

i-call working paper

No. 2/15

Is Digital Text-Watermarking the Long-Desired User Friendly Digital Rights Management? Copyright and Fundamental Values from a Comparative Perspective

Jessica C. Lai[‡] and Christoph B. Graber^{*}

NOVEMBER 2015

ABSTRACT

Many have argued that technologies used to protect copyrighted works usually go beyond the letter of the law and subsequently impinge on interests relating to freedom of information and expression, privacy and free choice. Classic examples are technologies that prevent CDs or DVDs from being accessed or copied under certain conditions, or that block or filter-out copyright-protected materials. This article assesses digital text-watermarking, which does not restrict users' access to or use of works, but individualises every user's copy by changing the formatting or words in a text (e.g. "not visible" for "invisible"). Every purchaser/user receives a unique version of the work, meaning that, if there is any illegal upload or usage, it is possible to determine which user the copy came from. The technology thereby allows legal (and illegal) use to be undertaken, but serves as a tool for enforcement when there is illegal use. This article assesses digital text-watermarking from a comparative law perspective, particularly the Civil Law and the Common Law traditions.

KEY WORDS

digital text-watermarking, copyright enforcement, intellectual property protection, individualisation of work copies

[‡] Jessica C. Lai, PhD, Postdoctoral Researcher at the University of Lucerne Faculty of Law.

^{*} Christoph B. Graber, PhD, is Professor of Law at the University of Zurich Faculty of Law. Comments are welcome at: christoph.graber@rwi.uzh.ch

I-CALL WORKING PAPERS are the result of research that takes place at the Chair for Legal Sociology and Media Law (Professor C.B. Graber) at the University of Zurich. The papers have been peer-reviewed.

SUGGESTED CITATION: Jessica C. Lai and Christoph B. Graber, 'Is Digital Text-Watermarking the Long-Desired User Friendly Digital Rights Management? Copyright and Fundamental Values from a Comparative Perspective', *i-call Working Paper No. 2 (2015)*, Zurich, Switzerland: University of Zurich (an edited version of this article will be published in *European Intellectual Property Review*, published by Sweet & Maxwell, in 2016.).

Published by:
i-call, Information • Communication • Art • Law Lab at the University of Zurich
Professor Christoph B. Graber, PhD
Chair for Legal Sociology and Media Law
University of Zurich, Faculty of Law
Treichlerstrasse 10
8032 Zurich
Switzerland

ISSN 1664-0144
© Information • Communication • Art • Law Lab, Switzerland

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

Permission to use this content must be obtained from the copyright owner.

IS DIGITAL TEXT-WATERMARKING THE LONG-DESIRED USER FRIENDLY DIGITAL RIGHTS MANAGEMENT? COPYRIGHT AND FUNDAMENTAL VALUES FROM A COMPARATIVE PERSPECTIVE

1.	INTRODUCTION.....	4
2.	DRM: ITS EMERGENCE AND ITS PROBLEMS	5
3.	WHAT IS DIGITAL TEXT-WATERMARKING?	11
4.	DIGITAL TEXT-WATERMARKING AND FUNDAMENTAL VALUES.....	13
	4.1 FREEDOM OF INFORMATION AND EXPRESSION	13
	4.2 RIGHTS TO PRIVACY AND DATA PROTECTION	15
	4.3 FREEDOM OF CHOICE	15
5.	DIGITAL TEXT-WATERMARKING AND COPYRIGHT LAW....	16
	5.1 COPIES OR ORIGINAL/DERIVATIVE WORKS?	16
	5.2 RIGHT TO PROTECT THE INTEGRITY OF THE WORK.....	18
	5.3 FICTION VS NON-FICTION	19
6.	CONCLUSION	20

1. INTRODUCTION

Up until now, digital rights management (DRM) and technical protection measures (TPMs) have been rather blunt instruments that can *ex ante* prevent users accessing and using works that they legally purchased, sometimes preventing legal or permitted uses.¹ As an illustration, a TPM might prevent a user from copying a purchased eBook onto more than a certain number of devices, from printing it out, or may only allow the user to print out a low-quality version. Another DRM might monitor how the user uses a purchased work and report this back to the vendor or right holder, which might change the rules of access and use thereafter. These are restrictions that irritate everyday users, who often just want to use their copy of a work the same way that they would an analogue copy. It may even be the case that individuals want to use their copies of a work within the confines of a permitted use or exception to infringement, as per the law in their jurisdiction.

Of course, the problem is that we no longer live in an analogue world, where reprographic replication takes time and effort and results in sub-standard copies. Instead we live in a digital world, where making high-quality copies of works is simple and virtually costless. Intellectual property (IP) owners have a valid interest in protecting their property and their businesses and business models, which may require the use of restrictive technologies. It may also require that Internet users are “non-anonymous” so that they can be sued for infringement. On the other side, users have an interest in undertaking permitted uses of copyrighted works and in being opaque online so as to be anonymous and thereby better achieve communicative freedom. To date, the balancing of these different concerns has tended to favour IP owners, which have been able to use TPMs to protect their interests. However, the picture has not been so dire because – much to the ire of IP owners – no TPM has proved to be unhackable. We are, thus, at an impasse. Arguably, the market should meet the interests of users, to some extent, with respect to the dislike of overly restrictive TPMs. This is in part because there is a degree of futility in using TPMs when they are contrary to users’ expectations. While users are willing to put up with a certain level of inconvenience or frustration, a TPM will be hacked if this level is exceeded. TPMs to date have not been refined enough to meet this intricate balance.

Regulation by software and hardware that determine which works we can access and how we can use certain works obviously affect our freedom of information and expression. TPMs that remove anonymity additionally impact on our right to privacy. Furthermore, there are particular issues related to the fact that, by automatically preventing IP infringement, technology can remove choice or the ability to break the law. The elimination of user choice is seldom discussed, but is important because it encapsulates a core tension between, on the one hand, the desirability of a secure world in which laws are *de facto* always enforced and “undesirable” behaviour is

¹ See e.g. James Grimmelmann, ‘Regulation by Software’ (2005) *Yale Law Journal*, 114, pp. 1719-1758; Sonia K. Katyal, ‘Filtering, Piracy, Surveillance and Disobedience’ (2009) *The Columbia Journal of Law and the Arts*, 32 (4), pp. 401-426; Mark A. Lemley, ‘The Law and Economics of Internet Norms’ (1997-1998) *Chicago-Kent Law Review*, 73, pp. 1257-1294, at p. 1287; and Dan L. Burk, ‘Legal and Technical Standards in Digital Rights Management Technology’ (2005-2006) *Fordham Law Review*, 74, pp. 537-573.

barred from taking place, and, on the other hand, the value of liberty and the connected ability to flaunt laws by choice. The blunt nature of classic TPMs has meant that they have, more or less, removed user choice to defy the law.

