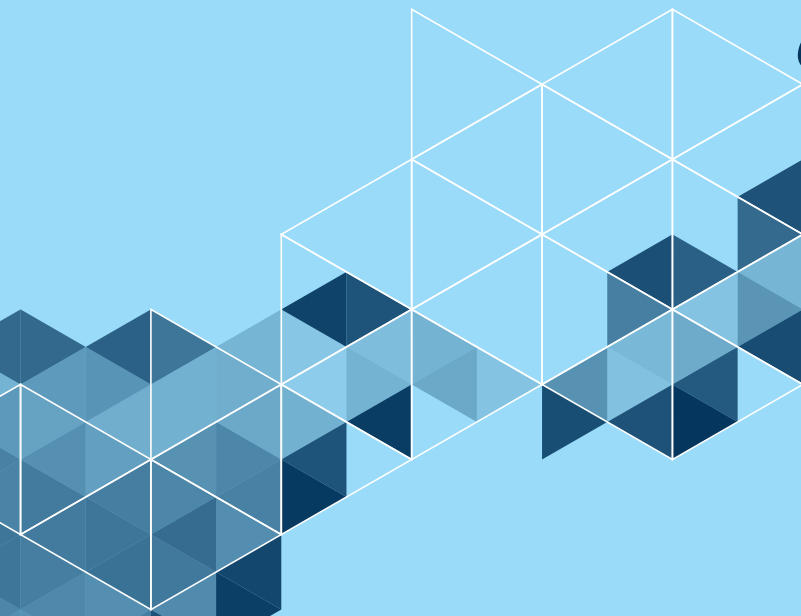


# TECHNOLOGICAL PROTECTION MEASURES AND THE LAW

## Impacts on Research Education & Preservation

Anthony D. Rosborough



Knowledge  
Rights  
21

21<sup>st</sup> Century Access  
to Culture, Learning  
& Research



# CREDITS

## Organisation

This study was done in collaboration with the CREATE Centre, University of Glasgow, UK.

## Author & Organisational Affiliation:

**Anthony D. Rosborough**, Assistant Professor of Law & Computer Science at Dalhousie University and Doctoral Researcher at the European University Institute.

## Reviewers

**Benjamin White**, CIPPM, Bournemouth University, Knowledge Rights 21

**Stephen Wyber**, International Federation of Library Associations and Institutions (IFLA), Knowledge Rights 21

**Design** SPRESSO design studio, The Hague; Square-up Agency, Brussels

## Funding

The publication is issued as part of the Knowledge Rights 21 project, funded by Arcadia – a charitable fund of Lisbet Rausing and Peter Baldwin.

[www.knowledgerights21.org](http://www.knowledgerights21.org)    [www.arcadiahfund.org.uk](http://www.arcadiahfund.org.uk)

## Legal Disclaimer

The information in this report is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. Neither the authors of the report nor the organisations involved in its creation shall bear liability for damages of any kind, including, without limitation, direct, special, indirect, or consequential damages that may result from the use of these materials, subject to any liability which is mandatory due to applicable law.

## Creative Commons

This publication is available under the Creative Commons Attribution 4.0 International licence. You are free to share, copy and redistribute this material in any medium or format, and adapt, remix, transform, and build upon the material for any purpose, even commercially, provided you give appropriate credit.

©Anthony D. Rosborough    ©Knowledge Rights 21

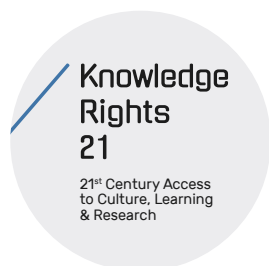
## Visuals by [Unsplash](https://unsplash.com/)

Nonexclusive, worldwide copyright license to download, copy, modify, distribute, perform, and use images, including for commercial purposes, without permission from or attributing the photographer or Unsplash.



# ACKNOWLEDGEMENTS

This study was funded by Arcadia – a charitable fund of Lisbet Rausing and Peter Baldwin, through the Knowledge Rights 21 (KR21) programme of the Stichting IFLA Foundation.



## **Knowledge Rights 21**

Knowledge Rights 21 is focused on bringing about changes in legislation and practice across Europe that will strengthen the right of all to knowledge. It is built on a conviction that access to knowledge is essential for education, innovation and research, and that everyone in society should have the possibility to access and use information in both analogue and digital forms. This, in turn, will help Europe deliver on its economic, social, environmental and democratic potential.

This study does not constitute legal advice, and any views expressed are those of the author. Any institution or other entity wishing to use the findings of the study should consult a copyright lawyer on the findings herein. All information is provided in good faith for guidance and reference purposes only. It is of a general informational and educational nature, and the publishers and authors take no legal responsibility for the accuracy of the information provided, nor for any loss or damage resulting from any such information.

## **About the Three Reports:**

This report is the first in a three-part series assessing the legal status and providing evidence on Technological Protection Measures (TPMs). This report provides a comparative doctrinal analysis of TPMs in the 27 Member States of the European Union plus key comparator jurisdictions including the UK. That document contains a detailed analysis of the status of TPMs and copyright exceptions, and different national approaches taken inside and outside of Europe to ensure access to works for beneficiaries of exceptions and limitations to copyright. Report 2 provides evidence on the effects of TPMs for researchers, libraries and archives, gathered from a survey of researchers and institutions. The results offer insight into specific impediments to research, education and preservation, as well as the outcomes of legal requests to rightsholders to provide access. Report 3 provides economic evidence of the costs of dealing with TPMs in the preservation of digital materials. Quantitative data are analysed from the MAME video game emulation project, revealing significant labour costs and missing use arising from the need to circumvent TPMs to preserve digital materials, an issue relevant to a range of digital preservation and research contexts.

# TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	3
ABOUT THE THREE REPORTS.....	3
EXECUTIVE SUMMARY.....	6
INTRODUCTION.....	7
<b>PART ONE: THE IMPACTS OF TECHNOLOGICAL PROTECTION MEASURES ON RESEARCH, EDUCATION, AND PRESERVATION.....</b>	<b>10</b>
<b>A. Research Barriers.....</b>	<b>10</b>
<b>B. Educational Barriers.....</b>	<b>11</b>
<b>C. Preservation Barriers.....</b>	<b>11</b>
<b>PART TWO: OVERVIEW OF TECHNOLOGICAL PROTECTION MEASURES &amp; ANTI-CIRCUMVENTION LAW.....</b>	<b>14</b>
<b>A. Origins &amp; Development of Anti-Circumvention Law.....</b>	<b>14</b>
1. The WIPO Internet Treaties.....	15
2. The Digital Millennium Copyright Act and the "Access Right".....	17
3. The Impact of Free Trade Agreements.....	19
<b>B. Types and Evolution of TPMs.....</b>	<b>20</b>
1. Analogue TPMs.....	21
2. Digital TPMs.....	21
3. Web-Based TPMs.....	23
4. Categories of TPMs According to Prohibited Activities.....	25
<b>PART THREE: COMPARATIVE DOCTRINAL ANALYSIS.....</b>	<b>27</b>
<b>A. Conceptualisation of "TPMs".....</b>	<b>27</b>
<b>B. Prohibited Acts.....</b>	<b>29</b>
1. Private circumvention.....	30
2. Manufacture or Distribution of Circumvention Tools.....	30
3. Circumvention Services.....	31
<b>C. Mens Rea Requirement (Knowledge or Intent).....</b>	<b>35</b>
<b>D. Criminal Penalties.....</b>	<b>37</b>
<b>E. Exceptions &amp; Limitations.....</b>	<b>39</b>
1. EU Member States.....	41
2. Extra-EU Jurisdictions.....	46
<b>F. Obligations on Rightsholders to "Make Available" or Provide Access.....</b>	<b>50</b>
<b>G. Flexibilities &amp; Opportunities for Future Exceptions.....</b>	<b>66</b>
1. EU Member States.....	66
2. Extra-EU Jurisdictions.....	69
3. International Trade Dynamics.....	69
<b>PART FOUR: RECOMMENDATIONS.....</b>	<b>72</b>
CONCLUSIONS.....	73





# EXECUTIVE SUMMARY

**This report provides an analysis of Technological Protection Measures (TPMs) and their impacts on copyright law across various European and non-European jurisdictions, with a specific focus on the implications for research, education, and preservation activities carried out by organisations like libraries, archives, and museums.**

TPMs, originally developed to curtail digital content from being copied or accessed unlawfully, have increasingly affected legitimate activities that rely on exceptions and limitations to copyright. Among these activities are Text and Data Mining (TDM), scholarly research, and the preservation of cultural heritage materials and works. The report highlights the widening gap between the assurances and freedoms provided by copyright exceptions and the practical realities faced by users, particularly in the European context. Its attention is focused on the practical application of anticircumvention and TPM-related laws that are shaped by EU directives yet suffer from a lack of harmonisation and effective enforcement of user rights and other guarantees.

The report recommends significant amendments to existing European legal frameworks to better align TPM frameworks in national copyright statutes with public interest objectives. As outlined in Part IV, key recommendations include expanding the scope of permitted circumvention for research-related activities, empowering research organisations to facilitate lawful circumvention, and imposing stricter timelines on rightsholders to provide access to TPM-protected works. The report concludes that without practical means to circumvent TPMs, the legal exceptions and limitations are rendered largely ineffective, necessitating urgent reforms to ensure that TPMs do not undermine research, access to knowledge, and preservation.

# INTRODUCTION

**Concurrent with copyright's foray into the digital environment is a reliance on technical means of protecting works or "technological protection measures" (TPMs). With marginal costs of copying near zero and the relative ease of reproduction and distribution online, rightsholders have since the mid-1990s been engaged in an arms race to suppress the perceived threat of digital technologies in various ways. Key in this battle has been the reliance on TPMs that monitor and enforce policies set by rightsholders. Supplementary to the exclusive rights guaranteed by copyright law, TPMs are tools that technologically enforce copyright (along with private contractual terms) in association with digital works.**

The proliferation of TPMs has also produced numerous externalities, however. In certain instances, TPMs can restrict access and use of copyright works even when the purpose of that access or use is in furtherance of an exception or limitation to copyright. Similarly, TPMs may prevent public domain works from being freely accessed or may prevent non-infringing uses of works as part of analytical processes such as text and data mining (TDM), which may only incidentally touch upon exclusive rights. In other instances, the liability risks involved in circumventing TPMs can restrict activities that are entirely unrelated to copyright, including activities like reverse engineering, security research, and the repair of software-dependent devices.<sup>1</sup>

TPMs therefore allow rightsholders to grant or deny access to information on a relatively individual or privately determined basis, often without regard to lawfully permitted uses or access to works. To an extent, TPMs can be regarded as tools for enforcing contractual override through technologically imposed restrictions. In all, the "public good" nature of information and the near zero marginal costs for rightsholders to invoke and assert TPMs has culminated in legitimate cause for concern about their widespread use and reliance, particularly in relation to digital content that is important for public knowledge, research, and education. These concerns over TPM overreach warrant a deeper look into their prevalence, status, and impacts.

In furtherance of the need for a deeper understanding, this report is the first of three analyses focusing on the impacts of TPMs on research, education, and preservation. The purpose of this report is to provide an overview of the legal status of technological protection measures in the law of select European and comparator jurisdictions, including a brief history and typology of TPMs and their relationship to copyright and related right exceptions. To this end, the primary focus of this report is centred on a doctrinal and comparative analysis of TPMs, including the scope of protections afforded to rightsholders and the applicability of exceptions and limitations to copyright and related rights.

<sup>1</sup> Anthony D Rosborough & Aaron Perzanowski, "Repair as Research: How Copyright Impedes Learning About Devices" (2024), Forthcoming in the Michigan Technology Law Review.



**Part I** of the report begins with a brief overview of the impacts of TPMs and anti-circumvention law on research, education, and preservation. This overview canvasses the common obstacles posed by TPMs as experienced by users and institutions. A more fulsome analysis and articulation of these negative externalities is canvassed in Report 2.

**Part II** of this report then provides an analysis of different technical implementations of TPMs and those most used to protect library and archival works, including a brief survey of the research and educational activities they most commonly prohibit.

**Part III** engages in a doctrinal legal analysis of the legal protection afforded to rightsholders who implement TPMs, along with a look at the potential mitigating or limiting measures at law that may protect the public interest. Overall, the report's analytical focus is centred on TPMs in the European context but draws insights from approaches to anti-circumvention laws implemented elsewhere for guidance. The report concludes with suggestions for how the EU's TPM framework could be made more responsive to copyright users and those seeking to avail themselves of various exceptions and limitations.





Georges Tasios / Unsplash



# PART ONE: THE IMPACTS OF TECHNOLOGICAL PROTECTION MEASURES ON RESEARCH, EDUCATION, AND PRESERVATION

**Over the past several decades, TPMs have created significant and disproportionate challenges for public-interest uses of copyright works. Though TPMs were devised to restrict unlawful uses of copyright works, there has since been a growing recognition of their tendency to primarily restrict lawful uses and their relatively low efficacy in preventing infringement.<sup>2</sup> Importantly, libraries, museums and archives are key institutions for public-interest uses of copyright materials. They play a crucial role in the preservation and dissemination of knowledge, and increasingly find themselves constrained by TPMs in ways that limit their capability to facilitate research.**

## A. RESEARCH BARRIERS

One of the primary functions of research organisations is to support scholarly research by providing access to vast collections of digital content. However, TPMs often restrict the ability of these organisations to fulfil this role effectively. For instance, TPMs may prevent libraries from lending e-books or may limit the number of times a digital work can be accessed, copied, or printed, impeding scholars from thoroughly engaging with the content in a manner necessary for their research projects.<sup>3</sup>

Text and data mining (TDM) is another example of a research activity that is faced with TPM-enabled restrictions. TDM is increasingly important for researchers in fields such as digital humanities, social sciences, and scientific research, where large datasets are analysed to uncover patterns, trends, and insights. However, TPMs often prevent researchers from legally accessing and extracting data from original digital texts, even when such activities would fall under copyright exceptions or fair use/fair dealing provisions. This restriction can severely limit the scope and depth of research, forcing scholars to work with incomplete data or to seek out costly and time-consuming licences for content that should otherwise be freely accessible for academic and scientific research purposes.

It is for these latter reasons that TPMs can also create disparities in research capabilities between well-funded institutions and those with fewer resources. While larger organisations may be able to negotiate licences that allow for the circumvention of TPMs for TDM purposes, smaller institutions often cannot, leading to an uneven playing field among researchers. This inequality can undermine the collaborative nature of academic and scientific research and, in the long run, may result in a less diverse and representative body of scholarly work.

<sup>2</sup> See e.g. Carys Craig, "Locking Out Lawful Users: Fair Dealing and Anti-Circumvention in Bill C-32" in Michael Geist, ed, *From "Radical Extremism" to "Balanced Copyright"* (Toronto: Irwin Law, 2010) at pp. 177–203.

<sup>3</sup> For an overview of our empirical findings with respect to these impacts, see Report 2, Parts 4 and 4.1 in particular. These empirical findings reveal that libraries, archives, and research support institutions face significant barriers caused by TPMs and are left with little guidance or assistance in dealing with TPMs that appear to override assurances and freedoms offered by copyright exceptions.

## **B. EDUCATIONAL BARRIERS**

In the realm of education, TPMs have similarly restrictive effects. Educators and students rely on access to digital resources for classroom instruction, homework, and independent study. But TPMs can prevent the copying, sharing, or even viewing of digital content in ways that are essential for educational use. For example, TPMs may limit the ability of educators to share excerpts of e-books or media with students, or to use these materials in online learning environments. In the wake of the COVID-19 pandemic, the impact of these restrictions has become palpable and of deep concern to educators.<sup>4</sup>

TPMs can also restrict the ability to create accessible educational materials for students with disabilities. For example, a digital textbook protected by a TPM may not be convertible into a format that is compatible with screen readers, leaving visually impaired students without the necessary resources for their studies. While there are widely adopted legal exceptions intended to address these issues (discussed further in this report), the presence of TPMs can still create practical barriers, as circumventing them can be often technically difficult and require expertise and know-how that is not widely held.

The lack of flexibility allowed by TPMs creates further challenges in educational settings. While, for example, terms of a licence agreement may be negotiated, TPMs often operate autonomously and automatically. This creates challenges for teachers seeking to adapt materials to suit the needs of their students, such as by compiling a digital course packet from various sources. TPMs can prevent such adaptations and compilations, requiring educators to find alternative materials or to take other self-help measures that detracts from time that could be better spent on instruction and curriculum development.

## **C. PRESERVATION BARRIERS**

Non-commercial organisations like libraries, museums, and archives are often tasked with the preservation of knowledge and cultural heritage. In the digital age, this involves not only storing physical objects like books, art, and audio tapes, but also ensuring the long-term accessibility of digital content. TPMs, however, pose significant obstacles to such preservation efforts.

In addition to broader preservation challenges posed by copyright in the digital environment, digital content protected by TPMs can become even further inaccessible as technology evolves.<sup>5</sup> For example, a digital work protected by a certain type of TPM may not be viewable on future devices if the technology that the TPM itself is using becomes obsolete. This situation can lead to a loss of access to culturally and historically significant materials, undermining the preservation mission of these institutions. In a similar vein, TPMs can prevent archivists from creating backup copies of digital content or from migrating data to newer formats, increasing the risk of digital decay or loss over time.

<sup>4</sup> For a more complete articulation of the challenges faced by educators and educational institutions in relation to TPMs, please see Report 2, Part 2.2 “accessibility, teaching and learning”.

<sup>5</sup> For an overview of the challenges to preserving digital materials arising from copyright law and TPMs, see Report 3, Part 2.1 “Impediments to Digital Preservation arising from Copyright”.

Further challenges to preservation arise from the legal uncertainties surrounding the circumvention of TPMs for archival purposes. Even where exceptions exist, such as those often provided for libraries and archives under copyright law, the risk of legal action or disputes with publishers can deter institutions from undertaking necessary preservation work. This legal ambiguity and low appetite for risk forces many organisations to err on the side of caution, potentially sacrificing important preservation activities and deciding to not provide access to what has been preserved to avoid the risk of litigation.

