportionally effective protection. Shortly, industries conjured and installed systems to safeguard digital content, *managing end users' digital rights*. The third chapter has been devoted in a summarized DRM overview, historical-background information about P2P with case-law assessment, and the edifice of a representative DRM model. Without reaching privacy issues yet, any relevant legal instruments establishing DRM have been identified, subsequently legitimizing their deployment into the markets.

The primal underlying concept of DRM installation has shifted from securing intellectual property rights. These technologies converted themselves into an ally to global surveillance economy, shifting the locus of their implementation, and meddling with consumers' privacy. To what extent constitutions authorize privacy-tampering operations, is adaptively reflected in data protection legislation. Particularly, the fourth chapter reviewed European legislation, comparing the *harmonizing* effect of the repealed Directive to the *standardizing* effect of the Regulation. According to literature's DRM systems grading, the taxonomy revealed various shades, and

³²¹ Code regulates behavior.

See: Lawrence Lessig, "Code version 2.0" (2006)

persistent monitoring architectures proved to *exceed the legitimacy boundaries*. In providing an answer to this chief question respecting DRM technology:

“Digital Rights Management technologies versus end-user privacy”

it should be said that *the findings echo negative response, since privacy threats outnumber licit considerations*. How DRM technologies function nowadays evidences that the right to privacy should prevail over the right to intellectual property protection, or at least sideline it. Besides, technology should vindicate private life as long as respect to human dignity is still an ideal. Lamentably, it is only a moment ago that European legislation drastically interfered, delivering a heavy-handed legislative piece, acting as a disciplinarian. Scarce enforcement till recently, attributed to feeble mass-market resistance, has benefited DRM actors, and has disrespected individual users. As an information controller, DRM systems have remained privacy-neutral, yet parties’ situated interests have persuaded regulators by using strategic rhetoric. Principles (and obligations) such as data minimization, purpose specification, storage limitation and transparency were regularly encroached, absent true enforcing tools.

A genuinely promising future in European data protection field is the Regulation’s objective. Towards an EU internal market, free movement of data could not be ignored. Moreover, moral and societal implications ought to be reconsidered, not to mention political pressure. Chapter five itemizes potential antidotes for this ill-conceived asymmetry. On the one hand, external assistance is furnished by privacy-enhancing technologies, applied subsequently and *a posteriori*. On the other hand, internal processes involve data protection by design and by default (privacy by design), a series of principles embedded in DRM architecture, utilized *a priori*.

The current legislation’s revision in data protection has been a momentous occasion. By dint of a modern approach, former false DRM planning could be re-regulated in practice, rectifying digital rights’ trajectory in cyberspace.

Bibliography

Case Law

- A&M Records, Inc. v Napster Inc. (2001)
- Eastmond v. Canadian Pacific Railway, FC 852 (2004)
- Karen Millen Fashions Ltd v Dunnes Stores Ltd Case C-345/13 (2014)
- Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005)
- Nintendo of Europe GmbH v. PC Box Srl, 9Net Sr C-355/12 (2014)
- Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984)
- United States v. Reichart, 747 F.3d 445, 456, 6th Cir. 2014)

Literature

- Article 19 (Human Rights Organization) “Privacy and Freedom of Expression in the Age of Artificial Intelligence” (April 2018)
- Bartow A, “Our Data, Ourselves: Privacy, Propertization, and Gender”. University of San Francisco Law Review, Vol. 34, p. 633, (2000)
- Becker, E., Buhse, W., Gunnewig, D., Rump, N.: “Digital Rights Management, Technological, Economic, Legal and Political Aspects”. Berlin: Springer-Verlag Berlin Heidelberg (2003)
- Boneh D. and others, “Functional Encryption: Definitions and Challenges” 6597 Lecture Notes in Computer Science (2011)
- Broumas A., “Code, Access to Knowledge and the Law: The Governance of Knowledge in the Digital Age”, 5 U. Ottawa L. & Tech. J. 221 (2008)
- Bulow J., “An Economic Theory of Planned Obsolescence the Quarterly Journal of Economics”, Volume 101, Issue 4, 1, Pages 729–749 (1986)
- Butland N. C.; Sullivan J. J., “Pirate Tales from the Deep [Web]: An Exploration of Online Copyright Infringement in the Digital Age”, 13 U. Mass. L. Rev. 50 (2018)