This paper examines digital text-watermarking, a new kind of DRM for literary works,² and how it may organise and balance-out these different interests and concerns. It introduces digital text-watermarking as a contrast and alternative to existing DRM, particularly as a technology that is still in the interest of right holders, but more proportionate with respect to users, *ex ante/ex post* enforcement and user choice. Digital text-watermarking does not restrict users' access to or use of works. Instead, it individualises every user's copy by varying formatting or the words of the text. Every user receives a unique version of the work, meaning that, if there is any illegal upload or usage, it is possible to determine which user the copy came from. So far, it is envisaged that this technology be used for non-fiction (e.g. textbooks and manuals) rather than fictive novels, poetry or works of a more artistic nature. Nevertheless, it raises many questions, such as whether we can say that the versions are copies of the work, if modifications affect authors' moral rights, if the differences affect our access to information and, thus, affect our freedom of expression, if the individualistic nature of the works removes our anonymity enough to affect our right to privacy, and how the technology relates to user choice.

Part two of this paper analyses DRM, its history and issues to date. This is followed by a more in-depth description of what exactly digital text-watermarking is and how it works. Part four then examines the technology in light of its potential effects on the freedom of information and expression, the right to privacy and data protection, and freedom of choice, particularly in comparison to existing DRM. This is followed by an analysis of how the technology fits into copyright law. It does so from a comparative law perspective, looking at the Civil Law and Common Law traditions.

2. DRM: ITS EMERGENCE AND ITS PROBLEMS

It was only at the beginning of the 1990s that the Internet started its truly spectacular expansion, eventually becoming the ubiquitous and all-pervasive medium of communication that we know today. "Being digital", the vision of one of the Internet's most optimistic prophets,³ rather rapidly unveiled one of its main underlying ambiguities: While consumers have been praising the Internet as the "celestial jukebox"⁴ providing easy and unlimited access to the world's treasure-chest of literature, music and (moving) images, producers and owners of content have been concerned with the protection of their IP rights online. As a response to the IP-related concern, content owners have developed DRM to regulate access to

² See e.g. James Bridle, 'Digital Rights Protection and the Future of Writing', *The Guardian* (30 June 2013), available online at <http://www.theguardian.com/books/2013/jun/30/digital-rights-management-protection-sidim> (all online sources were accessed 5 November 2015); and Fraunhofer, 'SiDiM – Sichere Dokumente durch individuelle Markierung', available at <https://www.sit.fraunhofer.de/de/angebote/projekte/sidim/>.

³ Nicholas Negroponte, *Being digital*, 4th edn, New York: Knopf, 1995.

⁴ Paul Goldstein, *Copyright's Highway: From Gutenberg to the Celestial Jukebox*, 1st edn, New York: Hill and Wang, 1994.

and use of works by the means of technology. Mostly through the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA) and the Business Software Alliance (BSA), large and mostly US-based right owners successfully lobbied the World Intellectual Property Organization (WIPO) to develop new instruments of international law aimed at the protection of IP rights in the digital environment. On 20 December 1996 the WIPO Diplomatic Conference adopted the WIPO Copyright Treaty (WCT)⁵ and the WIPO Performances and Phonograms Treaty (WPPT).⁶ As a core element of the two Internet treaties, contracting parties are required to provide “legal protection and effective legal remedies” against the circumvention of TPMs.⁷ TPMs are aimed at regulating copying, distribution, access to and use of digital content online. The term DRM is commonly used interchangeably with TPM. However, there is no consensus as to whether the two terms are synonymous or whether one is broader than the other. As noted to us by Dan Burk, TPMs can be used in situations where there are no rights in play, such as on works that are in the public domain.⁸ DRM, on the other hand, relates to the management of rights, as the name suggests, making it arguably narrower than the term TPM. At the same time, one may manage their digital rights with a non-technical means, indicating that the term DRM could be broader than TPM. For the purposes of this paper, we will use the terms TPM and DRM as they relate to technical means of managing digital rights.

Since 1996 more than 90 countries have ratified the WCT and the WPPT and – as a response to their treaty commitments – many contracting parties have implemented the obligations regarding the anti-circumvention of TPMs within their national IP legislation.⁹ For example, the United States (US) did so in the Digital Millennium Copyright Act¹⁰ and the European Union (EU) implemented the treaties in the so-called Information Society Directive, requiring EU Member States in turn to implement anti-circumvention provisions at the national level.¹¹

Right holders consider TPMs as a necessary response against copyright piracy. Piracy has indeed been facilitated by the Internet, since digital content in combination with a global networked environment allow for the production and

⁵ WIPO Copyright Treaty (WCT), 36 ILM 65 (adopted on 20 December 1996, entered into force 6 May 2002).

⁶ WIPO Performances and Phonograms Treaty (WPPT), 2186 UNTS 203; 36 ILM 76 (adopted on 20 December 1996, entered into force 20 May 2002).

⁷ Articles 11 and 12 WCT and Articles 18 and 19 WPPT.

⁸ Many thanks to Dan for his assistance.

⁹ For a review see WIPO, Standing Committee on Copyright and Related Rights, Survey on Implementation Provisions of the WCT and the WPPT, Prepared by the Secretariat, (WIPO Doc. SCCR/9/6, 25 April 2003), available online at http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=16415. See also Jacques de Werra, ‘The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Legislations (Australia, Japan)’, in: Jane C. Ginsburg (ed.), *Adjuncts and Alternatives to Copyright: Proceedings of the 2001 Congress of the Association Littéraire et Artistique Internationale*, New York 2002, pp. 179-279 [hereinafter de Werra, ‘The Legal System of Technological Protection Measures under the WIPO Treaties’].

¹⁰ Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (28 October 1998). The DMCA is part of the US Copyright Act and the anti-circumvention rules are codified at 17 U.S.C. § 1201.

¹¹ EU Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (InfoSocDirective) (22 June 2001) OJ L 167 [hereinafter EU Directive 2001/29/EC]. The rules on anti-circumvention are codified in Articles 6 and 8 of the Directive. The Information Society Directive requires implementation at EU Member State level.

dissemination of perfect copies of content at no cost. On balance, the technological response that TPMs offer against piracy seems to be less damaging to the entertainment industry's image than the thousands of lawsuits that it has instigated against individual right owners over the years. Nevertheless, activists on the Internet have been designing tools that enable TPMs to be hacked, resulting in right holders considering legal protection against such circumvention as being necessary. With the proliferation of TPMs, three layers of protection of digital content can be identified. First, the legal protection afforded by the system of copyright law, second the technological measures protecting digital content against access and use (copying and dissemination) and thirdly the legal protection of TPM against circumvention.¹²

With the second and third layers of protection, TPMs have become "legalised enclosures", as James Boyle rather maliciously put it in his lucid critique of DRM.¹³ Boyle's critique of DRM is founded on his observation that they install private walls preventing the public from access and use of cultural information by "enrolling private actors to act as enforcement agents in a way that sidestepped the rights, duties, and privileges between citizen and sovereign."¹⁴ What is more, the "technological anticopying devices" are coated "with the authority of the law" since anti-circumvention rules are being generalised through codification in national copyright statutes.¹⁵ There has been a lot of debate in the academic literature on whether anti-circumvention rules belong at all in legislation on copyright. Rather than adding to this debate we would like to focus on discussing the social costs that TPMs are causing.