Overall, the impact of TPMs on organisations engaged in research, education, and preservation is far reaching and multifaceted. Though TPMs theoretically serve the function of preventing unauthorised use of copyrighted works, their implementation and practical effect often hinders the very activities that these institutions are meant to support and encourage. To address these challenges, there is a growing need for legal reforms and the development of more flexible TPM implementations that more appropriately balance the rights of content creators with the public's interest in access to knowledge, culture, and the necessary inputs for scholarly and scientific research.





Alexi Ruban / Unsplash



# PART TWO: OVERVIEW OF TECHNOLOGICAL PROTECTION MEASURES & ANTI-CIRCUMVENTION LAW

## A. ORIGINS & DEVELOPMENT OF ANTI-CIRCUMVENTION LAW

The beginning of anti-circumvention law is often understood to be the signing of the 1996 WIPO Internet Treaties. However, earlier and concurrent legal developments taking place during the late 1980s in the United States and Europe foreshadowed and strongly influenced the enshrinement at the international level. Throughout the 1980s, the United States recording industry was at war with consumers,<sup>7</sup> resulting in largely failed attempts to rein in unauthorised home copying of audio works with legislation such as the *Audio Home Recording Act*.<sup>7</sup> The challenges posed by digital technologies led to the Clinton administration's creation of the Information Infrastructure Task Force (IITF) in 1993 which developed a national strategy for intellectual property. In its 1995 report, the IITF recommended the recognition of technological protection measures within copyright law, including prohibitions on circumvention and activities that facilitate or support it.<sup>8</sup> Despite enormous pushback to this approach from public interest groups and other stakeholders at the time, the IITF's recommended approach was adopted by the United States Trade Representative (USTR) in its efforts to build international consensus as part of the WIPO treaty negotiations. This approach recognised that technological solutions alone could not neutralise the perceived threat posed by digital technologies, and what was needed was a comprehensive framework within copyright law that protects certain technologies and formats while prohibiting certain activities and uses of competing technologies or devices.

In Europe, anti-circumvention law had an earlier, yet more benign, start. In contrast to the United States' quest to neutralise threats perceived by the recording and entertainment industries, the impetus for the European recognition of TPMs and anti-circumvention law was focused principally on incentivisation and internal market harmonisation. In the 1980s, European copyright law carried a fragmented and inconsistent approach to protecting computer programs and the lack of harmonisation risked stunting the growth of a European software industry.

<sup>6</sup> In the late 1980s, there was immense controversy in the United States over the capabilities of the Digital Audio Tape (DAT) format. The fears of the recording and entertainment industries were centred around the DAT format's capability of producing lossless copying by consumers at home. The advent and introduction of this technology acted as the impetus for the United States' Audio Home Recording Act that, in turn, formed the normative basis for the United States' position at the World Intellectual Property Organization just a few years later. For more on this history, see Taro J Kawamura, "Digital Audio Tape Technology: A Formidable Challenge to the American Copyright System" (1989) 4:2 Am U J Int'l L & Pol'y 409 at 410.

<sup>7</sup> 1623, 102d Cong. (1992) (United States).

<sup>8</sup> US, Information Infrastructure Task Force, "Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights" (US Government Printing Office, 1995) [NII Report].

In its 1988 Green Paper on Copyright and the Challenge of Technology – Copyright Issues Requiring Immediate Action (the “EC Green Paper”), the European Commission recognised the need for “technical devices” for computer programs and other emerging technologies.<sup>9</sup> The EC Green paper was unclear about whether the preferred solution would be to mandate technical standards for protecting computer programs or to enact legal protections to prevent unauthorised circumvention. What eventually transpired in Directive 91/250/EEC (the “Computer Programs Directive”) was the latter, requiring Member States to provide remedies against “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 unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program”.<sup>10</sup>

Given the infancy of the European software industry, the Computer Programs Directive’s anti-circumvention provisions were largely uncontroversial at the time. The distinct legal status for computer programs relative to other copyright works and the relatively narrow application of anti-circumvention within the broader copyright system also left little reason for pushback from public interest or civil society groups. Yet, while narrow in scope, the Computer Programs Directive’s recognition of TPMs and anti-circumvention was sufficient for EU lawmakers to become acquainted with the notion of technological protection as part of copyright law. The European and American approaches to anti-circumvention, though diverging in their rationale and impetus, would later prove to be both complementary and highly influential in shaping the international framework at WIPO.

## **1. The WIPO Internet Treaties**

As a precursor to the 1996 WIPO Internet Treaties, the WIPO Committee of Experts on a Possible Protocol to the Berne Convention (the “Committee of Experts”) explored various approaches related to copyright in the emerging digital environment. Among the approaches it explored were legal recognition for “technical devices” and prohibitions on the sale, rental, or unauthorised use of copy-protection circumvention devices. Given the precedents already set in the United States and the European Union, technological protection was regarded as a logical extension of copyright in its adaptation to the digital environment. Early proposals by the Committee of Experts reflected prohibitions on importing, manufacturing and distributing “protection-defeating devices” as well as offering services that have the same effect. Notably missing from these early proposals, however, were prohibitions on the act of circumvention itself.

The discussions and debates that took place at WIPO in response to the Committee of Experts’ various proposals included active engagement and contribution from countries from all continents and regions of the globe. These delegations brought various concerns ranging from disproportionate impacts on developing countries, to overbroad prohibitions on tools or devices that only incidentally aid in circumvention, to the impairment of access to information in libraries and public institutions.<sup>11</sup>

<sup>9</sup> Commission of the European Communities, Green Paper on Copyright and the Challenge of Technology – Copyright Issues Requiring Immediate Action, COM (88) 172 final.

<sup>10</sup> Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs [Computer Programs Directive], Article 7(1)(c).

<sup>11</sup> WIPO Summary Minutes MCI 1996, p. 75–76/para 517.

In the end, the text arrived upon was that which now comprises the similarly worded Articles 11 of the WIPO World Copyright Treaty and Article 18 of the WIPO Performances and Phonograms Treaty. The former provides that:

**“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.”**

Though Article 11’s text permits flexibility in national implementation, it also contains ambiguities that have resulted in highly divergent approaches to anti-circumvention law. Perhaps most prominently, in requiring “adequate legal protection and effective remedies”, Article 11 sets only minimum standards for protection. It leaves significant discretion to national governments to determine, for example, the scope (if any) of lawful exceptions permitting circumvention, the status of existing exceptions and limitations to copyright, or whether “effective remedies” may include criminal penalties.

Secondly, the text of the provision provides little guidance or clarity on the precise activities that fall within the ambit of “circumvention”. Despite early drafts of the provision targeting primarily the manufacturing or distribution of circumvention tools or offering circumvention services (the “preparatory acts”), Article 11 does not provide such specificity. One potential interpretation is that the prohibition on the act of circumvention *per se* was implied from the outset.<sup>12</sup>

Third, the treaty language mandates legal protection against the circumvention of “effective” technological measures without further specificity. As will be explained in Part II, the nebulous concept of “effective” has left an ambiguity in anti-circumvention law that persists today. Though many national lawmakers have attempted to provide legislative clarity on when TPMs are considered effective,<sup>13</sup> the goal of providing certainty remains elusive given the rapid technological change that has taken place over the past several decades.<sup>14</sup>

<sup>12</sup>. Jeffrey P. Cunard, Keith Hill and Chris Barlas Current Developments in the Field of Digital Rights Management Prepared for World Intellectual Property Organization Standing Committee on Copyright and Related Rights Tenth Session, 2003, WIPO document SCCR/10/2 p.46. Available from [http://www.wipo.int/documents/en/meetings/2003/sccr/doc/sccr\\_10\\_2\\_rev.doc](http://www.wipo.int/documents/en/meetings/2003/sccr/doc/sccr_10_2_rev.doc)

<sup>13</sup>. For example, many EU Member States include a standalone definition of when TPMs are considered “effective”. The Netherlands, for example, provides that “Technological measures are deemed to be ‘effective’ where the use of a protected work is controlled by the author or his successors in title through application for an access control or a protection process, such as encryption, scrambling or other transformation of the work or a copy control mechanism which achieves the protection objective”, Copyright Act (2021–2022), s. 29a. This can be contrasted to Canada’s Federal Court, which in *Nintendo v King*, 2017 FC 246 interpreted Canada’s Copyright Act in contrast to that of the United Kingdom, and found that, “... [I]t is clear that access control TPMs do not need to employ any barrier to copying in order to be ‘effective’”.

<sup>14</sup>. Ian Brown, “The evolution of anti-circumvention law” (2006) 20:3 International Review of Law, Computers & Technology 239.

In all, the anti-circumvention language in the WIPO Internet Treaties has left sufficient flexibility to national governments to take quite wide-ranging approaches to TPMs and anti-circumvention law. In one regard, the flexibility and malleability afforded by the WIPO Internet Treaties is a positive attribute. In theory, it allows national governments to tailor anti-circumvention law to suit their domestic political, cultural, economic environments through various exceptions and limitations. To some extent, this is what has occurred; with some jurisdictions devoting only minimal attention to prohibiting circumvention while others have enacted robust, prescriptive rules bolstered by criminal sanctions. But in practice, the flexibility afforded to national governments has enabled less desirable trends. As section 3 of this Part further describes, imprecise treaty language has enabled a gradual ratcheting higher of domestic anti-circumvention laws through successive bilateral and multilateral free trade agreements. The result is a growing global norm of TPMs and anti-circumvention law that is far more restrictive than what is described in the WIPO Internet Treaties.

## **2. The Digital Millennium Copyright Act and the “Access Right”**

In the United States, the process of implementing the WIPO Internet Treaties presented an opportunity to devise a distinct approach to anti-circumvention that embodied the longstanding perceived threat posed by digital technologies held by the recording and entertainment industries. In effect, lawmakers in the United States (and particularly those responsible for developing the US position during the WIPO negotiations) sought to enact stronger protections than what were required by the treaties. The hope had long been to create a more stringent standard that would influence anti-circumvention law’s global implementation. In describing the WIPO treaty standard as the “floor” and the proposed approach to implementation as the “ceiling”, the United States saw itself responsible for taking a leadership position and to provide other countries with a model for technological protection.<sup>15</sup> The result was §1201 of the Digital Millennium Copyright Act.<sup>16</sup>

§1201 implemented the WIPO Internet Treaties with a few improvisations. The first is a clear prohibition on the act of circumvention, including criminal penalties. It further prohibits and invokes criminal penalties for manufacturing, importing, or “trafficking” in circumvention tools or devices, as well as offering circumvention services for others. §1201 includes a collection of exceptions permitting the act of circumvention, but those exceptions do not apply to the provision of circumvention services or so-called trafficking in circumvention tools or devices. As is described further in this report, the tendency for some European Member States to not explicitly prohibit the trafficking in tools presents an opportunity to enact a more balanced approach to anti-circumvention law in Europe that could better account for the public interest in access to information. In contrast, the United States’ approach incorporates only narrow permanent exceptions, including accommodations for law enforcement, enabling accessibility, protecting personal privacy, security testing, and others.

<sup>15</sup>. Bill D Herman & Oscar H Gandy Jr., “Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings” (2006) 24 Cardozo Arts & Entertainment, 120–190 at 134.

<sup>16</sup>. Digital Millennium Copyright Act, 17 USC § 1002(c) (Supp. V 1993) [DMCA].

To account for unforeseen consequences of anti-circumvention law at the time the DMCA was enacted, §1201 includes a periodic review process led by the Librarian of Congress (LoC) known as the “Triennial Review”. This process allows the LoC to issue case-by-case and temporary exemptions permitting certain circumvention activities in relation to certain works or technologies for limited terms of 3 years. As will be further discussed, this periodic exemption approach is distinguishable from the approach taken in the European countries studied. While in some cases these European jurisdictions have complaint and review processes resulting in adjudication of TPM overreach, these processes are generally confined to specific disputes or grievances, and do not result in blanket exemptions. Importantly, the DMCA exemptions apply only to the act of circumvention, and may not extend to offering circumvention services or trafficking in circumvention tools or devices. Since the DMCA was enacted, numerous §1201 exemptions have been granted by the LoC, including allowing circumvention for excerpts of works for educational purposes by universities or K-12 institutions, access to medical device data, cell phone and mobile device “unlocking”, repair of motorised land vehicles, software preservation, and computer security research.<sup>17</sup> The list of exemptions has grown over the years, with many having been renewed several times.

The DMCA’s §1201 introduced a new approach to anti-circumvention law that has been globally influential in the years and decades following. The first aspect of this approach is its clear distinction between the act of circumvention and the “preparatory acts” in offering circumvention services or distributing the tools necessary for circumvention. In turn, this impacts the application of exceptions and limitations, which apply only to the former and not to the latter.

Perhaps even more impactful, however is §1201’s conceptualisation of the role and purpose of TPMs as techniques that “effectively control access to a work”. This can be distinguished from the wording found in the WIPO Internet Treaties which provide an explicit reference to the connection between effective technical measures and the exercise of copyright and related rights. Namely, Article 11 of the WIPO World Copyright Treaty refers to “effective technological measures *that are used by authors in connection with the exercise of their rights ... and that restrict acts, in respect of their works, which are not authorized ...*”. Under the WIPO conceptualisation of TPMs, the activities being prohibited by anti-circumvention law must bear some reasonable connection to copyright or related rights. §1201, however, includes no such link and ostensibly allows rightsholders to assert that circumvention, in the absence of any otherwise infringing activity, can be the subject of an independent cause of action or claim. This approach stands in contrast to the conceptualisation in EU directives and within European Member States, which generally require a stronger connection between unauthorised circumvention and infringement of exclusive rights.<sup>18</sup>

<sup>17</sup>. <https://www.govinfo.gov/content/pkg/FR-2021-10-28/pdf/2021-23311.pdf>

<sup>18</sup>. For example, Hungary defines a TPM as “... any device, component, method or technology that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works, which are not authorized by the copyright holder ...” (Act No. LXXVI of 1999 of Copyright, Article 95).

The DMCA's broad conceptualisation of the role and function of a TPM has enabled a much more robust and heavy-handed approach to anti-circumvention in the United States<sup>19</sup> that has been growing internationally, with significant pushback and protest from public interest groups and fair use advocates.<sup>20</sup>

### 3. The Impact of Free Trade Agreements

In contrast to the United States' approach to TPMs that "effectively control access" found in the DMCA, many countries implemented the WIPO Internet Treaties in ways that were much more in line with the treaty text. For example, Australia's initial implementation of the WIPO World Copyright Treaty occurred through the Copyright Amendment (Digital Agenda) Act, 2000.<sup>21</sup> This implementation included a definition of "technological protection measure" as "a device, product, technology or component (including a computer program) that ... in the ordinary course of its operation, prevents, inhibits or restricts the doing of an act comprised in the copyright". Key to this conceptualisation of a TPM is the clear link between the operation of a TPM and acts relevant to the exercise of copyright or related rights. Similarly, the European Union's implementation of the WIPO World Copyright Treaty's Article 11 in Article 6(3) of the Information Society Directive contains a link between the function of TPMs and activities relevant to the exercise of copyright:

／ **"... 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 authorised by the rightholder of any copyright or any right related to copyright as provided for by law ..."**

By describing TPMs as measures that prevent or restrict acts that relate to exclusive rights, this language implies that their effects ought to be measured and balanced in relation to broader exceptions and limitations to copyright. In effect, preserving this connection between prohibited circumvention and rights infringement leaves less room for an interpretation that results in a *sui generis* regime controlling "access" to works. This distinction is key to understanding the distinct approach to anti-circumvention in Europe as compared with the United States. As will be further articulated in Part II, this conceptualisation of TPMs is replicated in many (but not all) EU Member States and countries outside of Europe, permitting exceptions and limitations to copyright to have a more direct impact on the scope of anti-circumvention law.

19. See e.g. *Lexmark International, Inc. v. Static Control Components, Inc.* 572 U.S. 118 (more) 134 S. Ct. 1377; 188 L. Ed. 2d 392 (2012); and *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F. 3d 1178 (2004).

20. Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised" (1999) 14:2 *Berkeley Technology Law Journal* 519-566 at 543.

21. Copyright Amendment (Digital Agenda) Act 2000, Act No. 110 of 2000 as amended (Australia), online: <https://www.legislation.gov.au/C2004A00702/latest/text>



Through successive bilateral and multilateral free trade agreements (FTAs), however, this traditional conceptualisation of TPMs has been slowly replaced by the “effectively controls access” notion found in §1201 of the DMCA. In the case of Australia, for example, the conclusion of the US-Australia Free Trade Agreement (AUSFTA) in 2004 resulted in Australian copyright law’s adoption of a new set of rules for “access control” TPMs, which are defined as “any technology, device, or component that, in the normal course of its operation, controls access to a work ... or protects any copyright”.<sup>22</sup> Through other FTAs, the “access control” TPM approach has since been adopted by a growing number of countries globally.<sup>23</sup> The result is a growing global *de facto* standard that reflects the DMCA-style anti-circumvention law and which reaches significantly beyond what Article 11 of the WIPO World Copyright Treaty requires.

## B. TYPES AND EVOLUTION OF TPMS

The previous section makes clear that “technological protection measures” are principally legal conceptions rather than technical objects or phenomena. Though technical restrictions on accessing and copying protected works of various kinds existed long before they were recognised by copyright law, their legal significance depends entirely on the prohibition on circumvention and related activities. In the absence of circumventing activities, the question of whether a specific technique or measure constitutes a “TPM” is entirely immaterial to copyright law. This explains why there is currently no exhaustive list or limitation on what constitutes a “TPM” in any jurisdiction. And for the same reason, with only a few exceptions,<sup>24</sup> there is generally no requirement or obligation on rightsholders to declare or give notice of TPMs used in association with copyright content or the devices in which it is embedded or played.<sup>25</sup> Likewise, there is also no formal registry or prescribed list of technical devices, systems, designs, or specifications that must be followed for a protective measure to be considered a “TPM”. In general, their only formal requirement is that they must be “effective”.