- Bygrave L. A., “Digital Rights Management and Privacy, Legal Aspects in the European Union” E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 418–446, 2003 (Springer-Verlag Berlin Heidelberg 2003)
- Bygrave L. A., “The Technologisation of Copyright: Implications for Privacy and Related Interests” Published in European Intellectual Property Review, vol. 24, no. 2, pp. 51–57 (2002)
- Cahya A., Prihandokoa, Litowa B., Ghodosi H., “DRM’s rights protection capability: a review”, The Proceeding of 2012 the First International Conference on Computational Science and Information Management, Volume 1 (2012)
- Chapman & Hall/CRC Computer and Information Science Series, “The practical handbook of Internet computing” (2005)
- Cianciardo J., “The Principle of Proportionality: The Challenges of Human Rights”, 3 J. Civ. L. Stud. (2010)
- Clark C., "The Answer to the Machine in the Machine" in P. Bernt Hugenholtz, ed., The future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium organized by the Royal Netherlands Academy of Sciences INAW) and the institute for Information Law 139-145 (Amsterdam 6-7 July 1995) (Kluwer Law International, 1996)
- Cohen J. E., “European Copyright Law – Even More Horizontal”, 32 IIC p. 532 (2001)
- Cohen J. E., “Privacy, Visibility, Transparency, and Exposure”, University of Chicago Law Review, Vol. 75, No. 1, Georgetown Public Law Research Paper No. 1012068 (2008)
- Cohen J. E., “What Privacy is for”, 126 HARV. L. REV. 1904, 1907 (2013)
- Cohen J.E., “Examined Lives: Informational Privacy and the Subject as Object”. Georgetown Public Law Research Paper No. 233597 (2000)
- Corrigan R., “Colmcille and the Battle of the Book: Technology, Law and Access in 6th Century Ireland”, OPEN U. 1-2 (2007)
- Curtis G. T., “Treatise on the Law of Copyright” 169 n.1 (Boston 1847)
- Danielsen, D. Boyle J., Shamans, Software, and Spleens: “Law and the Construction of the Information Society”, Cambridge, MA, Harvard University Press, 1996, ISBN

0674805224, 288 pp., \$43.00 (hb), \$18.50 (pb). Leiden Journal of International Law, 16(2), 399-416 (2003)

- De Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I., “The right to data portability in the GDPR: “Towards user-centric interoperability of digital services”, Computer Law & Security Review, Volume 34, Issue 2, Pages 193-203 (2018)
- Doctorow, C.: “Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future”. San Francisco: Tachyon Publications (2008)
- Drossos L., Tsolis D., Sioutas S., Papatheodorou T., “Digital Rights Management for e-Commerce systems” (Information Science Reference 2009, Hershey New York)
- Eckhardt J., Lundborg M. & Schlipp C., “Digital Rights Management (DRM) and the development of mobile content in Europe” Computer, Law & Security (2007)
- Eric Diehl, “Securing Digital Video, Techniques for DRM and Content Protection” (2012)
- Favale M., McDonald N. Gatzidis C., “Human Aspects in Digital Rights Management: The Perspective of Content Developers”, 13 SCRIPTed 289 (2016)
- Feigenbaum J., Michael J. Freedman, Tomas Sander, Adam Shostack, “Privacy Engineering for Digital Rights Management Systems” (2001)
- Froomkin, A. M., “The Death of Privacy?” 52 Stan. L. Rev. 1461 (2000)
- Forgó N., Hänold S. and Schütze B., “The Principle of Purpose Limitation and Big Data”, Springer Nature Singapore Pte Ltd. (2017)
- Gasser U. and Girsberger M., “Transposing the Copyright Directive: Legal Protection of Technological Measures in Eu-Member States - a Genie Stuck in the Bottle?” (November 2004 - Berkman Working Paper No. 2004-10)
- Gitelman L., “Raw Data” Is an Oxymoron, The MIT Press Cambridge, Massachusetts London, England, Massachusetts Institute of Technology (2013)
- Giuseppe Mazziotti “EU Digital Copyright Law and the End-User”, Springer-Verlag Berlin Heidelberg (2008)
- Glancy D. J. “The Invention of the Right to Privacy”, Santa Clara Law Santa Clara Law Digital Commons (1979)
- Gutwirth S., Pouillet Y., De Hert P., “Data Protection in a Profiled World”, Springer Netherlands (1st edition 2010)