When identifying social costs we would like to start with the fact that DRM is often overbroad as it does not necessarily mirror the parameters of copyright law. If a consumer, for example, insists on her fair-use-based entitlement to make a private copy of a DRM protected DVD, she has to challenge the copyright owner before a court, because the technology functions *ex ante*. This involves a reversal of the burden of proof, if compared to a situation without DRM where the enforcement of copyright is *ex post*. Often, DRM prevents consumers from shifting purchased content from one device to another. If a buyer of an e-book hacks the DRM protection in order to extract the content or transfer it to another device, she risks violating anti-circumvention rules. Furthermore, DRM can restrict a buyer of an e-book from a number of benefits that an owner of a printed book would have, including making annotations or highlighting sentences. In an EU-wide public consultation on the need for copyright reform conducted by the European Commission in 2014, respondents complained that the use of DRM to enforce territorial restrictions makes it impossible to access paid-for content while travelling outside of their Member State.¹⁶ Institutional users argued that DRM prevents one from re-selling content and thus

¹² De Werra, 'The Legal System of Technological Protection Measures under the WIPO Treaties', *supra* note 9, at p. 200.

¹³ James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' (1997) *University of Cincinnati Law Review*, 66, pp. 177-205, at p. 196.

¹⁴ *Ibid.*, at p. 200.

¹⁵ *Ibid.*

¹⁶ European Commission, Directorate General for Internal Market and Services, 'Report on the Responses to the Public Consultation on the Review of the EU Copyright Rules' (July 2014) [hereinafter EU Commission Copyright Report 2014], at p. 6.

foreclose the emergence of secondary markets.¹⁷ This is deplorable not only from a competition policy perspective but also when considering that secondary markets may contribute to the preservation of digital goods as cultural heritage.¹⁸ Overall, respondents argued that DRM inhibits consumers from making use of a number of copyright exceptions they would legally be allowed to enjoy.¹⁹

DRM endows content owners with the technological means to enclose information in a private domain and keep it from the public discourse.²⁰ This is problematic from a constitutional rights perspective since freedom of expression and information or freedom of speech (hereinafter: communicative freedom) presupposes speakers' access to a diversity of relevant information as a prerequisite for building and expressing their own opinions. If access to the enclosed information is conditional on the payment of a fee, less affluent participants in the discourse will be disadvantaged.

Particularly in the sphere of academic research, freedom of communication "requires access to information but – prior to this – knowledge about the existence of information".²¹ In order to get this knowledge, researchers should not be hindered by DRM from browsing for content on the Internet directly. From the perspective of scientific progress and freedom of research, DRM may have a number of detrimental effects – especially when academics at Universities, research units and libraries are barred from making legally allowed uses.²² In the humanities, for example, DRM may prevent scholars and teachers from incorporating clips of audiovisual works into their scholarly studies or classroom presentations.²³ What is more, researchers can be prevented from text mining, which is of utmost importance not only in the natural and social sciences but also in the humanities.²⁴ Taking an example from the natural sciences, imagine a biologist who needs to match the enormous amount of data collected in the Linne taxonomy in order to know what has been published on a certain species she is interested in. To do this, the researcher must engage in data-mining, which presupposes the possibility to re-format data. DRM will usually not allow such procedures.

As cloud services proliferate on the internet,²⁵ tethered DRM technologies are increasingly used as a means for copyright enforcement when users stream cultural content or software over the Internet to their smartphones or computers. Beyond

¹⁷ Ibid., at p. 21.

¹⁸ Indeed, the marketing of a digital cultural product on a secondary market assures the availability of the work as cultural heritage even in a case where the parties who control the supply of the work on the first market decide to stop its distribution (for example because they do no longer find it to be cost-effective).

¹⁹ EU Commission Copyright Report 2014, supra note 16, at p. 91.

²⁰ Yochai Benkler, 'Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain' (1999) *New York University Law Review*, 74, pp. 354–446.

²¹ Christoph B. Graber, 'Copyright and Access – a Human Rights Perspective', in Christoph B. Graber et al. (eds), *Digital Rights Management: The End of Collecting Societies?*, Bern: Stämpfli, 2005, pp. 71–110, at p. 72.

²² Christoph B. Graber, 'Beobachtungsstelle für technische Massnahmen im Urheberrecht: Erste Erfahrungen und Prüfung von Handlungsbedarf im Bereich der Wissenschaft' (2010) *SIC! - Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht*, 5, pp. 329–340, at p. 338.

²³ Patricia Akester, 'Technological Accommodation of Conflicts Between Freedom of Expression and DRM: The First Empirical Assessment', *University of Cambridge*, Research Paper 2009, available at <http://ssrn.com/abstract=1469412>, at pp. 54–64.

²⁴ EU Commission Copyright Report 2014, supra note 16, at pp. 64, 66.

²⁵ See Daniel J. Gervais, 'Copyright, Culture and the Cloud', in Sean A. Pager and Adam Candeub (eds), *Transnational Culture in the Internet Age*, Cheltenham, UK: Edward Elgar, 2012, pp. 31–54.

“perfect enforcement”²⁶ of IP rights, the technology allows for the tracking of every use that a consumer makes of certain content.²⁷ Monitoring user behaviour and collecting personal data raises concerns from a privacy perspective.²⁸ Privacy is considered to be a precondition for freedom of information and expression.²⁹ This is because individuals need to believe that they have privacy in order to feel that they can seek information freely, form opinions and express them with anonymity.³⁰ Without privacy, individuals cannot develop their true “selves”. Technologies that make individuals non-anonymous can thereby potentially affect both the interest of privacy and freedom of expression and information. According to the Court of Justice of the European Union (CJEU) data protection rights may be infringed when Internet service providers monitor user behaviour and collect data for the purpose of copyright enforcement.³¹

Additionally, dominant market players may be tempted to turn DRM into technical standards in order to control interoperability of a product. As Burk has shown for the US, anti-circumvention provisions of the DMCA have been used by dominant companies “to exclude from the marketplace not threats to the technical protection of a copyrighted product, but interoperable products that might disturb copyright holder’s plans for an adjacent market”.³² This has also been an issue in the 2015 US Copyright Office DMCA exemption hearings. Apparently, the DMCA’s prohibition of the circumvention of TPMs prevents diagnosis and repair of software in personal cars, commercial motor vehicles, agricultural machinery and other vehicles. In reaction to this, a number of submissions filed by Internet activists and NGOs have requested the Copyright Office for a DMCA Section 1201 exemption.³³

Finally, there are several issues associated with the fact that DRM removes user choice. As something that is little discussed compared to the relationship between DRM and freedom of information and expression and privacy/data protection, it is worth teasing these issues out. Roger Brownsword has argued that technologies that eliminate the option of non-compliance are generally not good for society because they eventually wear away peoples’ ability to assess what is the “right” or “moral”

²⁶ Jonathan Zittrain, ‘Perfect Enforcement on Tomorrow’s Internet’, in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford and Portland, OR: Hart Publishing, 2008, pp. 125–156, at p. 136.

²⁷ Christoph B. Graber, ‘Tethered Technologies, Cloud Strategies and the Future of the First Sale/Exhaustion Defence in Copyright Law’ (2015) *Queen Mary Journal of Intellectual Property*, 5 (4), (forthcoming).

²⁸ Julie E. Cohen, ‘A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace’ (1996) *Connecticut Law Review*, 28, pp. 981–1039.

²⁹ Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967.