Given the nearly 30 years that have passed since TPMs were incorporated into copyright laws, rightsholders and device manufacturers have in practice relied on many different techniques and protection schemes to safeguard works from unauthorised use and access. Technological advance and changes in the way that copyright works are distributed and accessed have also necessitated changes in approach to technical methods of protection. The following sections provide a high level and brief overview of the technical development of TPMs over the past several decades.

<sup>22</sup>. Copyright Amendment Act 2006, Schedule 12, s 1 (Australia), online: <https://www.legislation.gov.au/C2006A00158/latest/text>

<sup>23</sup>. See e.g. United States-Mexico-Canada Agreement (USMCA), Article 20.66; United States-Chile Free Trade Agreement, Article 17.7(5); United States-Bahrain Free Trade Agreement, Article 14.4(7); United States-Columbia Free Trade Promotion Agreement, Article 16.6(4); The Dominican Republic-Central America FTA (CAFTA-DR), Article 15.5(7); US-Korea Free Trade Agreement (KORUS), Article 18.4(7); Morocco Free Trade Agreement, Article 15.5(8); Oman Free Trade Agreement, Article 15.4(7); US-Panama Trade Promotion Agreement (TPA), Article 15.5(7); Peru Trade Promotion Agreement (PTPA), Article 16.7(4); Singapore Free Trade Agreement, Article 16.4(7).

<sup>24</sup>. See e.g. the approach taken by Slovenia in Part II(F) where rightsholders must place clearly visible markings on each copy of a copyright work in order to receive protection vis-à-vis anti-circumvention law. Furthermore, Germany’s anti-circumvention framework includes a labelling obligation, where “... protected subject-matter protected by a technological measure shall be clearly labelled with information on the characteristics of the technical measures”, further stipulating that any “person who protects works and other protected subject-matter by technological measures shall label these in order to facilitate rights-management and as afforded by the provisions of section 95b(2) with this name or the name of the enterprise and the address to which documents are to be delivered”.

<sup>25</sup>. Pamela Samuelson & Jason Schultz, “Should copyright owners have to give notice of their use of technical protection measures?” (2007) 6 J Telecommun High Technol Law 41–76.

## 1. Analogue TPMs

Before the ubiquity of digital content formats, some of the earliest TPMs were physical or analog controls that prevented unauthorised copying. One example is the Macrovision copy protection incorporated into VHS video cassette tapes dating back to 1985.<sup>26</sup> Analogue video signals are sent from the analogue tape to the screen or display as a series of lines. VHS tapes send not only visible lines that are shown on screen,<sup>27</sup> but also a series of invisible lines that allow the video cassette recorder (VCR) to calibrate the image so that it is displayed properly on screen. Macrovision augmented these invisible video signals in such a way that when a user attempted to record the playback of one VCR using a second (thereby making a reproduction of the tape), the image was scrambled, darker, and resulted in a rolling picture that was difficult to watch.<sup>28</sup>

Beyond the Macrovision system, there are many other antiquated copy protection systems for analog formats that would be considered “TPMs” in a legal sense. An example is the record protection mechanisms on audio cassette tapes. These functioned as small square holes on the bottom of the audio cassette tape which, if present, would instruct the recording device or player to not allow the user to record audio to the tape from another source. It is likely that the most intricate and innovative approaches to analogue copy protection are found in the video game industry, however, where rightsholders have employed a wide range of techniques such as “manual lookup”, puzzle solving, and requiring physical dongles and keys for gameplay.<sup>29</sup> Though all of these analogue protection schemes are far less technically sophisticated than today’s methods of technological protection, they represent some of the earliest technical approaches to preventing unauthorised uses of copyright works.

## 2. Digital TPMs

When it comes to copyright content in digital formats, rightsholders have devised and implemented a vast array of techniques to prevent unauthorised copying and access. At a very basic level, TPMs protecting digital formats can be categorised in two ways: cryptographic methods and “information-hiding” methods.<sup>30</sup> Though this distinction is helpful to understanding the function of TPMs, it should be noted that these approaches to protection are not mutually exclusive, and are often both present as part of a single TPM system or scheme.

<b>CRYPTOGRAPHIC METHODS</b>	► Where access to works is enabled through an access key (e.g. password) to decrypt digital files and information.
<b>INFORMATION-HIDING METHODS</b>	► Where information is stored on or within protected works (e.g. watermarking) to prevent playback on unauthorised devices or limited to specific users (i.e. authentication)

Fig.1 Approaches to protecting digital formats

<sup>26</sup>. <https://cs.stanford.edu/people/eroberts/cs181/projects/1999-00/dmca-2k/macrovision.html> give notice of their use of technical protection measures?” (2007) 6 J Telecommun High Technol Law 41–76.

<sup>27</sup>. Dan Maloney, “Rolling old school with copy protection from the 1980s” (27 May 2018), Hackaday, online: <https://hackaday.com/2018/05/27/rolling-old-school-with-copy-protection-from-the-1980s/>

<sup>28</sup>. For an excellent overview of Macrovision and how it functions on technical level, see Technology Connections, “The Copy Protection in VHS” (13 May 2018), YouTube, online: [https://www.youtube.com/watch?v=-VqsU1VK3mU&ab\\_channel=TechnologyConnections](https://www.youtube.com/watch?v=-VqsU1VK3mU&ab_channel=TechnologyConnections)

<sup>29</sup>. For a more detailed overview of the types of protection systems used by video game developers and studios, see Report 3, Part 5 “Results”, where a number of circumvention activities necessary for video game preservation are outlined, including microprocessor “decapping”, and simulation or “spoofing”. For a brief history of video game copy protection, see also, Lazy Gamer Reviews, “The History of DRM & Copy Protection Schemes” (27 October 2012), YouTube, online: [https://www.youtube.com/watch?v=HjEbpMgiL7U&ab\\_channel=LGR](https://www.youtube.com/watch?v=HjEbpMgiL7U&ab_channel=LGR)

<sup>30</sup>. Poonam Kadian et al., “Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey” (2021) 118 Wireless Personal Communications 3225–3249.

One of the earliest systems for information hiding was introduced as part of digital audio tape (DAT) formats. This included the largely unsuccessful “copycode” system, as well as the Serial Copy Management System (SCMS).<sup>31</sup> The latter system worked by marking “first generation” copies of audio tapes by adding an additional (inaudible) digital signal. For first generation copies, this additional signal would remain inaudible, but further “second generation” copies would be interrupted and distorted by it. As part of the 1987 Digital Audio Recorder Act (DARA) in the United States, technology manufacturers responsible for producing DAT devices and tapes were obligated to incorporate these information-hiding systems into the design of their products.<sup>32</sup>

Though digital formats have moved far beyond the DAT format and physical media, similar information-hiding techniques have been deployed in the years and decades since. Not unlike the SCMS, rightsholders often include instructions in digital file formats that dictate how the work can be accessed, used, and distributed. An example of this is Apple’s implementation of the Advanced Audio Coding (AAC) on its iTunes and iPod products known as “FairPlay”. The AAC standard was intended to replace the MP3 format through superior sound quality, but it also permitted additional layers of encrypted information to be stored within audio files. Apple’s FairPlay system devoted one of the encrypted AAC audio layers to store user information, track the number of times the file had been reproduced, and limited the number of devices it could be played upon.<sup>33</sup> FairPlay became infamous and eventually the subject of a class-action suit<sup>34</sup> for limiting device compatibility and restricting the use of purchased music files through iTunes to only Apple’s iPod device; thereby impairing fair competition.<sup>35</sup> Though FairPlay was much more sophisticated than the SCMS, it invoked similar concepts through attaching data to files embodying copyright works that limit what can be done with the original or copies, or restrict uses to view or listen only. Techniques similar to FairPlay remain commonplace in the video game industry<sup>36</sup> and for specialised software and embedded systems used in some industrial and commercial settings.<sup>37</sup>

In addition to information-hiding methods, TPM systems may also protect digital works through various implementations of cryptography. These systems borrow from general information security techniques to manage use and access to works, including unauthorised

31. Taro J Kawamura, “Digital Audio Tape Technology: A Formidable Challenge to the American Copyright System” (1989) 4:2 Am U J Int’l L & Pol’y 409 at 410.

32. Peter F Drahos and John Braithwaite, *Information Feudalism* (The New Press, 2002) at 183.

33. William Fisher, “iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media” (2004) Berkman Klein Center for Internet & Society Research Publication, online: <https://dash.harvard.edu/bitstream/handle/1/32866386/iTunesWhitePaper0604.pdf>

34. Jordan Golson, “iPod Lawsuit Against Apple Given Class-Action Status” (9 May 2012), MacRumors, online: <https://www.macrumors.com/2012/05/09/ipod-lawsuit-against-apple-given-class-action-status/>

35. It should be noted that Apple is not alone in its creation of a proprietary file format that restricts interoperability and access using third party devices or platforms. For example, Amazon and Adobe have each developed their own proprietary file formats to control unauthorised use and distribution of e-books and other files. Common among these systems for protecting text-based and literary works is a technique known as “watermarking”. This embeds the user’s personal information and other details into the metadata of the file so that it is visible once shared or distributed to others and can be used to track unauthorised reproduction. For a more detailed explanation of forensic watermarking in streaming and cloud-based content, see section 3 of this Part.

36. CREATE, “Video Game Preservation and Copyright TPMs Explorer” (Accessed 11 May 2024), online: <https://www.create.ac.uk/public-domain/video-game-preservation-and-copyright-tpms-explorer/>

37. For example, many software-dependent medical devices can only be serviced or repaired if the user can access “Service Mode” or the “Service Menu”. This requires authentication using a service password or service key to decrypt information stored on the devices. Robust websites have been built that instruct users on how to receive service passwords for devices such as CT Scanners and MRI Scanners. These resources are often essential in situations where the device manufacturer is no longer in business and able to provide support to technicians. <https://www.service-password.com/>

reproduction or distribution.

One common example is the Portable Document Format (PDF), which is often used to store and transmit literary works protected by copyright in addition to sensitive or confidential information. PDF documents can be protected from unauthorised access and infringement of copyright through password-based encryption and digital signatures that validate authenticity and permissions through cryptography.

Providing a comprehensive overview of encryption technologies is far beyond the scope of this report, but in broad terms encryption-based rights protection schemes store protected content in secure formats that must be decoded to be accessed, viewed/played, or reproduced. The two basic encryption techniques for copyright protection are “symmetric encryption” and “asymmetric encryption”.<sup>38</sup> The former relies on a private key (i.e. a password) for decryption which is shared by both the sender and receiver. Asymmetric encryption (commonly referred to as “public-key encryption”) incorporates two distinct but mathematically related keys. A public key encrypts the content while a series of individually assigned private keys can decrypt it. This allows for validation and verification to many authenticated users.

In either case, TPM systems invoking cryptography are more commonly referred to as forms of Digital Rights Management (DRM) because they often include both a rights enforcement and rights management function. This allows rightsholders to not only prevent certain unauthorised uses, but track and manage the scope of permitted ones. These systems vary widely in their technical elements and characteristics depending on the business model and commercial environment.<sup>39</sup>

### **3. Web-Based TPMs**

Concurrent with the rise of Web 2.0 has been a transformation of the technical foundations for accessing and using copyright works. In general, this transformation has resulted in a movement away from downloadable or independently executable files storing copyright works, to web-based applications and “streaming” content. Included in this collection of content is digital audio, video, images, text, and even 3D models. Whether viewed and accessed on YouTube or Apple Music or more institutional scholarly publishing platforms, cloud-hosted and web-based content have increasingly become the norm.<sup>40</sup> This shift from “files” to “platforms” has enabled a corresponding transformation in the common methods and techniques for protection and controlling use by rightsholders and content platforms. From a copyright protection perspective, the switch to clouds and streams from independently executable files offers advantages. Even very robust asymmetric cryptographic methods for rights protection result in vulnerabilities once the file has been decrypted. Once the file, message, or content has been decoded, it is no longer secure and may be reproduced, distributed, or used and accessed outside of the TPM scheme. Cloud-hosted streaming content avoids exposing independently executable files to these vulnerabilities.

<sup>38</sup>. Hsiu-Feng Lin et al., “A Copyright Protection Scheme Based on PDF” (2013) 9:1 International Journal of Innovative Computing, Information and Control 1–16 at 1.

<sup>39</sup>. Neils Rump, “Definition, Aspects, and Overview” in Eberhard Becker et al., (eds), *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (Springer, 2003) at 4.

<sup>40</sup>. Aaron Perzanowski & Jason Schultz, *The End of Ownership* (MIT Press, 2019) at 35–56.

As is the case with Digital TPMs described above, web-based TPMs are implemented using a variety of underlying technologies and techniques. These implementations often combine different approaches. For the purposes of illustration, however, they can be understood as falling along three broad categories: server and file level controls, secure connections, and forensic watermarking.

As is the case with Digital TPMs described above, web-based TPMs are implemented using a variety of underlying technologies and techniques. These implementations often combine different approaches. For the purposes of illustration, however, they can be understood as falling along three broad categories: server and file level controls, secure connections, and forensic watermarking.

<b>SERVER AND FILE LEVEL CONTROLS</b>  <b>SECURE CONNECTION</b>  <b>FORENSIC WATERMARKING</b>	▶ Controlling access to independently executable files stored on a server through user authentication (i.e. username and password).
	▶ Access and viewing of content is facilitated through a trusted execution environment that does not allow the user to download or independently execute the files or information under protection (e.g. streaming platform).
	▶ An information-hiding method incorporating imperceptible images or audio into streaming content where access and viewing capabilities of users can be recorded without authorisation and shared outside of the trusted execution environment. This stored metadata may allow rightsholders to determine the user, time, and internet protocol (IP) address associated with the unauthorised recording and reproduction.

Fig. 2 Web-based TPMs

Perhaps the most rudimentary of web-based approaches to technological protection are server and file level controls. These work by controlling access to the source of copies of works (stored as information or data on servers). To access digital works stored on servers, users will need to provide identification and authentication often in the form of a username and password. A further measure may be to restrict access only to registered users holding accounts with the online platform or service. Included in the category of server and file level controls would be file transfer protocols and hosting platforms that allow access and use within secure digital environments. Examples of these types of platforms range from online content stores such as Google Play or Apple's App Store, to e-commerce platforms hosting paid digital resources like Podia.com<sup>41</sup> or SendOwl.<sup>42</sup> This category may also include the more widely used and free-to-use file hosting platforms like Dropbox or Google Drive.

<sup>41</sup>. <https://www.podia.com/>

<sup>42</sup>. <https://www.sendowl.com/>



More advanced web-based approaches to technological protection allow users to access and view/play copyrighted content through a secure and encrypted connection to online content. This approach is widespread today, being implemented by major subscription-based streaming content platforms like Spotify and Netflix, but also an increasing number of academic and scholarly research databases.<sup>43</sup> In essence, these platforms create a trusted execution environment for content decryption and authentication that is performed in isolation from the rest of a user's system or device. This approach to cloud-hosted streaming content offers rightsholders the advantages of asymmetric encryption while avoiding granting users the opportunity to access the bare, unsecured, files or data that would otherwise be vulnerable to unauthorised reproduction and distribution.

But the advantages of cloud-hosted streaming content are not without their own vulnerabilities. While copyright content is made perceptible to users for viewing or listening, users can deploy various techniques to record or capture these streams and produce independently executable files that are infringing reproductions. These practices are commonly referred to as "stream capture" or "stream ripping", and have been the subject of controversy, scrutiny, and threatened litigation over the past decade.<sup>44</sup> In response to these vulnerabilities, rightsholders have devised a relatively new suite of techniques to track and trace unauthorised reproduction and distribution of streaming content known as "forensic watermarking".

Forensic watermarking builds upon the information-hiding techniques that date back to the early TPMs used to protect copyright works in digital formats. In essence, forensic watermarking adds imperceptible changes to the image, text, audio, video or other media that contains information relating to user identification. The intent behind forensic watermarking is to act as a deterrent and to monitor unauthorised reproduction and distribution of works. One provider of forensic watermarking technologies is ContentArmor, which describes the characteristics of the technology as requiring "fidelity, robustness, throughput, and security".<sup>45</sup> Fidelity refers to the importance of maintaining the quality and fidelity of the work, while robustness refers to the relative difficulty in removing the watermark from the digital content. Though forensic watermarking may not functionally prevent or "protect" copyright works from unauthorised reproduction or distribution, it nevertheless falls within the ambit of TPMs because of its function as "scrambling or other transformation" that achieves a copyright protection objective. The nuances of "effective" TPMs are further canvassed in Part II below.

#### **4. Categories of TPMs According to Prohibited Activities**

In addition to the technology underlying TPMs, they can also be categorised according to their approach to protecting copyright works. At a very high level, TPMs generally fall along two categories relating to the activities they prohibit: copy control TPMs, and access control TPMs. In some cases, this distinction is also laid out clearly in statutory drafting.<sup>46</sup> Nevertheless, at a functional level, the lines between copy controls and access controls can sometimes be unclear. This is because this distinction is primarily legal rather than technical. But in general terms the former prevent infringing activities, while the latter restrict access to content.<sup>47</sup> The following two tables provide a small selection of examples that illustrate the differences between these general branches of TPMs:

<sup>43</sup> See e.g. ProQuest, <https://www.proquest.com/>

<sup>44</sup> Lizzie Plaugic, "Record labels sue popular YouTube audio-ripping site" (28 September 2016) The Verge, online: <https://www.theverge.com/2016/9/27/13076534/youtube-ripping-lawsuit-mp3-sony-universal>

<sup>45</sup> <https://contentarmor.net/forensic-watermarking-technology/>

<sup>46</sup> See e.g. Australia, Japan, Singapore, the United Kingdom

<sup>47</sup> Dean S Marks & Bruce H Turnbull, "Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)", (1999), WCT-WPPT/IMP/3 at 7.