- Gutwirth S., Pouillet Y., De Hert P., Leenes R., “Computers, Privacy and Data Protection: An Element of Choice” Springer Netherlands (2011)
- Hildebrandt M., Gaakeer J., “Human Law and Computer Law: Comparative Perspectives” (Springer Netherlands 2013)
- Hofman J.: Introducing Copyright, “A plain language guide to copyright in the 21st century”, Vancouver: Commonwealth of Learning. (2009)
- Humphrey W. S., “The Software Engineering Process: Definition and Scope, Software Engineering Notes” (1989)
- Iannella R., “Digital Rights Management (DRM) Architectures”, D-Lib Magazine Volume 7 Number 6 (2001)
- INDICARE, Helberger N. (ed.), “State-of-the-Art Report: Digital Rights Management and Consumer Acceptability. A Multidisciplinary Discussion of Consumer Concerns and Expectations” (INDICARE, 2004)
- John Kuehl, “Video Games and Intellectual Property: Similarities, Differences, and a New Approach to Protection”, 7 Cybaris Intell. Prop. L. Rev. 313 (2016)
- Jonathan Zittrain, “The Generative Internet” (119 Harvard Law Review 1974 Berkman Center Research Publication No 2006/1 University of Oxford Faculty of Law Legal Studies Research Paper Series Working Paper No 28/2006 June 2006)
- Kang J., Shilton K., Estrin D., Burke J., and Hansen M. “Self-Surveillance Privacy” (December 21, 2010). UCLA School of Law Research Paper No. 11-01, Iowa Law Review, Vol. 97, p. 809, (2012)
- Kerr I. R., “If Left to Their Own Devices...How DRM and Anticircumvention Laws Can Be Used to Hack Privacy” in Michael Geist, ed., In the Public Interest 167-210 (Irwin Press, 2005)
- Kerr I. R., Maurushat A. and Tacit C. S., “Technological Protection Measures: Part I Trends in Technical Protection Measures and Circumvention Technologies” (2003)
- Koops B. and Clayton N.B. and Tjerk T. and Škorvánek I. and Chokrevski T. and Galič M., “A Typology of Privacy” University of Pennsylvania Journal of International Law 38(2): 483-575, Tilburg Law School Research Paper No. 09/2016, 488, 566 (2017)
- Koops B., “The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding” (November 1, 2011). Legsprudence, Vol. 5, No. 2, pp. 171-194, (2011)

- Kuhn T., “The Structure of Scientific Revolutions” (1970 ed.)
- Lessig L., “Code version 2.0” (2006)
- Lessig L., “Free culture” (2004)
- Liu Q., Safavi-Naini R. and Sheppard N. P., “Digital Rights Management for Digital Distribution” 21 Research and Practice in Information Technology, (2003)
- Maxwell, Winston and Bourreau, Marc, “Technology Neutrality in Internet, Telecoms and Data Protection Regulation” (November 23, 2014). Computer and Telecommunications L. Rev. (2014)
- Mayer-Schonberger V., “Beyond Copyright: Managing Information Rights with DRM”, 84 Denv. U. L. Rev. 181 (2006)
- Millard A., “America on record” 37-64 (1995)
- Moore, Adam D., “Defining Privacy”, Journal of Social Philosophy, Vol. 39, No. 3, pp. 411-428 (2008)
- Morgan D., Kang J.W., Kang J.M., “Minable Data Warehouse”. In: Filipe J., Cordeiro J. (eds) International Conference on Enterprise Information Systems. ICEIS. Lecture Notes in Business Information Processing, vol 24. Springer, Berlin, Heidelberg (2009)
- Myska M., “The True Story of DRM” Masaryk University Journal of Law and Technology (2009)
- Nissenbaum H., “Privacy as Contextual Integrity”, 79 Wash. L. REV. 119, 137-38, 155 (2004)
- Nye, Jr. J.S., Owens, W.A., “America's Information Edge” // Foreign Affairs. Vol. 75. No. 2, March-April (1996)
- Oberholzer F. and Strumpf K. abstract of “The Effect of File Sharing on Record Sales, an Empirical Analysis” (UNC.edu, March 2004)
- Oleksandr Stovpets, “Social-Philosophic View of the Intellectual Property Institution: Contemporary Features, Main Problems & Development Prospects”, Cogito: Multidisciplinary Res. J. 49 (2017)
- Papakonstantinou V.: “Legal Issues for DRM: The Future”, in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, Digital Rights Management for e-Commerce systems (Information Science Reference 2009, Hershey New York)