³⁰ Julie E. Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*, New Haven, MA: Yale University Press, 2012, at pp. 110–115; UN Human Rights Council (HRC), ‘Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue’, 17th Session (UN Doc. A/HRC/17/27, 2011), at para 53; Council of the European Union, ‘EU Human Rights Guidelines on Freedom of Expression Online and Offline’, Foreign Affairs Council Meeting (12 May 2014), at p. 18.

³¹ *Scarlet Extended NV v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* (24 November 2011) CJEU C-70/10, at para. 43.

³² Dan L. Burk, ‘Legal and Technical Standards in Digital Rights Management Technology’ (2005) *Fordham Law Review*, 74, pp. 537–573, at p. 565.

³³ See the proponent’s submission in classes 21 and 22 in the ongoing US Copyright Office DMCA Section 1201 Rulemaking. Available at <http://copyright.gov/1201/2015/comments-020615/> and at <http://copyright.gov/1201/2015/reply-comments-050115/>.

thing to do.³⁴ Brownsword believes that employing technology to reinforce a moral line reduces the opportunities for people to learn how to behave appropriately in society, or practice being moral. If individuals are not permitted to undertake moral reasoning or judgement, or make genuine choices, moral communities will not develop,³⁵ and individuals will start to view the moral responsibility as lying not with themselves, but merely in the system.³⁶ T.J. McIntyre and Colin Scott have made similar arguments.³⁷

There are two further problems if choice is removed. Firstly, if individuals have no choice for certain things, they will come to believe that the actions that are not blocked are socially and legally permissible. Put another way, individuals would tie possibility with legality and vice versa; hence the generation and stabilisation of normative expectations would be affected.³⁸ Secondly, over time, the regulation can become the norm;³⁹ one will simply consider the regulations to be the way things are and “customary”, such that there is a normative must behind complying with them. Possibly, people would even come to believe that things could not be any other way. This can happen when what one can or cannot do with something is determined by technology for such a long length of time that people forget that it is a matter of coding that could be written differently.

Jonathan Zittrain has further stated that enforcement via technology “collapses the public understanding of the law” because it removes the interface between the

³⁴ Roger Brownsword, ‘So What Does the world Need Now? Reflections on Regulating Technologies’, in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford and Portland, OR: Hart Publishing, 2008, pp. 125–156, at p. 136.

³⁵ *Ibid.*, at p. 42: “Where techno-regulation simply eliminates the possibility of deviating from the required pattern of conduct, where the only practical option is to do the right thing, then the conditions for moral community are surely compromised.”

³⁶ Karen Yeung, ‘Towards an Understanding of Regulation by Design’, in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford and Portland, OR: Hart Publishing, 2008, pp. 23–48, at pp. 79–107, 99.

³⁷ T.J. McIntyre and Colin Scott, ‘Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility’, in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford and Portland, OR: Hart Publishing, 2008, pp. 109–124, at p. 111, who state that “filtering may rob users of moral agency or responsibility in their use of the Internet, with the implication that they may freely do whatever it is technically possible to do, with no necessity of moral engagement in their activities. If such consequences were to follow through into wider patterns of social interaction, the consequences for responsibility and for social ordering generally, of such low-trust mechanisms of control might be troubling.”

³⁸ According to Luhmann, there are cognitive and normative expectations in society. Cognitive expectations are those that are adjusted if disappointed, whereas normative expectations are upheld irrespective of a breach of the expectation in an individual situation. For example, the expectation not to be hit on the street is a normative expectation. In the case that somebody would hit you (i.e. that your expectation would be violated), everybody would understand that you continue to insist on the expectation. The law is the main sphere in society where normative expectations are formed and Luhmann defines the generation and stabilisation of normative expectations as the function of the law. See Niklas Luhmann, *A Sociological Theory of Law*, Hoboken: Taylor and Francis, 2013, at pp. 31–40.

³⁹ See Mark A. Lemley, ‘The Law and Economics of Internet Norms’ (1997–1998) *Chicago-Kent Law Review*, 73, pp. 1257–1294, at pp. 1287–1292; T.J. McIntyre and Colin Scott, ‘Internet Filtering: Rhetoric Legitimacy, Accountability and Responsibility’, in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford and Portland, OR: Hart Publishing, 2008, pp. 109–124, at p. 123; and Mireille Hildebrandt and Bert-Jaap Koops, ‘The Challenges of Ambient Law and Legal Protection in the Profiling Era’ (2010) *The Modern Law Review*, 73 (3), pp. 428–460, at pp. 455–456.

law's terms and its application.⁴⁰ Individual choice about what one deems to be right or wrong is part of what makes us human. This disappears in a completely monitored and controlled environment and one loses the ability to judge "whether one's behaviour is an expression of character or is merely compelled by immediate circumstance."⁴¹ Analogously, Mireille Hildebrandt has maintained that "... in a constitutional democracy, law can neither assume compliance nor rule out non-compliance because citizens have the right to contest the law both when they vote for a new legislature and when they confront an alleged violation in court."⁴²

Overall, DRM to date has been over-encompassing, skewing the legally negotiated balance between rights holders' rights and users' permitted uses by *ex ante* preventing those uses from taking place, or by tethering technologies to vendors and removing user privacy. Though no DRM has proved to be unhackable, a third layer of protection, making circumvention of TPMs illegal in many circumstances, has kept the balance skewed. While right holders certainly have a valid interest in protecting their works and business models, DRM that prevents access or use of works *ex ante*, or that tracks users' use of works, is arguably disproportionate with respect to users and their interests, particularly in light of freedom of information and expression, the right to privacy and the interest in having choice. There is, thus, space for an alternative to currently used DRM that still meets the interests of right holders, but that is not so disproportionate with respect to users and their concerns pertaining to *ex ante* access to or use of works, in a manner that does not impinge to greatly on their privacy.

3. WHAT IS DIGITAL TEXT-WATERMARKING?

The concept of watermarking generally is not new. It first appeared in the late thirteenth century as a means to identify the source or manufacturer of paper, whereby paper was physically embossed during the manufacturing process. Paper continues to be watermarked by varying the thickness or density of certain parts of sheets of paper, such as to create an image via the consequential differential transmission of light. A common example of this is on paper money. The purpose of watermarking was, thus, attribution of source and – relatedly – a means to prevent forgery. The concept of watermarking has been developed into the digital world, but with different purpose; rather than being about source or authenticity of the vendor it is about users and being able to tie a purchaser to a particular copy of a work. Digital watermarking allows different copies of works to have different changes made to them. These changes act like a fingerprint, permitting the identification of copies of works to a specific sale, purchaser or source. Digital watermarking has long been used on multimedia data, such as videos and pictures.⁴³ These media are particularly susceptible to watermarking, as small changes can be made to the works

⁴⁰ Zittrain, *supra* note 26, at p. 151.

⁴¹ *Ibid.*

⁴² Hildebrandt and Koops, *supra* note 39, at p. 445.