Copy Control TPMs		
Approach	Method	Example
<b>ENCRYPTION</b>	▶ Encrypting digital files to prevent unauthorised duplication without a decryption tool or key	▶ Content Scramble System used on DVDs to encrypt and decrypt scrambled video data
<b>DIGITAL SIGNATURES</b>	▶ Attaching information (also often encrypted) to digital files that stores and records information to verify authenticity and permissions	▶ Adding digital signatures to PDF files or documents that record and manage how many copies or reproductions can be made
<b>WATERMARKING</b>	▶ Embedding imperceptible identifiers into digital files to discourage unauthorised copying or distribution	▶ The Serial Copy Management System (SCMS) developed for use with Digital Audio Tapes (DAT) formats
<b>AUTHENTICATION</b>	▶ Embedded microchips in computer hardware or game consoles that detect officially licensed cartridges or physical media (e.g. optical discs)	▶ Hardware authentication systems incorporated into the circuitry of Sony PlayStation and Nintendo game consoles

Fig. 3 Copy Control TPMs

Access Control TPMs		
Approach	Method	Example
<b>ENCRYPTION</b>	▶ Encrypting digital content to prevent unauthorised users from accessing or interpreting it without the appropriate decryption key	▶ Encryption of data transmitted over a network using a SSL/TLS encryption; requiring unique username and password to access encrypted diagnostic information of a device or system
<b>TIME OR GEOGRAPHIC-BASED RESTRICTIONS</b>	▶ Limited to accessing digital content through the use of set durations based on permission or geographic location of the user	▶ Geo-blocking of online content, IP address filtering, region-specific coding between media and playback devices, time-limited downloads or subscriptions with expiration dates (e.g. e-books)
<b>BIOMETRIC AUTHENTICATION</b>	▶ Using biometric characteristics (fingerprints, facial recognition) to verify the identity of users before granting access to content	▶ Unlocking a smartphone with a fingerprint or facial recognition as a precondition for accessing content

Fig. 4 Access Control TPMs



Nasa / Unsplash

# PART THREE:

## COMPARATIVE DOCTRINAL ANALYSIS

For the reasons outlined in Part One (A)-(B) above, anti-circumvention law has been implemented in countries around the world in different ways. This can be partly attributed to the fact that the WIPO World Copyright Treaty permits quite wide flexibility in implementation, but also the timing of international implementation has taken place over the course of nearly two decades. This has required that national lawmakers look at issues of copyright infringement and digital technologies at different points during their rapid technological development. Providing further influence, the conclusion of bilateral and plurilateral FTAs have determined the timing and approach to various countries' implementation of the WCT.

The following sections canvass the approaches to anti-circumvention law in 35 countries.<sup>48</sup> The majority of these countries are members of the European Union, allowing for an analysis of how various Member States have implemented the requirements of Directive 2001/29/EC (the "InfoSoc Directive") as well as Directive 2019/790 (the "DSM Directive"). But included in this analysis are also a number of other countries outside of the European Union which evidence unique and distinct approaches to anti-circumvention law. These approaches will be discussed in further detail in the proceeding sections.

### A. CONCEPTUALISATION OF "TPMS"

An important component of how anti-circumvention laws are structured is the definition and conceptualisation of a "TPM". Even the name itself, "technological protection measure", is not universally or uniformly used in legislative texts.<sup>49</sup> Some jurisdictions refer to them as "technical measures",<sup>50</sup> while others refer to them as "technological measures".<sup>51</sup> This is illustrative of the wider disharmonisation of EU anti-circumvention law and the lack of consensus of its intended scope and the types of activities it seeks to prohibit.

Most EU Member States have adopted a definition of "technological measure" that mirrors closely what is provided at Article 6(3) of the Information Society Directive. That section states:

“For the purposes of this Directive, the expression ‘technological measures’ means 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 authorised by the rightholder of any copyright or any related right to copyright as provided for by law ...”

<sup>48</sup>. These jurisdictions include Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, New Zealand, Poland, Portugal, Romania, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, The United Kingdom, and the United States.

<sup>49</sup>. The Information Society Directive refers to "technological protection measures" in its preambles, but later refers to "technological measures" in Article 6.

<sup>50</sup>. See e.g. Belgium and Luxembourg

<sup>51</sup>. See e.g. Portugal, The United States, The United Kingdom, Malta, Italy, and Hungary.



This language adheres quite closely to the WIPO World Copyright Treaty's conceptualisation of a TPM at Article 11, where it makes clear that "technological measures" are used by authors "in connection with the exercise of their rights under this Treaty of the Berne Convention ...". For the most part, EU Member States have not strayed too far from the conceptualisation of a TPM found in the Information Society Directive. The Czech Republic's conceptualisation of "technological measures" is a good example of the approach commonly seen across EU Member States. It provides that:

／ **"... technological measures means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works, which are not authorised by the author, if the author can control the use of a protected work through application of an access control or protection process, such as encryption, scrambling or other transformation of the work, or a copy control mechanism ..."**<sup>52</sup>

What is characteristic about this approach to conceptualising a TPM is its stipulation that TPMs are "designed to prevent or restrict acts, in respect of works ...". This maintains a logical connection between the intended function and scope of TPMs to the exercise of copyright and protection of the exclusive rights that comprise it. This can be contrasted with the approach seen in jurisdictions outside of the EU that are much more far-reaching. For example, Canada's definition of a "technological protection measure" (stemming from the DMCA tradition) provides that:

／ **"'technological protection measure' means any effective technology, device or component that, in the ordinary course of its operation ... controls access to a work ... and whose use is authorized by the copyright owner."**<sup>53</sup>

The conceptualisation of a TPM as something that "controls access to a work" has quite significant implications for characterising circumvention and the scope of prohibited activities. In defining a TPM as a technique that "controls access to a work", circumvention may not need to be carried out with an infringing purpose to be deemed unlawful. For these reasons, the "controls access to a work" conceptualisation of TPMs represents the high-water mark for anti-circumvention law in extending to a whole host of activities that may bear little (if any) relationship to copyright or infringement. Accessing software or embedded firmware on a device protected by a password or encryption, for example, may constitute unlawful circumvention even if the purpose is for maintenance or diagnosis of the device rather than use of the copyright work.<sup>54</sup> Of the jurisdictions surveyed, the United States and Canada (embodying the DMCA tradition) show the strongest adherence to this approach.

The European "in respect of works" approach to TPMs and anti-circumvention can be contrasted with the DMCA tradition by limiting its reach to only those acts of circumvention that encroach upon the exclusive economic rights of copyright owners. The practical implications of this are that it is lawful – in theory – for users, libraries, archives, or research organisations in Europe to carry out non-infringing circumvention activities without the assistance or consent of rightsholders.

<sup>52</sup>. Copyright Act (Copyright and Rights Related to Copyright), Article 43 (Czech Republic).

<sup>53</sup>. Copyright Act, RSC 1986 c C-42, s 41.1.

<sup>54</sup>. Anthony D Rosborough, "Unscrewing the Future: The Right to Repair and Circumvention of Software TPMs in the EU" (2020) 11:1 JIPITEC 26.



But as is further outlined in *Report 2*, this may not always be technically or practically feasible given the often sophisticated and highly varied techniques required to circumvent TPMs.<sup>55</sup> In an attempt to resolve this, the European approach encourages Member States to promote “voluntary measures”<sup>56</sup> taken by rightsholders to ensure that users can benefit from exceptions and limitations. As is outlined in this report and further explored in Reports 2 and 3, this approach has produced poor results and dismal participation from rightsholders. Given these dynamics, the primary impediment to a more responsive and user-centric approach to TPMs and anti-circumvention in Europe is wider access to the means of circumvention, including the sharing and distribution of circumvention tools and techniques. Cumulatively, this points to a need to reorient policy at the EU level and throughout Member States on facilitating access to the means of circumvention through channels of distribution that are not dependent on the consent or participation of rightsholders. The nuances of this approach are further articulated in Part IV below.

Looking beyond the United States and Europe, jurisdictions such as Japan, Australia, and Singapore, however, resemble a hybrid approach to their conceptualisation of TPMs. These jurisdictions include distinct concepts and definitions for copy-control measures versus access-control measures. Singapore, for example, distinguishes between a “protection measure” and an “access control measure”. The former is defined as “... any technology, device, or component that ... effectively permits or limits the doing of any act that constitutes a rights infringement”, while “access control measure” is defined as a technique that “effectively controls access to a protected copy”.<sup>57</sup> Under this approach, the “protection measure” more closely resembles what is envisaged in the WIPO World Copyright Treaty, while the “access control measure” goes beyond it.

As will be further described in section E below, these hybrid jurisdictions have also enacted schemes for exceptions and limitations permitting circumvention that create a distinction between lawfully circumventing an “access control measure” versus a “copy control” measure. In viewing the global landscape of anti-circumvention law, these hybrid jurisdictions are instructive for showing the importance of how TPMs are characterised, and the implications of adopting the “effectively controlling access” approach versus the “preventing unauthorised acts in respect of works” approach.

## B. PROHIBITED ACTS

The jurisdictions surveyed also showed distinct approaches to prohibiting circumvention activities. As explained in Part I, this can be attributed partially to the WIPO Copyright Treaty’s lack of specification as to what is meant by “adequate legal protection” and “effective legal remedies”. Of the jurisdictions canvassed, there are generally three prohibited acts in relation to circumvention.<sup>58</sup> Some countries prohibit all three, and others only one or two.

<sup>55</sup>. See e.g. Report 2, Part 4. “Findings: surveys of institutions” (p. 23), where it is shown that individual researchers and institutions resort to circumvention fairly infrequently, citing the practical difficulty in employing many of the required techniques and the legal uncertainty in doing so.

<sup>56</sup>. Information Society Directive, Recitals 51–52.

<sup>57</sup>. Copyright Act, 2021 at ss.422–443 (Singapore).

<sup>58</sup>. In addition to the three prohibited circumvention activities described here, New Zealand also prohibits “publishing information enabling or assisting another person to circumvent”, which is not made explicit in other jurisdictions.

The prohibited activities can be categorised as follows:

## 1. Private circumvention

Private circumvention, for the purposes of this report, refers to the activities or techniques necessary to circumvent a TPM. To be clear, “private circumvention” is not a concept explicitly recognised in copyright statutes or treaties, but it is a helpful concept for understanding the scope of commonly prohibited circumvention activities. Private circumvention is most closely related to the copyright concept of “private copying”, in that it is an otherwise unlawful act carried out for mostly private purposes in an isolated or single instance. For the sake of clarity, private circumvention may occur in organisational or within commercial settings (for example, within a library or public institution), so long as they do not involve assistance, tools, or circumvention devices provided by commercial third parties. The concept of private circumvention is important to establish for the purpose of analysis because, among the jurisdictions canvassed, “circumvention” is rarely defined.<sup>59</sup> This is particularly true within EU Member States. Within the DMCA tradition that influences the approaches of Singapore, Canada, and the United States’ anti-circumvention laws, defining “circumvent” is given more attention, however. Singapore, for example, defines “circumvent” as “... to avoid, bypass, remove, deactivate, descramble ... decrypt ... or otherwise impair” a TPM.

Within the EU context, meanwhile, “private circumvention” is embodied most closely in the obligation on Member States at Article 6(1) of the Information Society Directive. This requires Member States to “... provide adequate legal protection against the circumvention of any effective technological measures ...” A reasonable interpretation of this obligation on Member States is that it implies that the actual act of circumvention is included in “adequate legal protection”, but this is not reflected in national implementations. The Republic of Cyprus and Romania, for example, do not reference private circumvention in their lists of prohibited activities. In the absence of further interpretive guidance, it appears as though private circumvention in the absence of infringement is lawful in these countries. But in any event, given this inconsistency and the need to contrast the act of circumvention from related activities, “private circumvention” remains a useful distinction for categorising the differences in national approaches to anti-circumvention law.

## 2. Manufacture or Distribution of Circumvention Tools

The second activity targeted by most anti-circumvention regimes is the manufacture, sale, importation, or distribution of the means or “tools” necessary for circumvention. This is the first of what is often referred to as “preparatory acts” in that they are secondary activities that support or enable circumvention. In practice this may include the distribution or sale of specialised software for circumvention, or in some cases physical tools or hardware components needed to defeat authentication systems. Apart from Singapore<sup>60</sup> and New Zealand’s limited exception, the manufacture or distribution of circumvention tools is explicitly prohibited in every jurisdiction canvassed as part of this study.<sup>61</sup>

<sup>59.</sup> Within the EU, Poland is one of the few jurisdictions that elaborate upon what “circumvent” means, though only by including “elimination” of a TPM.

<sup>60.</sup> Singapore permits dealing in circumvention “devices” and “services” for most of its prescribed exceptions permitting circumvention of TPMs (access by non-profit libraries for purpose of acquisition, protecting personal information of users, interoperability between computer programs, encryption research, preventing minor access to online material, computer security testing). See Copyright Act 2021, ss. 428–433 (Singapore).

<sup>61.</sup> See New Zealand’s Copyright Act 1994, s. 226D(2), permitting the “making, importation, sale, or letting for hire of a TPM circumvention device to enable ... a qualified person to exercise a permitted act using a TPM circumvention device on behalf of the user of a TPM work”. As further explained in Part II(F), New Zealand’s anti-circumvention framework allowed “qualified persons” to carry out circumvention activities on behalf of others for “permitted uses” (namely, exceptions and limitations to copyright). This exception permitting the making or importation of circumvention devices is limited to persons prescribed by regulation and therefore not a general exception to the prohibition on manufacturing, importing, or distributing tools.

The obligation for EU Member States to include these prohibitions stems from Article 6(2) of the Information Society Directive, which provides (in part) that:

“**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 ... which ... are promoted, advertised or marketed for the purpose of circumvention ...**”

Similar obligations on EU Member States exist in relation to computer programs and stem from Article 7(1)(c) of the Computer Programs Directive, which states:

“**Member States shall provide ... appropriate remedies against a person committing any of the following acts: ... 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 unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.**”

Within the DMCA tradition, the prohibition on the manufacture or distribution of circumvention tools uses similar language. Notably, Canada’s prohibition is worded as follows:

“**No person shall ... manufacture, import, distribute, offer for sale or rental or provide – including by selling or renting – any technology, device or component if (i) the technology, device or component is designed or produced primarily for the purposes of circumventing a technological protection measure ...**”<sup>62</sup>

Overall, the prohibition on manufacturing or distributing circumvention tools represents a core tenet of anti-circumvention law. It is the most consistent category of prohibited acts described in the statutory texts of the jurisdictions canvassed.

### 3. Circumvention Services

The third and final activity that is often the subject of anti-circumvention law is in offering services (particularly on a commercial basis) to others that involves circumventing TPMs. In practice, this relates very closely to the prohibition on the manufacture or distribution of circumvention tools, and in practice, these activities often go hand in hand. Commercial circumvention services are often accompanied by or make use of specialised tools to functionally carry out circumvention. Having said that, it is predictable that some instances of circumvention require only specialised knowledge or commonly available tools or devices, in which cases the provision of circumvention services is often treated as a standalone offence. In the EU, the basis for this prohibition stems from Article 6(2) of the Information Society Directive, which provides that:

<sup>62</sup>. Copyright Act, RSC 1985 c C-42, s 41.1(c) (Canada).

“Member States shall provide adequate legal protection against ... the provision of services which ... are promoted, advertised or marketed for the purpose of circumvention ...”

The prohibition on the “provision of services” generally captures circumstances where TPMs are circumvented for others on a *commercial* basis. Every EU Member State that has implemented Article 6(2) has included a prohibition on offering circumvention services. The Netherlands’s implementation serves as a good example of the approach commonly taken by EU Member States:

1. Any person who circumvents any effective technological measures and knows or reasonably ought to know he is doing so is acting unlawfully.
2. Any person **who provides services** or manufactures, imports, distributes, sells, rents out or advertises devices, products or components or is in the possession of these for commercial purposes, is acting unlawfully if these:
  - a. are **offered, advertised or marketed for the purpose of circumventing** the protective operation of effective technological measures ...”<sup>63</sup>

The prohibition on offering circumvention services is replicated in countries that have adopted the DMCA approach to circumvention as well. In the United States, for example, §1201(a)(2) includes “services” among its conceptualisation of “trafficking”:

3. “No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that –
  - a. is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title ... .”

The foregoing three prohibited activities (private circumvention, manufacturing or distributing circumvention tools, and offering circumvention services) represent the three core activities normally the subject of anti-circumvention laws. The following chart represents the explicit prohibitions of these activities in the jurisdictions canvassed. Where a circumvention activity is not explicitly prohibited, it is left blank:

<sup>63</sup>. Copyright Act (2021–2022), Section 29a (The Netherlands).



Prohibited Circumvention Activities by Jurisdiction			
Jurisdiction	Private Circ	Tools	Servs
Australia	X	X	X
Austria	X	X	X
Belgium	X	X	X
Bulgaria	X	X	X
Canada	X	X	X
Croatia	X	X	X
Republic of Cyprus		X	X
Czech Republic	X	X	X
Denmark	X	X	X
Estonia	X		
Finland	X	X	X
France	X	X	X
Germany	X	X	X
Greece	X	X	X
Hungary	X	X	X
Ireland	X	X	X
Italy		X	X
Japan	X	X	X
Latvia	X	X	X
Lithuania	X	X	X
Luxembourg	X	X	X
Malta	X	X	X
The Netherlands	X	X	X
New Zealand		X	X
Poland	X	X	X
Portugal	X	X	X
Romania		X	X
Singapore	X	X	X
Slovakia	X	X	X
Slovenia	X	X	X
Spain	X	X	X
Sweden	X	X	X
Switzerland	X	X	X
United Kingdom	X	X	X
United States	X	X	X

Fig.5 Prohibited Circumvention Activities by Jurisdiction

## C. *MENS REA* REQUIREMENT (KNOWLEDGE OR INTENT)

Among the debates that took place at WIPO during the negotiation of what became Article 11 of the WIPO World Copyright Treaty, significant focus was dedicated to whether knowledge or intent must be required for circumvention to be unlawful. WIPO participants took various positions on this issue. Eventually, a requirement of “knowledge or reasonable grounds to know” became the position of the European Communities.<sup>64</sup> In effect, this would require rightsholders to prove that not only unauthorised circumvention took place, but that the person carrying it out (or providing tools or services, as the case may be) did so with the actual or constructive knowledge that the activity constituted circumvention. This requirement of *mens rea* – or a mental element necessary to accompany the act of circumvention – raises the evidentiary burden on rightsholders while excluding unintentional or potentially inadvertent circumvention of TPMs.