- Parsons J, Oja J. D., “New perspectives on Computer Concepts 2012: Introductory. Computers”. Dengang Learning (2009)
- Perry Mark, “Rights Management Information in the Public Interest: The Future of Canadian Copyright Law”, Michael Geist (2005)
- Pesses E. "Patent and Contribution: Bringing the Quid Pro Quo Into ebay V. Mercexchange," Yale Journal of Law and Technology: Vol. 11: Iss. 1, Article 10 (2009)
- Petrick P. “Why DRM Should be Cause for Concern: An Economic and Legal Analysis of the Effect of Digital Technology on the Music Industry”, Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-09, (November 2004)
- Popescu B., Crispo B., Tanenbaum A. and Kamperman F., “A DRM Security Architecture for Home Networks” DRM (2004)
- Posner R. A., “The Right of Privacy” (Georgia Law Review Vol. 12, No. 3. 1978)
- Romanou A., “The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise” Computer Law and Security Review 34, 99-110 (2018)
- Ronchi M. A., Politecnico di Milano in Lambros Drossos, Dimitrios Tsolis, Spyros Sioutas, Theodore Papatheodorou, “Digital Rights Management for e-Commerce systems” (Information Science Reference 2009, Hershey New York)
- Rose N. and Sweeney M., “The Hargreaves Report” (2011) 22(7) Ent LR 201
- Royle A., “Pirates Ahoy: Copyright and Internet File-Sharing”, 1 N.E. L. Rev. 51 (2013)
- Schönning J., “The legitimacy of the InfoSoc Directive” Faculty of Law University of Lund, Master’s Programme in European Business Law (Creative Commons Attribution 2.5 Sweden License 2010)
- Solove D. J., “A Taxonomy of Privacy”, 154 U. PA. L REV. 477 (2006)
- Solum L. B. and Minn C., “The Layers Principle: Internet Architecture and the Law”, San Diego Public Law Research Paper No. 55 (2004)
- Strykowski P. and Scorpecci D. “Piracy of Digital Content”, OECD Publishing, Paris (2009)
- Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan “If Piracy Is the Problem, Is DRM the Answer?” (Springer-Verlag Berlin Heidelberg 2003)

- The Canadian Internet Policy and Public Interest Clinic “Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law”. (2007)
- Tikkinen-Piri C., & Rohunen A. & Markkula J., “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”. Computer Law & Security Review. The International Journal of technology Law and Practice (2017)
- Tyrväinen P., “Concepts and a Design for Fair Use and Privacy in DRM”, D-Lib Magazine February Volume 11 Number 2 (2005)
- Van Blarckom G.W., Borking J.J., J.G.E. Olk, “Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents” The Hague (2003)
- Van Dijck J., “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology” Surveillance & Society 12(2): 197-208 (2014)
- Voigt P., Axel von dem Bussche, “The EU General Data Protection Regulation (GDPR), A Practical Guide” Springer International Publishing (2017)
- Warren S. D. and. Brandeis L. D. “The Right to Privacy” Harvard Law Review Vol. 4, No. 5 pp. 193-220 (Dec. 15, 1890)
- Westin A., “Privacy and Freedom” (New York: Atheneum 1967)
- Wexler R., The Private Life of DRM: Lessons on Privacy from the Copyright Enforcement Debates, 17 Yale J.L. & Tech. 368 (2015)
- Zignales N., “Digital Copyright, fair access and the problem of DRM misuse” Boston College Intellectual Property & Technology Forum (2012)

Legislation and Official Documents

- Article 29 Data Protection Working Party, “Guidelines on consent under Regulation 2016/679” 17/EN WP259 rev.01 (April 2018)
- Article 29 Data Protection Working Party, “Opinion 03/2013 on purpose limitation”, 00569/13/EN WP 203
- Article 29 Data Protection Working Party, “Opinion 4/2007 on the concept of personal data” (2007)

- Article 29 Data Protection Working Party, “Opinion 8/2014 on the on Recent Developments on the Internet of Things” 14/EN WP 223 (2014)
- Article 29 Data Protection Working Party, “Guidelines on transparency under Regulation 2016/679”, 17/EN WP260 (2017)
- Article 29 Data Protection Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679” (6 February 2018)
- Berne Convention for the Protection of Literary and Artistic Works (as amended in Paris on September 28, 1979)
- Charter of Fundamental Rights of the European Union
- Commission of the European Communities, Green Paper. “Copyright and Related Rights in the Information Society”, Brussels, 19 July 1995, COM (95) 382 final 49
- Commission of the European Communities: “Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (15th October 1992) COM (92) 422 final – SYN 287
- Convention of the Council of Europe Nr. 108 for the protection of individuals with regard to automatic processing of personal data
- Digital Millennium Copyright Act
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, also known as the Information Society Directive or the InfoSoc Directive
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 On the Legal Protection of Computer Programs