⁴³ See Melinos Averkiou, 'Digital Watermarking' (2006), available at <https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf>; and Mohan Durvey and Devshri Satyarathi, 'A Review Paper on Digital Watermarking' (2014) *International Journal of Emerging Trends & Technology in Computer Science*, 3(4), pp. 99-105.

that cannot be observed by the human eye. They are “noise-tolerant”. Furthermore, it does not matter which pixels are changed, making it simpler to create the algorithms necessary to effect the modifications. This is quite different with texts, which cannot be changed in the same way as visual media without human perception. For example, while one can change pixels in a video in a way that is not visually discernible, it is not possible to change characters in written text because there is no redundancy;⁴⁴ an “f” must be an “f”, semantics and syntax require that certain rules are obeyed, and structure and style are of import. Word texts are not noise-tolerant. Of course, it is possible to watermark documents (i.e. the embodiments of works) rather than the texts (or works) themselves. It is also possible to do so in an individualistic manner, e.g. with the purchaser’s name. However, this has not proved to be very successful, as it (1) irritates users, (2) can be easily hacked and (3) does not stop users from simply copying the text to a new document.

In recent years, researchers have been investigating means by which the text itself could be digitally watermarked.⁴⁵ This could be, for example, through playing with format, layout, line spacing, or intra- or inter-word spacing. However, though these methods play with the text, they nevertheless relate to the display or the embodiment of the work and are easily overcome by document-shifting the text. One must then go down to the “word level” in order to effect changes that cannot be so easily surmounted and cannot be removed, as they are not tied to a medium. This may be through adding extra commas, semi-colons, or similar punctuation marks where they are not strictly necessary. The problem with this approach is that it would be difficult to create an algorithm that can detect where in a text such changes could be made. A second possibility is turning active sentences into the passive. However, this can modify a text significantly, as active and passive sentences play different roles. Thirdly, synonyms could be substituted, but this again could alter the text too much, changing meaning. It is not possible to create an algorithm refined enough to determine for certain whether two words are interchangeable within a given context. Finally, modifications could be made where there could be more than one spelling of a word, known abbreviations or acronyms or substitution with jargon. This, however, could not be used on formal or academic texts, as they would be considered to be errors.

This paper looks at possible alterations that an algorithm could easily determine as feasible, that would not change the meaning of text, and that would not introduce incorrect changes. More specifically, it looks at the possibility of four types of changes: (1) changes around conjugation, e.g. “Victor and Anna” to “Anna and Victor”; (2) addition of hyphens in cases where hyphenation or non-hyphenation are both corrective, e.g. “cooperative” to “co-operative”; (3) modulation of lists, e.g. “music, audio books, videos or e-books” to “music, videos, audio books or e-books”;

⁴⁴ Priyanka Verma, Rakhshan Anjum Shaikh, Ketki Deshmukh, ‘A Novel Approach to Angle Based Invisible Text Watermarking with EBCDIC Coding’ (2013) *International Journal of Computer Applications*, 61(20), pp. 33-38, at p. 34.

⁴⁵ As discussed in Oren Avni and Martin Steinebach, ‘Digitale Wasserzeichen für textuelle Informationen’ (2010) *Information: Wissenschaft & Praxis*, 61(5), pp. 285-291, at pp. 287-288; and Xiaofeng Wang, ‘Digital Watermarking Research Based on Text’, *Third International Conference on Information Science and Technology* (23-25 March 2013, Yangzhou, Jiangsu, China).

and (4) playing with negatives, e.g. “not fair” to “unfair”.⁴⁶ By first identifying where changes could be made, making the modifications at certain points, but not others, every version of a work ends up unique.

Digital text-watermarking does not try to emulate a real-world friction (i.e. a limitation inherent in physical copies) and, hence, does not in any way restrict access to or use of works. As mentioned, the purpose of the watermarking is to allow vendors/IP owners to tie specific versions of works to specific purchasers/users and, thus, to connect any illegal use to a specific user. Additionally, it does not leave a digital trace (at least this is not its purpose). Instead, it has almost analogue-like effects by actually changing the text. This means that – unlike digital watermarks – what digital text-watermarking does to each sold version cannot be hacked or removed.

4. DIGITAL TEXT-WATERMARKING AND FUNDAMENTAL VALUES

As highlighted in the Introduction, technologies used by copyright owners can severely impact our ability to access and use works – and ultimately our privacy and communicative freedom – in a way that is not easily addressed by existing laws. They can furthermore remove user choice. This part of the paper investigates how digital text watermarking fares with respect to the concerns raised regarding communicative freedom, privacy and user choice.

4.1 FREEDOM OF INFORMATION AND EXPRESSION

What distinguishes digital text-watermarking from existing DRM is that it does not act *ex ante*. The technology is most certainly of benefit to right-holders, who can use it to tie a specific version to specific users. At the same time, it is more proportionate than DRM with respect to user-interests. This is because it represents a reversion to pre-DRM enforcement of copyright, whereby right-holders still have to enforce their copyright through the legal system and have the burden of proof to show infringement. Digital text-watermarking acts *ex post*, by assisting right-holders to prove infringement by specific users. It does not *ex ante* control users’ ability to access or use the copyrighted works, and users are not placed with the burden to prove their innocence or that their acts fall into a permitted use or exception. Therefore, from the perspective of access to information and the making of expression, digital text-watermarking is favourable over existing DRM.

That every version of a work is unique poses interesting questions particularly relating to whether we all have access to the same information or not. Within this issue, it does not matter that the technology is intended for non-fiction. On the one hand, it is arguable that the modifications do not change the sense (i.e. the ideas or information) of the text, just the expression, and therefore do not affect our access to

⁴⁶ These are the particular changes proposed by “Sichere Dokumente durch individuelle Markierung” (SiDiM), developed by the Fraunhofer Institute. See Avni and Steinebach, *supra* note 45, at pp. 288-290; and SiDiM, ‘SiDiM: Textwasserzeichen Evaluierung’, available at <http://www.boersenblatt.net/media/747/sidimevaluierung.pdf>.

information. On the other hand, one could posit that the expression is important. It is inarguable that society needs to have access to common ideas and information as a precondition for meaning-making in a democracy. As Peter Yu has rightly emphasised in a recent paper, “third parties can have strong interests in preserving the work and stabilizing its social and cultural meanings”.⁴⁷ In the context of our modern online world, one could extend this to a need to have expressions that are common to all. This is because we search for texts and exact expressions when looking for information on the Internet. If we all quote something slightly differently, it becomes harder to locate the source or to identify the “original”. Even offline, exact expression does matter.⁴⁸ To deny this would be to turn a blind eye to the fact that certain quotes defy the ages. Finally, copyright law permits the use of works for the purposes of quotation. The application of this permitted use is unclear if every version of a work varies slightly. Notably, while audience interests in the stability of works are equally important both in artistic and in scientific contexts,⁴⁹ it is not exactly immutability of a creative work that is always required,⁵⁰ but rather the possibility to identify a reference work for purposes like citation, comparison or falsification – depending on whether this happens within an artistic or scientific discourse. Hence, from a third party perspective, it would often be sufficient if the meta data that is digitally inscribed in the underlying work would remain immutable.⁵¹ This purpose is already fulfilled as both the Digital Millennium Copyright Act in the US and the EU Information Society Directive⁵² prohibit the intentional removal of such information.⁵³

It is important to note that digital text-watermarking – although leading to individualised copies – does not pose the same concerns as those raised by Eli Pariser⁵⁴ and Cass Sunstein⁵⁵ with respect to personalised content-filtering. Online content personalisation produces “filter bubbles”, which in turn affect our ability to

⁴⁷ Peter K. Yu, ‘Moral Rights 2.0’ (2014) *Texas A&M Law Review*, 1 (4), pp. 873–900, at p. 888.