In the end, the text of Article 11 does not include a *mens rea* requirement, but national approaches vary widely on this question. In general, the jurisdictions following the DMCA tradition do not include a *mens rea* requirement. Certain EU Member States, however, clearly require that circumvention activities be carried out with knowledge or “reasonable grounds to know” that the objective of the activity is to circumvent. Further distinctions can be drawn within the EU between those jurisdictions that have included a *mens rea* requirement for only certain circumvention activities and those who have adopted a more general approach. For example, The Republic of Cyprus requires that a person act “knowingly or having reasonable grounds to know” that the purpose of distributing circumvention tools or offering services are for circumvention to be deemed unlawful, but includes no such condition for private circumvention. Other jurisdictions attach a *mens rea* requirement to all three commonly prohibited acts. The following chart represents the inclusion of *mens rea* caveats in the national approaches canvassed:

<sup>64</sup>. WIPO Summary Minutes MCI 1996, p. 79/para 529.

Requirement of Knowledge or Intent by Jurisdiction		
Jurisdiction	Mens Rea Requirement	Scope
Australia	Yes	Only for “access control technological protection measures”
Austria	Yes	Private circumvention, tools, and services
Belgium	Yes	Private circumvention, tools, and services
Bulgaria	Yes	Private circumvention, tools, and services
Canada	No	
Croatia	Yes	
Republic of Cyprus	Yes	Services and tools only
Czech Republic	No	
Denmark	No	
Estonia	No	
Finland	No	
France	Yes	Services and tools only
Germany	Yes	Private circumvention, tools, and services
Greece	Yes	Private circumvention, tools, and services
Hungary	Yes	Private circumvention, tools, and services
Ireland	No	
Italy	No	
Japan	No	
Latvia	No	
Lithuania	Yes	Private circumvention, tools, and services
Luxembourg	Yes	Private circumvention, tools, and services
Malta	Yes	Private circumvention, tools, and services
The Netherlands	Yes	Private circumvention, tools, and services
New Zealand	Yes	Private, circumvention, tools, services, and “publishing information”
Poland	Yes	Private circumvention, tools, and service
Portugal	No	
Romania	No	
Singapore	No	
Slovakia	Yes	Private circumvention, tools, and services
Slovenia	No	
Spain	Yes	Private circumvention, tools, and services
Sweden	No	
Switzerland	Yes	Private circumvention, tools, and services
United Kingdom	Yes	Private circumvention, tools, and services
United States	No	

Fig.6 Requirement of Knowledge or Intent by Jurisdiction

## D. CRIMINAL PENALTIES

National implementations of anti-circumvention law vary in their interpretation of “effective legal remedies” against the circumvention of TPMs noted in Article 11 of the WIPO World Copyright Treaty. In some instances, unlawful circumvention is treated as its own actionable offence under copyright law and independent from infringement. In other cases, unauthorised circumvention grants rightsholders the same rights as they would have against a person who infringed their copyright. The latter is the approach taken in the UK, for example.<sup>65</sup> But a more significant disparity in legal remedies provided to rightsholders against the circumvention of TPMs is regarding criminal penalties. In many jurisdictions, unlawful circumvention is treated as a criminal offence (that is, punishable by imprisonment in addition to a fine). Other jurisdictions do not specify whether unlawful circumvention is treated as a criminal offence.

The following chart provides a summary of the jurisdictional approach to anti-circumvention and takes note of instances where criminal sanctions (e.g. imprisonment) are made explicit in relation to TPMs and circumvention.

Requirement of Knowledge or Intent by Jurisdiction		
Jurisdiction	Criminal Penalties	Scope
<b>Australia</b>	Yes	Private circumvention, tools, and services (for “access control” TPMs only). 5 years imprisonment and/or fines up to \$60,500.00
<b>Austria</b>	Unspecified	
<b>Belgium</b>	Unspecified	
<b>Bulgaria</b>	Unspecified	
<b>Canada</b>	Yes	Private circumvention, tools, and services
<b>Croatia</b>	Unspecified	
<b>Republic of Cyprus</b>	Yes	Services and tools only. “Liable on conviction to a fine not exceeding thirty thousand pounds ... or to imprisonment for a term not exceeding three (3) years or to both”
<b>Czech Republic</b>	Unspecified	
<b>Denmark</b>	Unspecified	
<b>Estonia</b>	Unspecified	
<b>Finland</b>	Unspecified	
<b>France</b>	Unspecified	
<b>Germany</b>	Yes	Unclear whether this extends to all three prohibited acts. Unlawful circumvention “liable to imprisonment of not more than one year or a fine”, while “in cases where the offender acts on a commercial scale”, criminal penalty “shall be imprisonment of not more than three years or a fine”.

<sup>65</sup>. See e.g. section 296ZA(3) of the Copyright Designs and Patents Act, 1988 (United Kingdom).



<b>Greece</b>	Yes	Private circumvention, tools, and services are “punished by imprisonment of at least one year and a fine of 2.900–15.000 Euro ...”
<b>Hungary</b>	Unspecified	
<b>Ireland</b>	Unspecified	
<b>Italy</b>	Yes	Services and tools “shall be liable to imprisonment of between six months and three years and a fine ...”
<b>Japan</b>	Yes	Private circumvention, services, and tools (in the case of “technological exploitation measures”) punishable by imprisonment for a term of up to three years if a person traffics in circumvention devices or offers commercial circumvention services.
<b>Latvia</b>	Unspecified	
<b>Lithuania</b>	Unspecified	
<b>Luxembourg</b>	Unspecified	
<b>Malta</b>	Unspecified	
<b>The Netherlands</b>	Unspecified	
<b>New Zealand</b>	Yes	Services, tools, and “publishing information” with the intent to infringe copyright
<b>Poland</b>	Yes	Services, tools, and “keeping any [circumvention] equipment or components thereof”
<b>Portugal</b>	Yes	Services and tools, “punishable by up to 6 months imprisonment or a fine of up to 20 days”
<b>Romania</b>	Yes	Services and tools, “shall constitute an offence and be punishable by imprisonment for a term of six months or three years or a fine”
<b>Singapore</b>	Yes	Private circumvention, tools, and services, however certain organisations are exempt from criminal penalties (non-profit library or archive, educational institution, an institution aiding persons with disabilities, or public and non-commercial broadcasting organisation that is prescribed by regulation)
<b>Slovakia</b>	Unspecified	
<b>Slovenia</b>	Unspecified	
<b>Spain</b>	Unspecified	
<b>Sweden</b>	Unspecified	
<b>Switzerland</b>	Unspecified	
<b>United Kingdom</b>	Yes	Services and tools treated as criminal offences
<b>United States</b>	Yes	Private circumvention, tools, and services

Fig.7 Criminal Penalties by Jurisdiction

## **E. EXCEPTIONS & LIMITATIONS**

In addition to criminal and civil penalties, national implementations of anti-circumvention law as part of copyright and related statutes vary widely in the exceptions and limitations made available to users and the public. On this point, it is worth distinguishing the European approach to exceptions and limitations permitting circumvention to that within the DMCA tradition. In the latter, TPMs and anti-circumvention provisions are treated as self-contained frameworks that operate in isolation from the general exceptions and limitations to copyright. This is consistent with the “access control” TPM approach that largely divorces TPMs and the activities they prohibit from copyright infringement. Within this framework, circumvention is permitted for very specific and exhaustive purposes that are independent from general copyright exceptions and limitations.

The European approach, on the other hand, connects the lawfulness of circumvention to a permitted use of a copyright work through general exceptions and limitations. This reflects the “in respect of works” legal conceptualisation of a TPM in the Information Society Directive that implies a logical connection between the acts prohibited by TPMs and the exercise of copyright. This comparison and contrast is important, because the European approach relies on pre-existing or general exceptions and limitations to copyright to structure its TPM and anti-circumvention frameworks, while the DMCA tradition requires a greater emphasis on enacting use-specific and circumvention-specific exemptions for various activities and uses of works. For these reasons, the policy solutions to TPM overreach in Europe may look different from the approaches taken in jurisdictions reflecting the DMCA tradition. This point is elaborated upon further in Part V of this Report.

Irrespective of these structural differences, ostensibly every jurisdiction canvassed has put in place an exception permitting circumvention to assist those with perceptual disabilities, evidencing the impact of the Marrakesh Treaty. Perhaps second-most common is an exception permitting cybersecurity testing or testing the integrity of computer programs. But beyond these general trends, the implementation of exceptions and limitations to anti-circumvention among the jurisdictions canvassed shows a variety of approaches.

The following two sections examine these implementations by looking first to EU Member States, and then to extra-EU jurisdictions. Given the harmonising effect of relevant EU directives, anti-circumvention law across Member States tends to take a similar shape. This harmonisation begins to disappear, however, when we look to jurisdictions that follow the DMCA tradition, for example, as well as other approaches.

### **1. EU Member States**

One key feature of the EU’s anti-circumvention framework is the application of general exceptions and limitations to copyright as the starting point for determining the lawfulness of circumvention. This is laid out in Article 6(4) of the Information Society Directive, which states that: “... 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), 2(e), 3(a), 3(b) or 3(e) the means of benefiting from that exception or limitation ...” Among this list are exceptions key to the work of libraries, archives, museums, and educational institutions, but unfortunately these exceptions are non-mandatory. What this means is that the obligation on Member States to “take appropriate measures to ensure that rightholders make available” will only apply where Member States

have opted to incorporate one or more of these non-mandatory exceptions into their national statutes. The consequence of the Information Society Directive's many optional copyright exceptions is that the related obligations on rightholders to give effect to those exceptions only exist when and where those exceptions have been adopted by a Member State.

The situation is slightly more promising in the case of text and data mining (TDM) conducted by research institutions and for the reproduction of cultural heritage works for preservation purposes. As discussed further below, these activities are specifically targeted by Article 7 of the Digital Single Market (CDSM) Directive. This provision makes clear that in contrast to the non-mandatory exceptions that require Member States to take "appropriate measures" only if adopted nationally, TDM and reproduction of cultural heritage works for preservation purposes mandate Member States to ensure that TPMs do not restrict these activities irrespective of which non-mandatory exceptions they have adopted.

Despite this relatively complex patchwork of overlapping exceptions in various directives, the approach stands in stark contrast to jurisdictions outside of the EU. These jurisdictions more often include a separate and distinct group of exceptions permitting TPM circumvention that are unrelated to the exceptions outlined in a country's copyright legislation. The novelty of the EU approach on this point is important to note because, as is further described in Section F, the applicable exceptions and limitations within EU Member States form the grounds for lawful circumvention. Therefore, the legal guarantees afforded to rightholders who deploy TPMs to protect their works are limited to preventing acts of infringement.

The second point of contrast between the EU and jurisdictions following the DMCA tradition is the notion of requiring Member States to encourage or require that rightholders to take some positive action to facilitate access to works where copyright exceptions or limitations apply. With only minor exception, obligating or "ensuring" that rightholders either enable circumvention or provide the "means to access" works is therefore a distinctly EU (and Information Society Directive, in particular) approach. This framework is initially described at Recital 51, which explains that:

“Member States should *promote voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided for in national law in accordance with this Directive. In the absence of such voluntary measures or agreements within a reasonable period of time, Member States should take appropriate measures to ensure that rightholders provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological measure or by other means.*”

Recognising that merely "promoting voluntary measures" may not produce tangible benefits from a public interest perspective, the Information Society Directive requires that Member States themselves "take appropriate measures" to ensure that effect is given to certain exceptions and limitations. The operative provision of the Directive on this point is Article 6(4).

<sup>65</sup>. Though as will be further discussed in Part F below, New Zealand's system is the closest analogue; permitting a "qualified person" as specified by regulations to circumvent a TPM on behalf of a user seeking to avail themselves of an exception or limitation to copyright.

That provision states (in part):

／ **"... 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), (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.**

**A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to *benefit from the exception or limitation concerned* ..."**

Taken together, a few remarks can be made about these provisions and requirements. The first is a general ambiguity in the notion that states "shall take appropriate measures to ensure" that rightsholders give effect to exceptions and limitations. As is further described in Part F below, Member States have taken quite different approaches to implementing these "appropriate measures". Second, Article 6(4) creates a minimum or mandatory list of exceptions and limitations that Member States *must* ensure effect is given to.<sup>67</sup> Other than the necessity caveat in relation to the private copying exception at Article 5(2)(b), it does not place maximums or limits on other exceptions and limitations that Member States could include as part of their "appropriate measures". In practice, many Member States have gone beyond those explicitly listed in the Information Society Directive. The following table provides a summary of the exceptions and limitations that states have identified as applying to private circumvention activities:

<sup>67</sup>. Namely, 5(2)(a), photocopying; 5(2)(c), reproductions by museums, libraries and archives; 5(2)(d), ephemeral recordings made by broadcasters; 5(2)(e), reproductions of broadcasts by social institutions; 5(3)(a), illustration for teaching or scientific research; 5(3)(b), use for the benefit of people with a disability; or 5(3)(e), use for public security purposes (including law enforcement or national security).



EU Member States & the UK																				
Exceptions and limitations permitting private circumvention according to the Information Society Directive																				
Jurisdiction	5.2 (a)	5.2 (b) <sup>68</sup>	5.2 (c)	5.2 (d)	5.2 (e)	5.3 (a)	5.3 (b)	5.3 (c)	5.3 (d)	5.3 (e)	5.3 (f)	5.3 (g)	5.3 (h)	5.3 (i)	5.3 (j)	5.3 (k)	5.3 (l)	5.3 (m)	5.3 (n)	5.3 (o)
Austria						X	X													
Belgium	X	X	X	X	X	X	X			X										
Bulgaria	X		X	X		X	X			X										
Croatia	X			X		X	X			X										
Rep. of Cyprus			X	X	X	X	X		X	X						X				
Czech Republic	X	X	X	X	X	X	X		X	X										
Denmark			X	X	X	X	X		X	X		X								
Estonia		X	X	X	X	X	X		X	X		X								
Finland			X	X	X	X	X			X										
France	X	X	X			X	X			X									X	
Germany	X	X	X	X	X	X	X			X										
Greece	X	X	X			X	X			X										
Hungary	X	X	X	X		X	X			X										
Ireland		X	X	X			X	X	X	X	X	X	X	X	X	X		X	X	
Italy	X	X	X	X	X	X	X		X											
Latvia			X	X		X		X	X	X									X	
Lithuania	X	X	X	X		X	X			X										
Luxembourg		X	X	X		X	X			X										
Malta	X	X	X	X	X	X	X			X										
The Netherlands	X	X	X	X		X	X			X										
Poland			X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Portugal	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
Romania			X	X	X	X	X			X										
Slovakia	X	X	X	X		X	X			X										
Slovenia	X	X	X	X		X	X			X									X	
Spain		X	X	X		X	X			X										
Sweden			X	X		X	X			X	X									
United Kingdom			X		X	X	X			X				X					X	

Fig.8 Information Society Directive – Exceptions and limitations permitting private circumvention

<sup>68</sup>. This column is highlighted in aquamarine to recognise the caveats placed on permitting circumvention to enable users to benefit from the private copying exception given the “to the extent necessary” caveat in article 6(4) of the Information Society Directive”.

In addition to the exceptions and limitations to copyright as provided in the Information Society Directive, further flexibilities permitting TPM circumvention and obligating to provide access stem from the DSM Directive's text and data mining exception for non-profit educational institutions and cultural heritage institutions. This exception permits copyright and *sui generis* database reproductions, along with an exception to the press publishers right for TDM purposes. This is set out in Article 3, which provides:

**"1. Member States shall provide for an exception to the rights provided for in Article 5(a) and Article 7(1) of Directive 96/9/EC, Article 2 of Directive 2001/29/EC, and Article 15(1) of this Directive for reproductions and extractions *made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research*, text and data mining of works or other subject matter to which they have lawful access.**

**2. Copies of works or other subject matter made in compliance with paragraph 1 *shall be stored with an appropriate level of security* and may be retained for the purposes of scientific research, including for the verification of research results.**

**3. *Rightholders shall be allowed to apply measures to ensure the security and integrity of the networks and databases where the works or other subject matter are hosted. Such measures shall not go beyond what is necessary to achieve that objective.***

**4. Member States shall *encourage rightholders, research organisations and cultural heritage institutions to define commonly agreed best practices concerning the application of the obligation and of the measures referred to in paragraphs 2 and 3 respectively.***"

Article 3 is drafted somewhat confusingly from an anti-circumvention law perspective. On the one hand, Article 3(2) implies an obligation on beneficiaries of the TDM exception to put in place some type of security measure to protected mined works. On the other hand, Article 3(3) places limitations on the purpose and scope of measures that may be used by rightsholders that effectively impede TDM. The logical implication is that this places a limitation on the scope of TPM protection to that which is necessary to ensure the security and integrity of networks and databases. The text of the Article then ends with an unsatisfactory resolution of these ambiguities in calling for rightsholders and beneficiaries of the TDM exception to work together toward "best practices". Though Article 3 does not refer explicitly to "technological measures" (the terminology found in the Information Society Directive and which extends to databases),<sup>69</sup> Recital 7 is helpful in sketching Article 3's overall purpose and intent:

<sup>69</sup>. Information Society Directive, Article 6(3).