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access
- Executive Office of the President of the United States, “Big Data and Differential Pricing” (February 2015)
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- S. Rept. 105-190 - The Digital Millennium Copyright Act Of 1998
- Universal Declaration of Human Rights
- WIPO Copyright Treaty
- WIPO Performances and Phonograms Treaty

Websites and Online sources

- Access to knowledge movement available at [https://en.wikipedia.org/wiki/Access to Knowledge movement](https://en.wikipedia.org/wiki/Access_to_Knowledge_movement) accessed 14 June 2018
- Amended Brief Amicus Curiae of Copyright Law Professors in Support of Reversal, Consortium of 18 Copyright Law Professors, available at <http://www-personal.umich.edu/~jdlitman/briefs/Amicus.pdf> accessed 22 June 2018
- Andrew Orłowski, “Lessig, Stallman on 'Open Source' DRM Best of all possible shaftings?” (April 2006) available at

- https://www.theregister.co.uk/2006/04/15/lessig_stallman_drm/ accessed 21 August 2018
- The 5 Vs of Big Data, Anil Jain, (17 September 2016) available at <https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/> accessed 8 July 2018
 - Apple DRM is illegal in Norway, says Ombudsman (24 Jan 2007) <https://www.outlaw.com/en/articles/2007/january/apple-drm-is-illegal-in-norway-says-ombudsman/>, accessed 15 June 2018
 - Brad Stone, “Amazon Erases Orwell Books from Kindle” (17 July 2009) available at <https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html> accessed 14 June 2018
 - Cision “Technical and Organizational Measures” available at <https://gdpr.cision.com/technicalorgmeasures> accessed 18 August 2018
 - Clickstream Analytics available at <https://searchcrm.techtarget.com/definition/clickstream-analysis> accessed 3 August 2018
 - Communication (25 April 2018) "Towards a common European data space" available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN> accessed 8 July 2018
 - Data Archiving for Modern Business Big Data Initiatives available at <http://hortonworks.com/wp-content/uploads/2014/02/Cisco-and-Hortonworks-Data-Archiving-.pdf> accessed 10 July 2018
 - Kyle Orland, “Denuvo’s DRM now being cracked within hours of release”, 19 October 2017, available at Ars technica, <https://arstechnica.com/gaming/2017/10/denuvos-drm-ins-now-being-cracked-within-hours-of-release> accessed 22 June 2018
 - The Rising Tide of Anti-DRM, “Disingenuous DRM Scoreboard”, August 07, 2007, available at <http://www.managingrights.com/2007/08/drm-scorecard.html> accessed 23 June 2018
 - Domestic streaming, International streaming and Domestic DVD, available at <https://www.reuters.com/finance/stocks/company-profile/NFLX.O> accessed 20 June 2018

- Don't call it DRM: what's Denuvo Anti-Tamper? 19 June 2014, available at <https://www.eurogamer.net/articles/2014-12-19-denuvo-anti-tamper-drm> accessed 22 June 2018
- Dr Frank Eickmeier “What does the ePrivacy Regulation mean for the online industry?” (14.02.2018) available at <https://www.eprivacy.eu/en/about-us/news-press/news-detail/article/what-does-the-eprivacy-regulation-mean-for-the-online-industry/> accessed 15 July 2018
- DRM: Copy Protection vs. Consumer Frustration (Event summary, keynote speaker Richard Gooch, International Federation of the Phonographic Industry) available at <https://www.musicbank.co.uk/product/drm-copy-protection-vs-consumer-frustration-transcript/> accessed 21 August 2018
- Dynamic list of cracked games <https://crackwatch.com/> accessed 22 June 2018
- Electronic Frontier Foundation “Cory Doctorow Rejoins EFF to Eradicate DRM Everywhere” available at <https://www.eff.org/press/releases/cory-doctorow-rejoins-eff-eradicate-drm-everywhere> accessed 21 August 2018
- Elements of the European data economy strategy (Digital Single Market, Policy, 25 April 2018) available at <https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy> accessed 8 July 2018
- European Commission, Digital Single Market, law, 12 January 2011 “Privacy and Data Protection Impact Assessment Framework for RFID Applications” available at <https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications> accessed 28 August 2018
- European Data Protection Board, available at: <https://edpb.europa.eu/> accessed 10 August 2018
- European Union Agency for Network and Information Security, “Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan”, Approved Version 1.0 Public, December 2015, available at <https://www.enisa.europa.eu/publications/pets> accessed 26 August 2018
- History.com Staff, “The first Sony Walkman goes on sale” (2009) available at <https://www.history.com/this-day-in-history/the-first-sony-walkman-goes-on-sale> accessed 12 June 2018