⁴⁸ There exists case law in the UK, EU and US that either acknowledges or leaves open the possibility that there may be rare situations where the “public interest” outweighs copyright, but cannot be met by the idea/expression dichotomy or a permitted use. See e.g. *Ashdown v Telegraph Ltd* (2002) EWCA 1142 (Civ) at paras 31, 33, 39, 43 and 45; *Ashby Donald and others v France* (2013) ECtHR Appl. No. 36769/08; and *Eldred v Ashcroft* 537 US 186 (SC 2003), affirmed 239 F 3d 372 (DC Cir 2001).

See also Jo Oliver, ‘Copyright, Fair Dealing, and Freedom of Expression’ (2000) *New Zealand University Law Review*, 19, pp. 89-131; Susy Frankel, ‘Protecting “Killer Cros” and “Fantasy Football”. The Ethics of Copyright Law’ (1998) *Victoria University of Wellington Law Review*, 28, pp. 191-207, at pp. 197-198; Patrick Masiyakurima, ‘Fair Dealing and Freedom of Expression’, in Paul LC Torremans (ed.), *Copyright and Human Rights. Freedom of Expression – Intellectual Property – Privacy*, The Hague: Kluwer Law International, 2004, pp. 87-108, at p. 92; and Eric Barendt, ‘Copyright and Free Speech Theory’, in Jonathon Griffiths and Uma Suthersanen (eds), *Copyright and Free Speech. Comparative and International Analyses*, New York: Oxford University Press, 2005, pp. 11-33, at [2.06]. A possible flaw with digital text-watermarking is that it could automatically make modifications to quotes within a text, which would obviously then make the quotes incorrect.

⁴⁹ Justin Hughes, ‘“Recoding” Intellectual Property and Overlooked Audience Interests’ (1999) *Texas Law Review*, 77, pp. 923-1010, at pp. 940-966 (emphasising non-owner interests in the stability of a work).

⁵⁰ Mira T. Sundara Rajan, *Moral Rights. Principals, Practice and New Technology*, New York: Oxford University Press, 2011, at pp. 21-22.

⁵¹ Neil Netanel, *Copyright’s Paradox*, Oxford: Oxford University Press, 2008, at p. 215.

⁵² EU Directive 2001/29 EC, supra note 11, at pp. 10-19.

⁵³ Yu, supra note 47, at p. 880.

⁵⁴ Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You*, New York: Penguin Press, 2011.

⁵⁵ Cass R. Sunstein, *Republic.com 2.0*, Princeton, N.J.: Princeton University Press, 2007.

obtain a diversity of information and to participate in deliberative processes, build common understanding and be citizens in a well-functioning democracy. Digital text-watermarking individualises some wording, but does not personalise it; there is no employment of a user profile to prioritise information according to what a filter deems we “want to see”. If done well, the meaning should be identical. Concerns relating to data collection to create profiles and the in-effect filtering out of certain information do not arise.

4.2 RIGHTS TO PRIVACY AND DATA PROTECTION

Though there is no personalisation of information, it would be incorrect to think that there are no problems relating to privacy. The individualistic nature of the copies removes users’ anonymity with respect to that work. Digital text-watermarking essentially allows copyright owners to bypass the need to go to ISPs for user information and is a means of tethering a version and its user to the vendor. There are, thus, privacy implications. The relevant question for the purposes of our inquiry is whether this level of non-anonymity affects our privacy enough that our communicative freedom is also impinged.

In all likelihood, digital text-watermarking would not affect privacy and expectations of privacy in a significant way that would consequently impact on freedom of information and expression. This is because it does not act as a digital beacon. By itself, it does not allow owners to track users’ usage and obviously does not collect or use user data, unlike certain DRM, which can allow vendors to monitor users. It only allows copyright owners to connect a version of their work to a specific purchaser when they see that version, for example, if they find that version being distributed or made available online. While there is a slight loss of anonymity, it is unlikely that a user’s behaviour would be affected, such that he/she would not seek or impart information in the same way as if digital text-watermarking did not protect the work. The loss of anonymity would not at all affect the ability to seek information. It would have more of an impact on the ability to make expression because an expression that uses enough of the work can be tracked back to the user. However, there are two points to be made. Firstly, the technology does not prevent the ideas in a work from being used in expression anonymously. Secondly, if the use is not an infringement of copyright, e.g. a portion is used for quotation, it is highly unlikely that enough modifications would be in that used portion in order to allow for the identification of the version copied from, not to mention that copyright owners would have very little interest in such use.

4.3 FREEDOM OF CHOICE

As the discussion above indicates, the majority opinion seems to be against the absolute removal of choice, including via technology ostensibly used to protect copyright. This is in large part connected to the philosophical notions that there is no

obligation to obey the law and that sometimes civil disobedience or conscientious objection are justified.⁵⁶

With this in mind, digital text-watermarking seems rather favourable, as it is far subtler and refined than DRM used to date and – being *ex post* – by no means removes user choice, or even copyright-owner choice. Black-and-white code is not imprinted onto each copy of a work, which then deals with situations without discretion. Users are simply discouraged from infringing the copyright of a work by the knowledge that the action can be traced back to them, but they may nevertheless deem it worth it or necessary to do so. The choice and moral responsibility is still theirs, as they are not technically inhibited from using their version of the work as they wish. Human decision-making is also not removed from the process of enforcing copyright, as the fingerprint that the digital text-watermarking technology literally imprints (or imprints literally) only allows for a work to be tracked back to its purchaser, not tracked *per se*. The fingerprint would also not make a copy tethered to the vendor in a way that would allow the latter to unilaterally (whether by technical or human means) to remove access to the work or delete it. In other words, there is no merging of the law and its execution. Of course, it is possible that a copyright owner has a computer program that detects the public distribution or making available of their work online, tracks it back to a particular purchaser and sends out a pro forma cease and desist letter, possibly including an arbitrarily set fine. However, because the user could always refuse to comply, human action (or at least another technology) is still required to truly enforce the copyright and a human being can still decide whether the use of the work falls within a permitted use or is justified by another value or interest, such as communicative freedom or the public interest.

5. DIGITAL TEXT-WATERMARKING AND COPYRIGHT LAW

5.1 COPIES OR ORIGINAL/DERIVATIVE WORKS?

One could question whether each of the versions created by digital text-watermarking really are copies of the original work. After all, they are all linguistically unique. Furthermore, it is a core tenet of copyright law that only the expression is protected, not the idea. If every version is expressed slightly differently to convey the same idea, it is possible that some of the versions could be themselves original works rather than copies of the original work, or derivative works, in which case the right to adaptation would come into play. Of course, this would depend on the specific changes made in each version. When the changes are merely subtle and non-substantive variations, it is unlikely that a court would deem a version to be an original work or even a derivative work. This is in both the Common Law and Civil Law traditions. In the former, the level of originality required is low. One is allowed to draw from the “stock of common knowledge”.⁵⁷ Originality will be found so long as the expression came from the author. Novelty is not required, but skill, labour and

⁵⁶ See Joseph Raz, *The Authority of Law: Essays on Law and Morality*, Oxford: Oxford University Press, 2009, Chapters 12, 14, 15.