**“... The protection of technological measures established in Directive 2001/29/EC remains essential to ensure the protection and the effective exercise of the rights granted to authors and to other rightholders under Union law. Such protection should be maintained while ensuring that the use of technological measures does not prevent the enjoyment of the exceptions and limitations provided for in this Directive ... In the absence of voluntary measures, Member States should take appropriate measures in accordance with the first subparagraph of Article 6(4) of Directive 2001/29/EC, including where works and other subject matter are made available to the public through on-demand services.”**

In effect, Recital 7 makes clear that the TDM exception under Article 3 of the DSM Directive applies also to anti-circumvention. Or, put differently, the mandatory exception for TDM reflected in Article 3 pre-empts anti-circumvention of TPMs. This also extends the scope of the “appropriate measures” that Member States must take to facilitate access or the means of circumvention to include TDM carried out by research organisations and cultural heritage institutions. For the foregoing reasons, those EU Member States that have implemented Article 3 of the DSM Directive are therefore obliged to ensure that rightholders make TPM-protected copyright works, databases, and press publishers’ works available to research organisations and cultural heritage institutions carrying out TDM.

The CDSM Directive’s Article 5 includes further clarifications to the scope of anti-circumvention. It addresses the use of copyrighted works in digital and cross-border teaching activities, allowing educational institutions to use copyrighted works for teaching purposes without needing to obtain explicit permission from rightsholders, under certain conditions. Member States are required to implement this exception but have the flexibility to decide whether educational institutions should pay “fair compensation” to rightsholders. Alternatively, Member States may opt out of the exception altogether if a sufficient licensing scheme is available.<sup>69</sup>

Though Article 5 of the CDSM does not explicitly mention TPMs or circumvention, its implications are significant. If TPMs prevent the use of materials in teaching as permitted under Article 5, Member States are expected to ensure that these measures do not obstruct the exercise of the exception. This is made explicit in the CSDM’s Article 7(2), which connects the requirements found in Article 6(4) of the Information Society Directive to the mandatory education exception at Article 5 of the CDSM. This may involve allowing educational institutions to circumvent TPMs to the extent necessary to use the materials for teaching purposes. For these reasons, Article 5 can be understood as indirectly facilitating the circumvention of TPMs in educational contexts where such actions are necessary to exercise the rights granted under this exemption.

Though many EU Member States have adopted and transposed Articles 3 and 5 of the CDSM into their national copyright laws, not all have. The following table provides an overview of these transpositions:

Transposition/Implementation of Articles 3 and 5 of the CDSM		
Jurisdiction	Implementation of Article 3, CDSM	Implementation of Article 5, CDSM
Austria	X	
Belgium	X	
Bulgaria	X	
Croatia	X	
Rep. of Cyprus	X	
Czech Republic	X	
Denmark	X	
Estonia	X	X
Finland	X	
France	X	X
Germany	X	X
Greece	X	
Hungary	X	X
Ireland	X	
Italy	X	X
Latvia		
Lithuania	X	
Luxembourg	X	
Malta	X	
The Netherlands	X	X
Poland		
Portugal	X	
Romania	X	
Slovakia	X	
Slovenia	X	
Spain		
Sweden	X	
United Kingdom		

Fig.9 Transposition/Implementation of Articles 3 and 5 of the CDSM Directive



It must be noted that the above implementations of Article 5 CDSM have not been harmonious. While Estonia's implementation of the article reflects quite closely the scope of permitted uses in the CDSM, Italy and Hungary, for example embody a more restrictive approach by either applying to a narrow range of copyrightable subject matter or limiting the scope or context of "teaching" where the exception can apply.<sup>70</sup>

As others have pointed out, the extension of Article 6(4) to include the DSM Directive's text and data mining exception may be superficial and unlikely to yield tangible benefits. Article 6(4) as a whole has been criticised for its ambiguity and ineffectiveness in materially benefiting beneficiaries of exceptions and limitations who are barred by TPMs.<sup>71</sup> Much of this inadequacy can be attributed to the fact that Article 6(4) leaves too much discretion and responsibility on Member States to implement. Taking "appropriate measures" is an inherently subjective standard that does not provide sufficient guidance in the face of a rapidly evolving technological landscape and evolving modalities of research. What may be an appropriate standard for providing access in one research context may be wholly inadequate for others. Further, Member States have taken divergent approaches to adopting various exceptions and limitations to copyright, resulting in a complex and difficult to navigate space for users looking to circumvent TPMs for non-infringing purposes. As will be further explored in Section G below, the mechanics of Article 6(4) are left largely to users to figure out in practice, with a scant record of assistance from complaint mechanisms and regulatory bodies.

## 2. Extra-EU Jurisdictions

Outside of the European Union, the exceptions and limitations to anti-circumvention laws shows much greater diversity and variation. Indeed, in the extra-EU jurisdictions studied, the malleability of the WIPO treaty language and absence of a harmonising directive has left significant latitude for states to take their own approaches to implementation. As Professor Jane Ginsburg pointed out nearly two decades ago, the treaty language does not even confine anti-circumvention to copyright law necessarily. The notion of "adequate legal protection" could in fact support solutions from other legislative and regulatory areas of competence.<sup>72</sup> Japan, for example, stands out in this regard for bifurcating its anti-circumvention laws among its copyright legislation<sup>73</sup> and unfair competition legislation.<sup>74</sup> Furthermore, administrative and regulatory processes that permit temporary exemptions (such as the United States' Triennial Review) to anti-circumvention law have allowed for bespoke approaches, such as Singapore's temporary exemption for "ordinary use of obsolete software", and "software with obsolete access dongles".<sup>75</sup> The cumulative effect of these dynamics makes for a more significant challenge in comparing and contrasting various approaches to exceptions and limitations. But despite this heterogeneity, a few common trends can be distilled from the countries studied.

<sup>70</sup>. For an overview of these implementations of the CDSM's Article 5 and its broader goal of modernising copyright exceptions to enable online educational use of materials, see Giulia Priora, Bernd Justin Jütte, Péter Mezei, "Copyright and Digital Teaching Exceptions in the EU: Legislative Developments and Implementation Models of Article 5 of CDSM Directive" (2022) *International Review of Intellectual Property and Competition Law* (IIC) 53, 543–566.

<sup>71</sup>. Thomas Margoni & Martin Kretschmer, "A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology" (2022) 71:8 *GRUR International* 685–701 at 695.

<sup>72</sup>. Jane C Ginsburg, "Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience" (2005) 29 *Collum J L & Arts* 11–37 at 20.

<sup>73</sup>. Copyright Act (Act No 48 of 1970), Act No 30 of 2018 at (xx)-(xxi).

<sup>74</sup>. See e.g. Unfair Competition Prevention Act (Act No 47 of 1993), Act No 33 of 2018 at (xvii)-(xviii) (Japan), although it should be noted that exceptions and limitations permitting circumvention are contained exclusively within Japan's copyright framework.

<sup>75</sup>. Copyright Regulations 2021, No S 882, ss. 93-94 (Singapore).

### *i. General Non-Infringing Uses Exception*

One approach, embodied in New Zealand and Switzerland's frameworks, is to include a general "non-infringing uses exception" permitting private circumvention for any non-infringing use of works. Article 39a(4) of Switzerland's copyright act, for example, provides that:

／ **"The ban on circumvention may not be enforced against those persons who undertake the circumvention exclusively for legally permitted uses."**<sup>76</sup>

Similarly, New Zealand limits the exercise of anti-circumvention laws from preventing or restricting the exercise of a "permitted act", which are the general exceptions and limitations to copyright.<sup>77</sup> In either case, this approach offers advantages from a user rights perspective in that it offers clarity and certainty in containing the scope of anti-circumvention law. This also eliminates the need for piecemeal circumvention-specific exceptions for various activities or uses.

A plausible explanation for why these two countries have been able to adopt this more straightforward approach is the latitude offered by their lack of harmonising instrument (be that something analogous to an EU directive or an FTA including anti-circumvention provisions). In contrast to New Zealand and Switzerland, the other extra-EU jurisdictions studied do not make general exceptions and limitations to copyright applicable to anti-circumvention law or provide a general non-infringing uses exception. They instead rely on self-contained exceptions within anti-circumvention frameworks that are siloed and cordoned off from the more general exceptions and limitations to copyright.<sup>78</sup> Supporting this hypothesis, With the exception of the United Kingdom,<sup>79</sup> these jurisdictions<sup>80</sup> have each concluded a bilateral or plurilateral FTA that has strongly influenced their approach to anti-circumvention exceptions and limitations.

### *ii. Prescribed Exceptions Permitting Circumvention*

The alternative approach taken by the extra-EU jurisdictions studied is to provide circumvention-specific exceptions. In other words, these are exceptions permitting circumvention that operate independently from the general exceptions and limitations to copyright. Exceptions of this sort are not always a perfect match when comparing jurisdictions, and there are often nuances that distinguish their scope and application from one another. For example, Singapore, Canada, and the United States each include a very analogous exception permitting circumvention of TPMs for the purposes of computer program level interoperability. Singapore's Copyright Act 2021 sets this out at section 430(1):

<sup>76</sup>. Federal Act of October 9, 1992, on Copyright and Related Rights (status as of January 1, 2022), Art 39a(4) (Switzerland).

<sup>77</sup>. Copyright Act 1994, s. 226D(1) (New Zealand).

<sup>78</sup>. Japan is the only potential exception to this, as further articulated in the table below. Japan's general non-infringing uses exception, however, only applies to its conceptualisation of "technological exploitation measures", which is a much narrower concept that applies to a much narrower set of activities.

<sup>79</sup>. The United Kingdom's approach to anti-circumvention exceptions and limitations, despite Brexit, remains strongly reflective of the harmonising effects of the Information Society Directive.

<sup>80</sup>. Namely, Australia, Canada, Japan, Singapore, United Kingdom, and the United States.

<sup>81</sup>. Copyright Act, RSC 1985 c C-42, s. 41.12(1) (Canada).

**“A person may circumvent a technological measure by doing an act in relation to a protected copy that is a computer program if – (a) the protected copy is not an infringing copy; (b) the act is done – (i) in good faith; (ii) with respect to particular elements of the computer program that are not readily available to the person doing the act; and (iii) *for the sole purpose of achieving interoperability of an independently created program with another computer program*; and (c) the act does not infringe the copyright in the firstmentioned program.”**

Along similar lines, Canada’s interoperability exception provides that a person has not unlawfully circumvented a TPM where:

**“... a person who owns a computer program or a copy of one, or has a licence to use the program or copy, and who circumvents a technological protection measure that protects that program or copy *for the sole purpose of obtaining information that would allow the person to make the program and any other computer program interoperable.*”<sup>81</sup>**

Though these exceptions possess minor differences with respect to “independently created” programs, and “obtaining information to allow” interoperability, they are in other respects quite similar. These exceptions can be contrasted to the United Kingdom which, given the lasting influence of Article 7 of the Computer Programs Directive, provides an exception permitting circumvention in order to:

**“... observe, study, or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do ...”<sup>82</sup>**

Though testing and studying programs to determine underlying ideas can be distinguished somewhat from “achieving interoperability”, the exceptions are roughly analogous. They both permit circumvention where the purpose is to access either the “elements” or “particular ideas and principles which underlie any element” of a computer program for similar purposes. The act of testing the functioning of a program also shares much common ground with achieving interoperability.

<sup>81</sup>. Copyright Act, RSC 1985 c C-42, s. 41.12(1) (Canada).

<sup>82</sup>. Copyright, Designs and Patents Act 1988, s.50BA (United Kingdom).

The similarities and differences between these approaches highlight the necessity of treating such exceptions as belonging to similar categories, even if in practice they result in somewhat different scope and application. The table below exemplifies common categories of exceptions permitting circumvention across the extra-EU jurisdictions studied:

Select Extra-EU Jurisdictions Exceptions & Limitations Permitting Private Circumvention										
Jurisdiction	Non-Infring. Uses	National Security	Use for Disability	Research /Priv. Study	Comp. Program Interop	Encryption Research	Privacy/ Personal Info	Cyber-security / testing	Libraries/ archives/ education	TDM
Australia	~	X			X	X	X	X	X	
Canada		X	X		X	X	X	X		
Japan	X			X		X				
New Zealand	X			X		X			X	
Singapore		X	X			X		X	X	
Switzerland	X		X	X					X	~
United Kingdom	~	X	X	X	X	X		X	X	~
United States		X	E		X	X	X	X	X	E

Fig. 10 Extra-EU Jurisdictions – Exceptions & Limitations Permitting Private Circumvention

E = statutory *exemption* granted through regulatory process rather than a permanent statutory *exception*

~ = a roughly analogous equivalent

A few qualifying remarks can be made about the general trends in these categories of exceptions and limitations. The first is that these categories are not exhaustive representations of the exceptions and limitations permitting circumvention in each jurisdiction. Some jurisdictions have enacted additional exceptions that extend beyond these general categories and into bespoke scenarios and uses.<sup>83</sup> The second is that some jurisdictions – particularly the United States and Singapore – include mechanisms for temporary exemptions permitting circumvention for more narrowly prescribed activities. Exemptions of this sort have been included in the analysis of trends and themes, but they should nevertheless be regarded differently given their temporary nature that is conditional upon periodic review and renewal.

As for remarks on the general trends shown, the most consistent and emphasised types of exceptions are those in relation to computer-related research and experimentation, including program interoperability, encryption research, and security testing. These exceptions are also often accompanied by national security exceptions that provide similar guarantees for computer program-related access relating to national security. The jurisdictions that seem to place less emphasis on computer-related research exceptions (namely, Switzerland, New Zealand, and Japan) are those with general “non-infringing uses” exceptions that would otherwise extend to such activities.

<sup>83</sup>. For example, Canada’s Copyright Act [s. 41.18(1)] includes an exception permitting circumvention of TPMs “on a radio apparatus for the sole purpose of gaining access to a telecommunications service by means of the radio apparatus”. An analogous exception is not replicated in the other jurisdictions studied.



As for exception permitting circumvention by non-profit libraries, archives, museums and similar organisations, most of the extra-EU jurisdictions studied include some type of exception to this effect, but vary quite significantly in scope. New Zealand and Switzerland, for example, permit circumvention by libraries for educational purposes, while most other jurisdictions narrow the purpose of circumvention purely to making a determination of whether to purchase or acquire a copy of the work. This latter approach is taken by the United States, Singapore, and Australia.

## F. OBLIGATIONS ON RIGHTSHOLDERS TO “MAKE AVAILABLE” OR PROVIDE ACCESS

As evidenced by the EU approach, many national approaches to anti-circumvention law include obligations on rightsholders to make works that are otherwise protected by TPMs available to beneficiaries of exceptions or limitations, or to provide the means of circumvention in some way. Within EU jurisdictions, the basis for this stems from Article 6(4) of the Information Society Directive (as well as Article 3 of the DSM Directive), requiring that Member States “... ensure that rightsholders made available to the beneficiary of an exception or limitation in national law ...” This obligation has led to the creation of administrative bodies in some Member States that can hear complaints and order rightsholders to take certain action(s).

Extra-EU jurisdictions have imposed similar obligations on rightsholders, and in some cases have empowered certain users and individuals with the authority to circumvent TPMs on behalf of others to give effect to certain exceptions and limitations. A summary of the obligations of rightsholders to make works available and empower individuals to carry out circumvention activities to give effect to exceptions and limitations is provided in the table on the next pages:

Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)			
Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Australia</b>	-	-	
<b>Austria</b>	-	-	
<b>Belgium</b>	-	-	
<b>Bulgaria</b>	-	-	Bulgaria has no formal complaint or enforcement body. It instead provides that “users who want to benefit from [an exception] for works which they have the legal right to use, but are impeded by a technological measure ... may request from the owner of the right to grant them the respective access in extend justified by the purpose”.
<b>Canada</b>	-	-	Canada has no formal complaint or enforcement body, but section 41.21 of its Copyright Act permits the creation of an administrative body or tribunal that could fulfil these purposes. To date, no body has been formed pursuant to section 41.21.

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Croatia</b>	✓	✓	Croatia's copyright act stipulates that where a use is allowed under one of the exceptions and limitations to copyright but is otherwise restricted by TPMs, "the authors or other persons who applied such measures or who are authorized or have the possibility to remove them, shall be obliged, by providing special measures or concluding contracts to enable the users or their associations access to such works and the use thereof in accordance with the limitations referred to in Article 82-87". Importantly, these obligations are accompanied by enforcement powers. Article 98(2) stipulates that the Minister competent for the State Intellectual Property Office may take action.
<b>Republic of Cyprus</b>	-	-	
<b>Czech Republic</b>	-	-	
<b>Denmark</b>	✓	✓	Denmark's copyright act empowers the Copyright Licence Tribunal, upon request, to order a rightsholder who has used effective technological measures to make such means available to a user which are reasonably necessary for the latter to benefit from an exception. If the rightsholder does not comply within 4 weeks from the decision of the Tribunal, the user may circumvent the TPM if they have "legal access to the work or the performance". This applies "only to the extent that the rightsholder has not, by voluntary measures, including agreements with other parties concerned, ensuring that the user may benefit from [the exceptions]".
<b>Estonia</b>	✓	~	Estonia allows users who are barred from making use of an exception or limitation to make a complaint to the "copyright committee". This committee is appointed by the Ministry of Justice and is a committee of experts that can make recommendations for amendments, but also "resolve, at the request of the parties, disputes related to copyright ... by way of conciliation of the parties". This stops somewhat short of an enforcement power, though does oblige rightsholders to participate in this procedure. For TPMs specifically, the copyright committee is empowered to "hear applications" pursuant to section 80(4) concerning TPMs, and upon application to the committee the parties are "required to enter into negotiations through the committee and conduct negotiations in good faith".