- Hulu available at <https://www.hulu.com/press/about/> accessed 20 June 2018
- Improving QoS With Big Data Analytics available at <https://tmt.knect365.com/telco-data-analytics-europe/improving-qos-with-big-data-analytics> accessed 8 July 2018
- Information Commissioner’s Office (UK), Principle (d): Accuracy, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/> accessed 18 August 2018
- Intellectual Property, Black’s Law Dictionary (10th ed. 2014) available at [http://www.chori.org/About CHORI/Downloadables/FAQs.pdf](http://www.chori.org/About_CHORI/Downloadables/FAQs.pdf) accessed 12 June 2018
- International Conference of Data Protection and Privacy Commissioners, Madrid Resolution, “International Standards on the Protection of Personal Data and Privacy”, (2009) available at http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf accessed 28 August 2018
- Intersoft Consulting services AG GDPR, available at <https://gdpr-info.eu/issues/consent/> accessed 3 August 2018
- IPEN - Internet Privacy Engineering Network available at https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en accessed 5 July 2018
- Metadata definition available at <https://www.merriam-webster.com/dictionary/metadata> accessed 5 July 2018
- Organization for Economic Cooperation and Development, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#part2> accessed 1 July 2018
- Peer to peer in Cambridge Dictionary <https://dictionary.cambridge.org/dictionary/english/peer-to-peer> accessed 23 June 2018
- PricewaterhouseCoopers Legal LLP (London), “Profiling” available at <https://www.pwc.lu/en/general-data-protection/docs/pwc-gdpr-profiling.pdf> accessed 12 August 2018
- Principles of the GDPR, “For how long can data be kept and is it necessary to update it?” available at <https://ec.europa.eu/info/law/law-topic/data->

- [protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en](#) accessed 13 August 2018
- Privacy Engineering Program, available at <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering>, accessed 5 July 2018
 - Privacy Enhancing Technologies – A Review of Tools and Techniques, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada (November 2017) available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#heading-0-0-5 accessed 11 August 2018
 - Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control (ReCRED) available at <https://www.recred.eu/> accessed 25 August 2018
 - Representation of WTO members available at https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm#collapseE accessed 24 June 2018
 - See Gartner IT Glossary, available at <https://www.gartner.com/it-glossary/d> accessed 20 June 2018
 - SLAUGHTER AND MAY, “New rules, wider reach: the extraterritorial scope of the GDPR” (June 2016) 3 available at <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf> accessed 20 August 2018
 - Spotify available at <https://en.wikipedia.org/wiki/Spotify> accessed 20 June 2018
 - Steve Kenny, “An Introduction to Privacy Enhancing Technologies” (May 2008) available at <https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/> accessed 25 August 2018
 - Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, Digital Single Market REPORT / STUDY (25 April 2018) available at <https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and> accessed 2 August 2018

- Synopsis of World Trade Organization available at https://www.wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm accessed 24 June 2018
- The Practitioner's Guide to Data Quality Improvement “Data Governance and Quality: Data Reuse vs. Data Repurposing” (February 2012) available at <http://dataqualitybook.com/?p=349> accessed 20 August 2018
- What is personal data?, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#examples-of-personal-data accessed 2 August 2018
- Wikipedia, “Always-on DRM” available at https://en.wikipedia.org/wiki/Always-on_DRM#cite_note-13 accessed 5 July 2018
- World Intellectual Property Organization available at http://www.wipo.int/treaties/en/text.jsp?file_id=283854 accessed 24 June 2018
- Yun Shen, Siani Pearson, “Privacy Enhancing Technologies: A Review” HP Laboratories HPL-2011-113 (2011) 17, available at <http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf> accessed 25 August 2018