⁵⁷ See *University of London Press Ltd v University Tutorial Press Ltd* (1916) 2 Ch 601.

judgement.⁵⁸ Hence, minor changes may make a work copyright protected. Nevertheless, given that the nature of digital text-watermarking is to make unnoticeable changes, it can hardly be the case the changes can then be said to make a new work.

This would likely also be the case in Civil Law jurisdictions, which have a higher originality standard. Notably, while the courts and many scholars in Civil Law countries continue to refer to the “imprint of personality” as an originality standard irrespective of the concept’s uselessness as an operational tool, there is “an unstoppable trend towards a more objective criterion of originality”.⁵⁹ Thus, although differences between copyright and *droit d’auteur* may not have entirely disappeared,⁶⁰ interpretations of originality are converging.⁶¹ Many courts in Civil Law jurisdictions are applying a test of creative choices that considers the availability of options within a human’s creative process. As Daniel Gervais has forcefully argued such a standard is not far away from what the US Supreme Court required in *Feist*,⁶² albeit differences in terminology.⁶³ In any case, it is unlikely that a watermarking-type of text alterations would pass the originality test in *droit d’auteur* jurisdictions. An overarching question is who the author would even be if there were separate copyright for the derived versions. Who would be the author who has used his/her skill, labour and judgement, or imprinted his/her personality?

Whether we have different works is almost a philosophical question rather than a legal one, as perhaps there is no original/derivative work, or perhaps a user would not notice the alterations, but the author would argue that the changes affect the flow of the sentence, style of the text, the rhythm of the words, or what the author wishes to emphasise. The author may even argue that the changes are grammatically incorrect, or affect the style of the author. As an illustration:

There are many stray cats and dogs and rats in the city.
There are many stray dogs and cats and rats in the city.
There are many stray cats and dogs, and rats in the city.
There are many rats and stray cats and dogs in the city.

None of these constructions are incorrect and they all have more or less the same meaning. However, the “most correct” or the one written in the “best style” depends on the author, their school of grammar and perhaps where they learnt English. For example, the authors prefer the final formulation and would not say that that the others are incorrect, but perhaps unwieldy (“stray cats and dogs and rats) or odd (“dogs and cats”). Notably, the placing of digital fingerprints on audio and

⁵⁸ See *Ladbroke (Football) Ltd v William Hill (Football) Ltd* (1964) 1 All ER 465 (HL).

⁵⁹ Ramón Casas Vallés, ‘The Requirement of Originality’, in Estelle Derclaye (ed.), *Research Handbook on the Future of EU Copyright*, Cheltenham, UK: Edward Elgar, 2009, pp. 102–132, at p. 112.

⁶⁰ Sam Ricketson and Jane C. Ginsburg, *International copyright and neighbouring rights: The Berne Convention and Beyond*, 2nd edn, vol. 1, Oxford: Oxford University Press, 2006, at para 8.05. For a comparison of the two traditions see the seminal study by Alain Strowel, *Droit d’auteur et copyright: Divergences et convergences. Etude de droit comparé*, Bruxelles: Bruylant, 1993.

⁶¹ Vallés, *supra* note 59, at p. 113.

⁶² *Feist Publications Inc v Rural Telephone Service Company Inc* (1991) 499 US 340.

⁶³ Daniel Gervais, ‘Feist Goes Global: A Comparative Analysis Of The Notion Of Originality In Copyright Law’ (2002) *Journal of the Copyright Society of the U.S.A.*, 49, pp. 949–981, at p. 981.

audiovisual works does not have these problems because the changes are not perceptible to humans.

5.2 RIGHT TO PROTECT THE INTEGRITY OF THE WORK

Because digital text-watermarking alters the work, questions regarding the moral rights of the author could surface, as authors (particularly in Civil Law countries) have the right “to object to any distortion, mutilation or other modification of, or other derogatory action in relation to the said work, which would be prejudicial to the author’s honor or reputation”, according to the Berne Convention.⁶⁴ The right to object to derogatory treatment of a work, which is often called the “right to protect the integrity of the work” or “right of integrity”, is considered to be the most important moral right protected under Article 6bis(1) of the Berne Convention. Although the inclusion of moral rights in the Berne Convention is considered to be a success of the authors’ rights movement, “there was never unanimity between the epistemic communities” involved in the negotiation process.⁶⁵ Moral rights and the right of integrity are indeed very much associated with an epistemology of *droit d’auteur*, focusing on the author’s personality (being reflected in the work) rather than the work as such. Similarly, Article 6bis of the Berne Convention has not been incorporated into the TRIPS Agreement of the World Trade Organization (WTO) due to resistance from the US, which feared that its legislation may not be fully compatible with Article 6bis.⁶⁶ In the TRIPS-plus bilateral, regional and plurilateral trade agreements that the US has adopted since 1995, moral rights have never been mentioned.⁶⁷ Summing up, the level of protection regarding the right of integrity is considerably higher under Civil Law than under Common Law.⁶⁸ There is, thus, a real possibility that digital text-watermarking could contravene the right of integrity in Civil Law jurisdictions.

In contrast to the Civil Law approach, Common Law countries tend to interpret the right narrowly such that it is not about the integrity of the work or the author’s personality, but the reputation and honour of the author,⁶⁹ in accordance with the exact wording of the Berne Convention.⁷⁰ Not only do Common Law jurisdictions

⁶⁴ WIPO, Berne Convention for the Protection of Literary and Artistic Works, 828 UNTS 222 (adopted on 9 September 1886), as revised at Stockholm (14 July 1967), Article 6bis(1).

⁶⁵ Willem Grosheide, ‘Moral rights’, in Estelle Derclaye (ed.), *Research Handbook on the Future of EU Copyright*, Cheltenham, UK: Edward Elgar, 2009, pp. 242–266, at pp. 243–244.

⁶⁶ Daniel J. Gervais, *The TRIPS Agreement: Drafting History and Analysis*, 4th edn, London: Sweet & Maxwell, 2012, at para 2.136. As a consequence, the dispute settlement mechanism offered by the WTO framework – which is exceptionally efficient in terms of international law standards – is not available for the settlement of right of integrity disputes at the level of international law.

⁶⁷ Yu, *supra* note 47, at p. 876.

⁶⁸ Many civil law states do not require any harm to the reputation or honour of the author, but just a negative impact on the integrity of the work; see Jacques de Werra, ‘The Moral Right of Integrity’, in Estelle Derclaye (ed.), *Research Handbook on the Future of EU Copyright*, Cheltenham, UK: Edward Elgar, 2009, at pp. 268–269.

⁶⁹ See, generally, Cyril Rigamonti, ‘Deconstructing Moral Rights’ (2006) *Harvard International Law Journal*, 47 (2), pp. 353–412; Mira T. Sundara Rajan, *Moral Rights. Principals, Practice and New Technology*, New York: Oxford University Press, 2011; Yu, *supra* note 47. See also *Pasterfield v Denham* (1999) FSR 168, at p. 182 (Overend J (Plymouth county court)); and *Confetti Records v Warner Music UK Ltd* (2003) EMLR 35, at para. 150 (Lewison J (EWHC)).