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Finland</b>	✓	✓	Finland's copyright act states that "the author shall offer the user ... the means to use the work in accordance with the provisions mentioned in the subsection if the user lacks the means to use the work owing to technological measures. If the author does not offer the means ... or if use of the work is not made possible by voluntary measures, such as agreements between authors and users of the works ... the matter shall be resolved by an arbitration procedure in accordance with section 54. [Section 54(6) provides for each party to appoint an arbitrator], "If a party concerned refuses the arbitration of a matter ... the matter may, upon application by a party concerned, be submitted to a court of justice for resolution. If the Court has granted authorisation in a matter ... the authorisation and its terms shall be in force until the matter has been settled with finality or until a higher court rules otherwise in regard of the appeal".
<b>France</b>	✓	✓	France empowers the "Regulatory Authority for Audiovisual and Digital Communication" (RAUDC) with ensuring compliance by rightsholders of the obligation to not "resort to technical measures which would have the effect of depriving the public of the benefit of ... exceptions". The RAUDC's mandate over TPMs is clarified at Article L331-12 where it is stated that its mandate includes "A regulatory and monitoring mission in the field of technical protection measures and identification of protected works and objects". More specifics are provided at Article L331-28, where it is stated that its authority exercises the following functions "(1) it ensures that the technical measures referred to in Article L331-5 do not result in harms due to their mutual incompatibility or their inability to interoperate...(2) It ensures that the implementation of technical protection measures does not have the effect of depriving the beneficiaries of the exceptions ... (3) It also ensures that the implementation of technical protection measures does not have the effect of depriving persons benefiting from the exception of reproduction for purposes of collection, conservation, and on-site consultation ..." Article L331-29 further states that "The authority's decisions are made public while respecting the secrets protected by law. They are notified to the parties who can lodge an appeal before the Paris Court of Appeal ... The president of the authority refers abuse of dominant position and practices to the Competition Authority hindering the free exercise of competition of which he may become aware in the sector of measurements techniques. This referral may be made in as part of an emergency procedure".

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Germany</b>	-	-	
<b>Greece</b>	✓	✓	Greece's copyright law states that "if the rightsholders do not take voluntary measures including agreements between rightsholder and third parties benefiting from the exception, the rightsholders and third parties benefiting from the exception may request the assistance of one or more mediators selected from the list of mediators drawn up by the Copyright Organization. The mediators make recommendations to the parties. If no party objects within one month from the forwarding of the recommendation, all parties are considered to have accepted the recommendation. Otherwise, the dispute is settled by the Court of Appeal of Athens trying first and last instance".
<b>Hungary</b>	✓	✓	Hungary's copyright law states that "[i]f no agreement is reached between the beneficiary of a free use and the rightholder about the conditions of making the free use possibility (Article 95/A) in spite of the protection against the circumvention of technological measures (Article 95), any of the parties may turn to the Mediation Board. The procedure may also be initiated by the representative organisations of the beneficiaries. In such a case, the effect of the award of the Mediation Board – in the absence of a stipulation of the contrary – shall extend to all members of such organisation who are beneficiaries of free use ... If no agreement has been reached ... the beneficiary of free use may turn to the court within 15 days ... and may demand in a lawsuit that the court oblige the rightholder to make the free use possible according to the conditions indicated by him".
<b>Ireland</b>	-	-	Ireland does not create or task an administrative body or tribunal with hearing complaints or resolving disputes. It instead grants complainants the right to apply to an "appropriate court" for an order. Namely, Ireland's copyright law states "where a technological protection measure has prevented a person (in this section referred to as a 'complainant' from undertaking in respect of a work the permitted act, the complainant may request the owner or licensee of the rights in that work ... to provide an effective means of carrying out that act. Where within a period of 30 working days from the date of the request, the respondent declines or fails to provide such an effective means of allowing the complainant to undertake in respect of the work the permitted act, the complainant may apply to the appropriate court for an order directing the permitted act".



## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Italy</b>	✓	✓	Italy's copyright law creates a "Committee on Copyright" to hear and resolve complaints with respect to TPMs impeding exceptions and limitations. It is also empowered to compel rightsholders to "allow the utilisation of protected works". The Committee on Copyright is also empowered to make recommendations to Parliament with respect to TPMs. The operative portions of the law are that "rightsholders who have applied technological measures under Art 102 quarter of this Law, are obliged to remove them, upon request of the competent authority, in order to allow the utilisation of the protected works and of subject-matter, for public security purposes or to ensure the proper performance of an administrative, parliamentary or judicial proceeding". ... "The rightsholders are obliged to adopt proper solutions, also by means of specific agreements with the associations representing beneficiaries in order to allow the exercise of the exceptions ... on beneficiaries' specific request and on the condition that the beneficiaries have acquired the lawful possession of the copies of the work or of the protected subject-matter or have lawfully accessed to them in order to use them ... including the payment of the fair compensation, if due...". "In the absence of such agreements, both parties may apply to the committee under Article 190 so that it may carry out the mandatory attempt for dispute resolution, pursuant to the criteria set out in art 194-bis. Article 190 creates a 'Committee on Copyright' established at the Office of the President of the Council of Ministers that 'shall study matters regarding copyright or matters connected therewith and shall furnish information upon questions relating to such matters, when so requested by the President of the Council of Ministers, or when special provisions so require. The Committee shall carry out the mandatory attempt at settlement, under Article 71'".
<b>Japan</b>	-	-	
<b>Latvia</b>	-	-	Latvia does not create an independent or administrative body or task one with hearing complaints and resolving disputes. It instead directs complainants to mediation. The Latvian copyright act provides that, "where the Act states that users who cannot make use of an exception because of a TPM have "the right to request that the author gives access to such works taking into account the restrictions of the rights of an author. The author may refuse to provide such a possibility if the use of the work is contrary to [the normal exploitation of the work] ..." and that "If the user of the work and the author cannot reach an agreement in respect of [a request for access to avail oneself of an exception], they may apply to a mediator".

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Lithuania</b>	-	-	Lithuania adopts a primarily mediation-focused approach, with the possibility of referring matters to a regional court. Lithuania's copyright act provides that, "... users of [exceptions] must be provided with conditions or adequate means (i.e. decoding devices and other) enabling to use legitimately accessible objects of copyright, related rights or sui generis rights to the extent necessary for the users of the rights to benefit from the [exceptions] ... When the owners of copyright, related rights and sui generis rights do not take measures (i.e. do not provide the decoding devices, do not conclude agreements with the users of the rights, etc.) which would enable the users to benefit from the limitations specified in paragraph 1 of this Article, the users of the rights who have the right to benefit from such limitations, may apply to the Council for mediation in such dispute. The mediator(s) shall present proposals and help the parties to reach agreement. If the parties do not accept a proposal of the mediator(s), the dispute shall be settled by Vilnius regional court".
<b>Luxembourg</b>	-	-	Luxembourg leaves disputes surrounding TPMs and the inability to give effect to exceptions and limitations to a court process. The Luxembourg copyright act provides that, "[t]o the extent that the rightsholders fail to take the measures provided [to allow exceptions], the beneficiaries of the aforementioned exceptions, a professional group or an association representing their interests are entitled to bring an action for cessation in accordance with Article 81 of this law in order to cease the application of technical measures which hinder the exercise of said exceptions".
<b>Malta</b>	-	-	Malta has not created an administrative body or tribunal to resolve TPM-related complaints or disputes. Malta's copyright act provides merely an obligation on rightsholders to "make available to the beneficiary [of an exception] the means of benefiting from that exception, to the extent necessary to benefit from that exception or limitation"

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Netherlands</b>	-	-	The Netherlands has not created an administrative body or tribunal to resolve or hear TPM-related complaints or disputes. It does include a provision [section 29a(4)] that permits “further rules” in relation to TPMs that “maybe issued by an order in council that oblige the author or his successors in title to provide the user ... with the means necessary to benefit from [exceptions]. It is possible that these further rules could permit the creation of a complaint or resolution body.
<b>New Zealand</b>	-	-	New Zealand does not have an administrative body or tribunal to hear or resolve TPM-related complaints or disputes. It instead relies on a “qualified person” who is prescribed by statute or regulation to circumvent TPMs for others to give effect to exceptions and limitations. This process is described further in this section of the report below.
<b>Poland</b>	-	-	
<b>Portugal</b>	✓	✓	Portugal limits legal protection against unauthorised circumvention in situations “where it is found [that a TPM] has been applied without a protected work, or that it has been applied out the authorisation of the holder of the copyright or related rights”. Portugal’s copyright law tasks a “Mediation and Arbitration Commission” with hearing complaints and disputes in relation to TPM overreach, and tasks the Court of Appeal with hearing appeals from decisions reached by the Mediation and Arbitration Commission. It requires that the Mediation and Arbitration Commission reach decisions or conclusions within three (3) months of application.
<b>Romania</b>	-	-	Romania includes only a general obligation of rightsholders to “make available to the beneficiaries of [exceptions] the means necessary for access to the works or any other subject matter of protection”.
<b>Singapore</b>	-	-	Singapore has not created an administrative body or tribunal to hear or resolve TPM-related complaints or disputes. It instead relies on a periodic review process that takes place every four years, but is in all other respects very similar to the Triennial Review process in the United States. This process does not address individual circumstances where users seek access but allows for temporary exemptions to be created. This is discussed further in Section G below.
<b>Slovakia</b>	-	-	

## Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)

Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Slovenia</b>	-	-	Slovenia has not created an independent complaint or dispute resolution body for TPMs. It instead points generally to mediation to resolve disputes. Slovenia's copyright act provides that rightsholders who use TPMs to protect works must provide "on request and within the shortest time possible, those persons having legal access to a copy of a copyright work or other subject matter of related rights with the means to apply the limitations to rights [exceptions] ... by modifying a technological measure or by other means" ... "If the rightsholder fails to secure the means ... the persons seeking to apply the limitations on rights may request mediation". To give practical effect to this obligation, however, Slovenia requires that rightsholders give notice of their use of TPMs. Slovenia's copyright act further requires that rightsholders "or importers" shall "put a clearly visible marking on each copy of a copyright work or other subject matter of related rights manufactured or imported for commercial purposes, indicating ... information on the technological measure and its effects; and ... his registered name and address in order to ensure an effective implementation of [the rightsholder's obligation to provide access]."
<b>Spain</b>	-	-	Spain has adopted a fairly passive approach to its obligation to ensure that rightsholders provide access to TPMs in order to give effect to exceptions and limitations. It points generally to the civil courts as the ultimate body to hear complaints in the absence of rightsholder compliance. Spain's copyright act provides that "where intellectual property right-holders have not taken voluntary measures, including agreements with interested parties, for the fulfilment of the obligations [to enable exceptions & limitations], the beneficiaries of these limits may bring the matter before the civil courts".
<b>Sweden</b>	-	-	Sweden has not created an administrative body or tribunal to hear TPM complaints or disputes. It rather vaguely provides that "a Court may" (at the request of a user) order "with penalty of a fine ..." "make it possible for the user to exploit the work".

Enforcement of Exceptions and Limitations Permitting Circumvention (EU Member States and the UK)			
Jurisdiction	Complaint Body?	Enforcement Powers?	Details
<b>Switzerland</b>	✓	-	Switzerland's copyright act creates a "monitoring office" for TPMs that monitors and reports on the effects of TPMs, particularly their impacts on exceptions and limitations. The monitoring office is intended to "act as a liaison between user and consumer groups and users of technological measures, encouraging "cooperative solutions". This includes a reporting and complaint process. The Monitoring Office for Technological Measures (OTM) is somewhat novel in that few other jurisdictions have actually taken this type of approach (a body created specifically for TPMs rather than a general copyright complaint body). It has published reports of investigations, but these are only available in French, Italian and German.
<b>United Kingdom</b>	✓	✓	The CDPA creates a process where a person prevented from carrying out a permitted act due to a TPM may issue a notice of complaint to the Secretary of State (SoS). Following receipt of the notice of complaint, the SoS may give to the owner of the copyright work or an exclusive licensee "such directions as appear to the Secretary of State to be requisite or expedient" for the purposes of (a) establishing whether any voluntary measure or agreement relevant to the copyright work the subject of the complaint subsists; or (b) (where it is established that there is no subsisting voluntary measure or agreement) ensuring that the owner or exclusive licensee of that copyright work makes available to the complainant the means of carrying out the permitted act the subject of the complaint to the extent necessary to so benefit from that permitted act." This entire process includes a caveat that it only applies "where a complainant has lawful access to the protected copyright work, or where the complainant is a representative of a class of persons, where the class of persons have lawful access to the work". In practice, the UK's complaint and review process has heard relatively few complaints and disputes, which is elaborated further upon below.
<b>United States</b>	-	-	The United States does not have a complaint or dispute resolution body beyond its Triennial Review process carried out by the Librarian of Congress. This is discussed further in Section G below.

Fig.11 Intermediated Circumvention of TPMs



In all, of the 27 EU Member States examined, only 9 have put in place administrative bodies or tribunals to hear complaints or resolve disputes involving TPMs. Importantly, the standards and timelines for rightsholders to take action or make the “means of circumvention available” vary widely. These standards can be divided into three broad categories. The first are those jurisdictions that require rightsholders to take action quickly. These range from immediate (in the case of Austria) to “the shortest time possible” (or 72 hours in the case of TDM) in the case of Slovenia. Also in this category is Bulgaria’s provision requiring rightsholders to provide access for TDM purposes within 72 hours. The second category comprises jurisdictions that allow rightsholders to take considerably more time to provide the means of access. This ranges from “four weeks” in the case of Denmark to “30 days” in the case of Ireland. It also includes Portugal’s rather long period of three months. Finally, the third and largest category are those jurisdictions that impose no time constraint at all on rightsholders to provide the means of access. This group represents 19 of the 27 EU Member States studied. The following table illustrates these differences among EU Member States:

<b>User Position Related to Circumvention Among EU Member States &amp; the UK</b>			
<b>Jurisdiction</b>	<b>Statutory obligation on rightsholder</b>	<b>Timeline</b>	<b>Remedy for non-compliance</b>
<b>Austria</b>	must “make the necessary means available immediately”	Immediate	Court application or private litigation
<b>Belgium</b>	“take the necessary measures to enable ... beneficiaries of the exceptions...to benefit from said exceptions ...”	Unspecified	Court application or private litigation. Action can also be brought by Minister
<b>Bulgaria</b>	“provide access to the work to the extent justified by the purpose”, including a specific provision allowing TDM for which rightsholders are required to provide access within 72 hours of the request	Unspecified, 72 hours for TDM only	Unspecified
<b>Croatia</b>	Rightsholders are “obliged to enable users or their associations to access works”	Unspecified	Administrative process
<b>Rep. of Cyprus</b>	Rightsholder must “provide the means” to benefit from enumerated exceptions	Unspecified	Unspecified
<b>Czech Republic</b>	Rightsholders are “obliged to make the work available”	Unspecified	Unspecified
<b>Denmark</b>	Rightsholders must make “means available to a user which are reasonably necessary for the latter to benefit from an exception”	4 weeks	Administrative process

User Position Related to Circumvention Among EU Member States & the UK			
Jurisdiction	Statutory obligation on rightsholder	Timeline	Remedy for non-compliance
<b>Estonia</b>	Rightsholder must “adjust the measure to allow the permitted use (including reaching an agreement or contract) within a reasonable period of time”	Unspecified	Administrative process
<b>Finland</b>	Rightsholder must “provide the means to use the work”	Unspecified	Arbitration followed by court application or private litigation
<b>France</b>	Rightsholder must “take necessary measures to allow the user to benefit from an exception”	Unspecified	Administrative process followed by court application or private litigation if unsuccessful
<b>Germany</b>	Rightsholders must “provide the means required to bring about the respective entitlement (exception)”	Unspecified	Unspecified
<b>Greece</b>	Rightsholders must “provide the means to benefit from the exception”	Unspecified	Mediation followed by court application or private litigation if unsuccessful in resolving the dispute
<b>Hungary</b>	Voluntary measures of rightsholders, and an obligation to reach an agreement with users seeking access	Unspecified	Mediation followed by court application or private litigation if unsuccessful in resolving the dispute
<b>Ireland</b>	Rightsholder must ensure that the beneficiary of an exception has the means of benefiting from the exception within 30 days from the request of the user	30 days	Court application or private litigation

User Position Related to Circumvention Among EU Member States & the UK			
Jurisdiction	Statutory obligation on rightsholder	Timeline	Remedy for non-compliance
<b>Italy</b>	Requirements are divided according to the purpose. For TDM, rightsholder must “allow the extraction of a copy for the exceptions of quotation and TDM for research”, for public security or administrative and legal proceedings, rightsholders are obligated to “remove” TPMs, and for other purposes, rightsholders must “adopt appropriate solutions” (including agreements with trade associations) for exceptions and limitations	Unspecified	Dispute resolution by administrative body
<b>Latvia</b>	[if the user] cannot implement [exceptions] due to the effective technological measures used by the author, he or she has the right to request that the author gives access to such works taking into account the restrictions of the rights of an author. The author may refuse to provide such a possibility if the use of the work is contrary to the [normal use of the work of an author]	Unspecified	Mediation and dispute resolution process
<b>Lithuania</b>	Rightsholder must “provide with the conditions or appropriate means (e.g. decoding devices) to make the work available (as long as there is no commercial benefit for the user)”	Unspecified	Mediation or settlement, with litigation as a last resort
<b>Luxembourg</b>	Rightsholder “must take the necessary measures, in particular by contractual means, in order to guarantee beneficiaries, who have lawful access to the protected work or service, an unhindered exercise for ... exceptions”	Unspecified	Court application or private litigation
<b>Malta</b>	Rightsholders must “make available the means” of circumvention	Unspecified	No specific process is described

User Position Related to Circumvention Among EU Member States & the UK			
Jurisdiction	Statutory obligation on rightsholder	Timeline	Remedy for non-compliance
<b>The Netherlands</b>	Obligations are unclear. Refers to more prescriptive rules that may be enacted pursuant to an order in council (regulations)	Unspecified	No specific process is described
<b>Poland</b>	None	Unspecified	Unspecified
<b>Portugal</b>	TPMs that prevent exceptions and limitations are not protected. Article 221 provides that TPMs may not create an obstacle to the normal exercise of exceptions and “free and permitted uses”, or to works in the public domain or “works published with public funding”	Three months	Mediation and arbitration, with appeals to court
<b>Romania</b>	Rightsholders must “make available the necessary means to access”		None specified
<b>Slovakia</b>	Unspecified	Unspecified	None specified
<b>Slovenia</b>	Rightsholders must provide access within the “shortest time possible”	“Shortest time possible” or 72 hours in the case of TDM.	Mediation process
<b>Spain</b>	Rightsholders must provide the means to beneficiaries of exceptions with “the appropriate means to enjoy them, in accordance with their purpose, provided that such beneficiaries have lawful access to them”	Unspecified	Court application or private litigation

User Position Related to Circumvention Among EU Member States & the UK			
Jurisdiction	Statutory obligation on rightsholder	Timeline	Remedy for non-compliance
<b>Sweden</b>	Article 52f states that "Anyone who, pursuant to [an exception] may exploit a work protected by copyright is entitled to make use of a copy of a work to which he lawfully has access as referred to in the relevant provision, notwithstanding the fact that the copy is protected by a technological measure". The obligations on rightsholders to facilitate this is unclear	Unclear	Court application or private litigation
<b>United Kingdom</b>	Section 296ZE of the CDPA creates a user compliant process with the Secretary of State (Intellectual Property Office) where TPMs interfere with "permitted acts". Upon receiving a complaint, the Secretary of State has wide ranging powers, including giving the rightsholder "such directions as appear ... requisite or expedient" for ensuring that the "means of carrying out the permitted act" are made available to the complainant.	Unspecified	Court application or private litigation for breach of statutory duty

Fig.12 User Position Related to Circumvention Among EU Member States & the UK



Overall, the picture that emerges shows a lack of emphasis on ensuring that copyright exceptions and limitations can, in practice, be realised upon where TPMs provide an impediment. The majority of European jurisdictions impose no time constraints on rightsholders to provide access, and most rely on users to commence legal action in civil courts to enforce their rights. This would presumably leave users in a position where they are responsible for financing the legal costs of such enforcement, or at the very least, bear the burden of proving that a rightsholder has fallen short of their statutory obligation(s).