⁷⁰ De Werra, ‘The Moral Right of Integrity’, *supra* note 68, at p. 268 (identifying the formula “author’s honour or reputation” as threshold condition).

read the right to integrity very narrowly, there are also very few cases where moral rights have been raised and even fewer successfully argued.⁷¹ Moreover, though named “moral rights”, the interests of “honour or reputation” are different from those of “moral” or “spiritual” interests, the latter of which are wider.⁷² This means that it is not enough that the author does not like what has been done. Rather the rights are viewed from an objective standpoint, requiring that the intervention reflects badly on the author from the perspective of the public, such as to be prejudicial to the author’s honour or reputation.⁷³ Nevertheless, though narrow in scope and application, certain modifications, especially those that affect the style and rhythm of sentences, perhaps even introduce errors or change the play of words, could arguably fall within the Common Law right, if they reflect poorly on the author, such as to affect the author’s honour or reputation. The difficulty is that this would have to be assessed on a case-by-case basis.

5.3 FICTION VS NON-FICTION

Digital text-watermarking is currently anticipated for non-fiction. Naturally, the questions raised in the preceding paragraphs are also relevant for textbooks, manuals, news articles etc., and not just fictive works. However, if we presume that the changes to non-fiction works are not significant enough to make the individual versions original works, whether from a Civil Law or Common Law perspective, then it is probable that there will be few problems within copyright law, as it is unlikely that authors of such works would claim a breach of their moral rights. This is undoubtedly a sweeping generalisation. For example, an author of an academic textbook may feel the same way about his/her work as the author of a fictive novel.

Here a difference may play out in our Civil Law and Common Law comparison, as illustrated in Table 1. Because Civil Law jurisdictions focus on the “integrity of the work”, it is unlikely that it matters whether a work is fiction or non-fiction. Any modification to any text could potentially affect the integrity of the work as the author’s personality (as reflected in the work) might get harmed in both cases. Be it that a non-fictive work demands a similar amount of author creativity as a fictive one, the right of integrity guarantees that the work in both cases is and remains exactly as the author made it, thereby excluding any changes by third parties whatsoever “irrespective of whether these changes improve or negatively impact on the author’s honour or reputation”.⁷⁴ This is possibly different in Common Law jurisdictions because of the objective perspective on the “honour and reputation of the author” and not the work per se. It is arguable that, from this perspective, the type of change made becomes relevant relative to the type of work it is made to. For non-fictive

⁷¹ Indeed, the US barely knows moral rights.

⁷² This difference has been particularly pointed out with respect to the use of moral rights to meet the interests of indigenous peoples; see WIPO IGC, Secretariat, ‘Glossary of Key Terms Related to Intellectual Property and Genetic Resources, Traditional Knowledge and Traditional Cultural Expressions’, Nineteenth Session (WIPO Doc. WIPO/GRTKF/IC/22/INF/8, 2012), annex, at p. 22. See also Susy Frankel, ‘Towards a Sound New Zealand Intellectual Property Law’ (2001) *Victoria University of Wellington Law Review*, 32, pp. 47-73, at p. 69.

⁷³ *Tidy v Trustees of the Natural History Museum* (1996) 39 IPR 501; and *Pasterfield v Denham* (1999) FSR 168, at p. 182 Overend J (Plymouth county court).

⁷⁴ De Werra, ‘The Moral Right of Integrity’, *supra* note 68, at p. 269.

works, changes in style and syntax may not so greatly impact on the honour and reputation of an author, whereas alterations that affect semantics or correctness may. In contrast, for fictive works, errors are not so dire for the honour and reputation of an author, but modifications that affect style, syntax or semantics may be.

Table 1: Civil Law vs Common Law Comparison for Fiction or Non-Fiction Works

	Fiction	Non-Fiction
Civil Law “integrity of the work”	Changes in semantics, introduction of errors, as well as changes that affect style and syntax.	Changes in semantics, introduction of errors, as well as changes that affect style and syntax.
Common Law “honour and reputation of the author”	Changes that affect style, syntax or semantics.	Modifications that change semantics or introduce errors.

Nevertheless, questions relating to whether a version could be an original work and whether there could be a moral rights issue can only be answered on a case-by-case basis. Moreover, all types of changes listed in the above table can affect more than moral rights of authors – irrespective of the copyright/droit d’auteur divide. As we have argued above, there is also a public rather than private interest of audiences that they know which work they are referring to when receiving/discussing its social and cultural meaning.

6. CONCLUSION

Digital text-watermarking is not perfect. Developers themselves have acknowledged certain limitations.⁷⁵ As an illustration, when an adjective qualifies a noun, the algorithm may make introduce an error, e.g. “private military and army personnel” cannot be changed to “private army and military personnel”, as “private” qualifies “military”. Furthermore, the shorter the text, the fewer modification possibilities there are. Cory Doctorow has further criticised the technology, saying that it would not be difficult to make a text non-identifiable simply by taking two or more versions, comparing them, noting the differences and randomly varying them.⁷⁶ Thus, although digital text-watermarking cannot be hacked, it can be circumvented as a version can be altered such that the copyright owners can no longer track the version back to the original purchaser.⁷⁷ He has further argued that knowing who purchased a work does not necessarily tell us who is legally liable for a

⁷⁵ Avni and Steinebach, supra note 45, at pp. 288-289.

⁷⁶ Cory Doctorow, ‘Lost in Translation: Why a Supposed German Breakthrough in E-book DRM is Just as Dumb as the Old E-book DRM’ (2013) *Publishers Weekly*, 260 (27), p. 15.

⁷⁷ Though this depends on the sophistication of the modification, as it is often possible to track changes made to electronic documents.

breach of copyright.⁷⁸ Both of these arguments are true. However, keeping in mind that no technology is or can represent “perfect enforcement” (whatever that might mean), the more relevant point may be that the technology creates a disincentive to infringe copyrighted works without removing free choice from users to access or use the work however they wish, the discretion of copyright owners, or the possibility of judicial scrutiny. As it is not a technology that affects access or use of works, its impact on freedom of information and expression are considerably minimised compared to existing DRM. Similarly, because the technology is not tethered, but only a means to trace use *ex post*, it has only nominal effects on issues pertaining to privacy and anonymity. In other words, we should be looking at the overall balance a technology creates rather than searching for a perfect technology. With the overall balance in mind, we should be concerned with digital text-watermarking’s disregard for the moral rights of authors and the importance of exact expression, which we sometimes need in order to understand something exactly the way it should be understood and to share expressions that are common to all. From that perspective existing DRM seems advantageous as it guarantees information immutability by “ensuring the integrity of documents, images and music”.⁷⁹

⁷⁸ Doctorow, *supra* note 76, at p. 15.

⁷⁹ Kenneth W. Dam, ‘Self-Help in the Digital Jungle’ (1999) *Journal of Legal Studies*, 28(2), pp. 393-412, at p. 405; see Yu, *supra* note 47, at p. 899.