Even where jurisdictions have established administrative review processes separate from private legal action, it is not obvious that their processes are straightforward or clear, or that the tribunals and other bodies that hear them are accessible and within the practical reach of users and researchers. This suggests that much progress could be made across Europe if jurisdictions imposed tighter time constraints on rightsholders, drawn greater awareness to the availability of enforcement bodies, and empowered those bodies to ensure that rightsholders' obligations are followed up on and given practical effect. Such practical effect could include public reporting of administrative review decisions to develop objective standards that could guide future complaints, not unlike the common law's principle of *stare decisis*.

Outside of EU Member States, Switzerland and the United Kingdom are the only jurisdictions examined that have incorporated TPM complaint mechanism processes into their copyright frameworks, the latter of course having implemented its process led by the SoS before Brexit.

A response to a Freedom of Information request communicated in May of 2023 by the United Kingdom's Intellectual Property Office (IPO) sheds further light on how this process has been used in practice. Within the last ten years, the IPO has received just three complaints. The first was received in 2015 and related to someone wishing to make a personal copy of CD they own, which was resolved through a voluntary agreement with the copyright owner. The second was also received in 2015 and concerned literary works on websites being used for the purpose of TDM. The IPO did not uphold the complaint because it was not considered to qualify for consideration by the SoS under section 296ZE(9) of the CDPA. Finally, the third complaint, received in 2022, was made in relation to accessible copies of an eBook for the purposes of research and private study, and for copies for TDM for non-commercial research. Officials at the IPO requested additional information from the complainant to determine whether the use was in scope, but the request for further information was not responded to. In all, despite the United Kingdom having one of the more robust and resourced complaint and enforcement bodies to hear TPM complaints, the history over the past decade shows that relatively few complaints have come forward for resolution. The relatively few complaints that have been filed over the past ten years suggest that users are either unaware of this process or do not feel that it can adequately address their needs.<sup>84</sup>

Administrative bodies or tribunals to hear and resolve TPM complaints are only one potential avenue for giving effect to exceptions and limitations, however. New Zealand offers an example of an alternative approach that could alleviate some of the shortcomings evidenced by the paucity of complaints and disputes in the United Kingdom.

<sup>84</sup>. For a more detailed analysis of the complaints filed with the United Kingdom's Intellectual Property Office and similar complaint mechanisms in EU jurisdictions, see Report 2, Part 4.

As mentioned previously in this report, two aspects of New Zealand’s approach enable users with the means to give effect to exceptions and limitations. The first is that the prohibited conduct in relation to TPMs is narrowed considerably. In particular, New Zealand’s prohibitions on circumvention, the manufacture and distribution of circumvention tools, or offering services, are all limited to circumstances where it is known that such activities, tools, or services will be used to infringe copyright.<sup>85</sup> It is therefore legally permissible to offer services or distribute circumvention tools that are utilised specifically to give effect to exceptions and limitations. Second, New Zealand specifies particular individuals and organisations, referred to as “qualified persons”, to offer circumvention services or provide access to circumvention tools. Among the “qualified persons” are librarians of a prescribed library, the archivist of an archive, an educational establishment, or any other person specified by regulation. New Zealand’s copyright act also sets limits on the costs or fees charged for circumvention by qualified persons:

／ **“A qualified person who exercises a permitted act on behalf of the user of a TPM work must not charge the user more than a sum consisting of the total cost of the provision of the service and a reasonable contribution to the qualified person’s general expenses.”**<sup>86</sup>

This approach offers a number of potential advantages over a complaint and dispute resolution body. One such advantage is that it clearly designates certain individuals with the competence and authority to circumvent TPMs on behalf of others for non-infringing purposes. This provides end-users with a more tangible solution to giving effect to exceptions and limitations. The second and related advantage is that it bypasses the need for rightsholders to be involved in the adjudication or resolution of a complaint. Aside from the potential opposition to providing access or the means of circumvention by rightsholders, a resolution approach is more likely to result in procedural delays and inefficacies.

Overall, the approach taken primarily within EU Member States to impose obligations on rightsholders to provide access to TPM works invites critique, as the objects and purposes of the obligations on rightsholders to provide the “means” of benefiting from various exceptions and limitations are not being realised upon. TPMs are actively inhibiting research, effective delivery of education and teaching, and placing a chilling effect on innovative uses of copyright works<sup>87</sup> that are otherwise strongly in the public interest.<sup>88</sup> The notion of legal protections

<sup>85</sup>. Copyright Act 1994, s. 226A (New Zealand).

<sup>86</sup>. Ibid., at 226E.

<sup>87</sup>. Though the empirical and doctrinal studies conducted throughout this three-part series of report focuses primarily on the impacts of TPMs in relation to digital materials impacting research, education, and teaching, it should be noted that TPMs also frequently impact non-consumptive uses of copyright works in ways that do not implicate exclusive rights whatsoever. The clearest example is in the case of TPMs that are used to protect largely utilitarian software in computerised systems and devices. Often access to this software is needed for the repair, maintenance and diagnosis of computerised devices and machinery. Access to this type of software may also be needed in the development of third-party components or peripherals with the goal of achieving interoperability between two devices or systems. Software in these contexts often lacks any measurable independent commercial value, but is nevertheless subject to copyright protection which can in turn receive the additional benefits of TPM protections and anti-circumvention. For more on the “paracopyright” aspects of TPM protections and examples of the activities they prohibit, see Anthony D Rosborough, “Unscrewing the Future: The Right to Repair and Circumvention of Software TPMs in the EU” (2020) 11(1) JIPITEC 26-48, and Anthony D Rosborough, “If a Machine Could Talk, We Would Not Understand It: Canadian Innovation and the Copyright Act’s TPM Interoperability Framework” (2021) 19 J L & Tech 141–172.

<sup>88</sup>. As is further outlined in Report 2, TPMs are acting as an enormous impediment to research, lending, learning and teaching, text and datamining, and even access to works through on-site systems in University libraries and national libraries. (Report 2, Part 4, “Findings: Survey of Institutions” (p. 21).

for technological artefacts within copyright law remains a mostly alien and nebulous concept to researchers and institutions that are otherwise familiar with general copyright exceptions and limitations. The inability to quickly ascertain which technological restrictions amount to a “TPM”, and which activities amount to “circumvention” leads to reluctance and a presumption of non-use in practice.

These dynamics call for a closer look at potential solutions to the unrealised promise of lawful circumvention across EU Member States. On the one hand, relatively few jurisdictions have put administrative review processes or a dispute resolution bodies in place. This suggests that greater access to TPM works to give effect to exceptions and limitations could be achieved through stronger processes of this sort within Member States. On the other hand, the United Kingdom example points to more fundamental issues with placing access obligations on rightsholders. Despite the SoS’ well formulated and procedurally robust complaint and review process, it has not seen a level of engagement and activity from complainants that reflects the impediments and delays to research, education, and preservation of works. It may be that the transaction costs and procedural hurdles in resolving TPM overreach this way are simply too onerous on users. If so, this suggests that simply providing complaint or administrative review mechanisms within EU Member States with more authority and resources may not solve the public interest costs created by endemic invocation of TPMs by rightsholders in association with digital materials. As is further explored in the next section, a more direct and practically beneficial process for ensuring that users can benefit from exceptions and limitations may instead be found in a more general widening of the scope of lawful circumvention and related activities.

## **G. FLEXIBILITIES & OPPORTUNITIES FOR FUTURE EXCEPTIONS**

The ability for national lawmakers across the EU to widen the scope of lawful circumvention-related activities finds relatively little constraint from the WIPO World Copyright Treaty. Article 11 requires only that countries provide “adequate legal protection” and “effective legal remedies”. Just as the malleability in this wording has enabled more restrictive approaches to anti-circumvention law, it could also enable more permissive approaches that give better practical effect to exceptions and limitations. The following two sections provide a brief overview of potential approaches that could be taken within the EU and outside of it to achieve these ends.

### **1. EU Member States**

The first and most obvious means by which EU Member States could provide more permissive and balanced approaches to anti-circumvention laws would be to implement the Information Society Directive’s voluntary exceptions, the DSM Directive’s TDM exception, and to make explicit reference to such exceptions as part of their anti-circumvention frameworks. At present, the implementation and application of various exceptions and limitations to anti-circumvention laws is haphazard and inconsistent. Significant progress could be found through a more harmonised implementation alone.

But, as mentioned in Section F above, the implementation of exceptions and limitations permitting circumvention is only meaningful if users, including those within research institutions and libraries, can make practical use of such flexibilities. The complaint and dispute resolution bodies – sparsely formed and often lacking in teeth – also seem unlikely to be the most effective and timely solution to access restrictions. Given these dynamics, it may be that in addition to implementing the voluntary and mandatory exceptions and limitations in the InfoSoc Directive and the CSDM, Member States also adopt a more expansive interpretation of the “adequate legal protection” referred to in Article 6(2) of the Information Society Directive.

At present, Article 6(4) requires that Member States take appropriate measures to ensure that beneficiaries can take advantages of exceptions and limitations in relation to *private circumvention*. It does not, however, require that Member States take appropriate measures to ensure that circumvention tools or services also be made available to give effect to those exceptions and limitations. In this regard, Article 6(2) is somewhat more self-contained, requiring Member States only to provide “adequate legal protection” against the manufacture or distribution of tools and offering circumvention services. “Adequate legal protection” is not met where prohibitions on the manufacture or distribution of tools and offering circumvention services frustrate the operation of Article 6(4). As an alternative to complaint and dispute resolution bodies that are relied upon in relation to *private circumvention*, Member States could allow for the manufacture and distribution of tools and offering circumvention services *insofar as they are necessary* to give effect to an exception or limitation. This would be consistent with the whole of Article 6, recognising that it does not prohibit Member States from enabling access to circumvention services and tools as part of their obligations to ensure that rightsholders make available the “means of benefiting” from an exception. Such an approach might be analogous to Singapore, where the exception permitting private circumvention for “research on encryption technology” provides that:

**“431 –**

**1. A person may circumvent an access control measure by doing an act in relation to a protected copy if –**

- a. the act is done in the course of any encryption technology and is needed to conduct that research;**

**(...)**

**2. A person may deal in a circumventing device if –**

- a. the device is used only in circumstances to which subsection (1) applies;**
- or**
- b. at the time of dealing, the person does not know or reasonably know that the device will be used in any other circumstances;**

**3. A person may deal in a circumventing service if –**

- a. the service is performed only in circumstances to which subsection (1) applies; or**
- b. at the time of dealing, the person does not know and could not reasonably have known that the service will be performed in any other circumstances ...”** <sup>89</sup>

<sup>90</sup>. Copyright Act 2021, s. 431(1)-(3) (Singapore).

And though no EU Member State shares presently adopts this approach, there is at least some precedent for a more relaxed approach to permitting circumvention services and tools with Estonia as an example. Notably, Estonia's copyright act does not explicitly prohibit offering circumvention services or manufacturing and distributing circumvention tools. In fact, Estonia's copyright act is silent on the scope and character of prohibited acts in relation to TPMs, stating only that authors and holders of any related rights "may, in order to protect their rights, add technological measures to a work or object of related rights".<sup>90</sup> Given this very broad interpretation of "adequate legal protection" against the offering of circumvention services or provision of circumvention tools, it is plausible that an approach similar to Singapore's would nevertheless remain consistent with the Information Society Directive's Article 6(2).

The principal benefit of this approach is that it would effectively switch the onus from what is now upon users to prove that accessing a TPM work is consistent with an exception and limitation, to be placed upon rightsholders to prove that it is not. Such a scheme could be further supported by Member States if they were to enact a similar approach to New Zealand in designating certain individuals or institutions with permission to offer circumvention services or deal in circumvention devices.

Finally, there remains an opportunity for the European Commission to take a leadership role in modernising the EU's TPM framework. Article 12(1) of the Information Society Directive tasks the European Commission with submitting a report to the European Parliament that examines the application of TPMs "in light of the digital market", and in particular whether Article 6 confers "a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures". The European Commission is further tasked with proposing amendments to the Information Society Directive where necessary. In following up on this obligation, the Commission should consider the operation of Article 6 in its entirety, and with particular attention given to the scope and effectiveness of complaint and dispute resolution bodies created within Member States. Should the Commission find opportunity to propose amendments to anti-circumvention law in a general sense, it should strongly consider broadening the grounds for lawful offering of circumvention services and dealing in circumvention tools so that the practical benefits of various exceptions and limitations can be more widely received.

Reliance on administrative tribunals and compliant bodies to adjudicate complaints and resolve TPM overreach is a wonderful solution to the problem in theory. After two decades of dismal results, however, this approach has been wholly inadequate in practice. In contrast, an approach that empowers users and research institutions to more directly access the means of circumvention to give effect to exceptions and limitations is more likely to bear fruit.

<sup>90</sup>. Copyright Act, RT I 1992, 49, 615, s. 80(3) (Estonia).



## 2. Extra-EU Jurisdictions

Jurisdictions outside of the EU find no constraint from harmonising directives, and periodic review and exemption processes afford lawmakers with far more flexibility than what is offered in the EU. Having said that, this flexibility does not always deliver the benefits it seems to promise. The United States Librarian of Congress, for example, has implemented numerous new exemptions permitting circumvention throughout its history of Triennial Reviews. This includes several promising and responsive exemptions for the repair of motorised land vehicles, cybersecurity research (including vulnerability testing), and TDM. As progressive and responsive as these exemptions are, they are limited in application to only acts of private circumvention. The same restriction also applies to Singapore's periodic review and consideration of new permitted grounds of circumvention, despite several of its permanent exceptions allowing offering services and dealing in tools.<sup>91</sup>

The reason for this restriction stems from the treaty language that has been responsible for the DMCA approach to anti-circumvention's proliferation. Common terms in FTAs' intellectual property chapters relating to TPM circumvention include stipulations on the scope of new exceptions and limitations that can be put in place by national governments. The Canada-United States-Mexico Agreement (CUSMA), for example, permits state parties to enact "additional exceptions or limitations for non-infringing uses of a particular class of works ...", but only in relation to private circumvention.<sup>92</sup> Similar restrictions exist in FTAs with anti-circumvention chapters embodying the DMCA-tradition applicable to other countries.

The practical effect of this is a significant narrowing of the flexibility offered to national governments to implement meaningful exceptions permitting circumvention. Without the ability to create new exceptions that permit offering circumvention services or dealing in circumvention tools, jurisdictions bound by these obligations are, from a certain point of view, in a far worse position than EU Member States to create tangible solutions for beneficiaries of exceptions and limitations.

## 3. International Trade Dynamics

Finally, an overarching variable with the potential to impact both EU and extra-EU jurisdictions' approaches to anti-circumvention laws stems from a new set of international trade obligations with growing prevalence. In addition to the proliferation of the "effectively controls access" TPM conceptualisation described in Part I(A)(3) above, recent years have borne witness to a proliferation of "digital trade" chapters in FTAs. These chapters vary in scope and content, but generally touch upon cross-border data flow, the protection of personal information, and consumer protection in the digital environment. A growing number of FTAs with these chapters, however, have included "source code" provisions that prohibit states from requiring the transfer of or access to "source code of software" or to "an algorithm expressed" in source code as a condition for importation, sale, or market access. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018) (CPTPP) provides that:

<sup>91</sup>. Copyright Act 2021, s. 435 (Singapore)

<sup>92</sup>. Agreement between the United States of America, United Mexican States, and Canada (7 January 2020), 20.66(4)(h)-(5).

**“No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.”**<sup>93</sup>

The effect of this type of provision is to prohibit states from forcing disclosure or access to source code and related information about how software functions or behaves. In some other agreements, this includes not only software, but “an algorithm expressed in that source code”<sup>94</sup> By placing prohibitions on not only mandating source code disclosure but also “algorithms”, the potential impact of these restrictions could be quite far reaching.<sup>95</sup> In addition to their inclusion in an increasing number of FTAs, prohibitions on source code disclosure form part of the European Commission’s Digital Trade agenda<sup>96</sup> and forms part of several recently concluded bilateral and regional trade agreements.<sup>97</sup>

The impact that these obligations may have on options for recalibrating anti-circumvention laws may not be immediately apparent. Though the intent behind these provisions is to prevent unauthorised or “forced” technology transfer, they are poised to act as a double-edged sword for less hostile inquiries led by governments. Namely, these “source code” obligations may tie the hands of national governments in implementing obligations on rightsholders to facilitate circumvention of TPMs or to disclose technical information about how a given TPM works. For example, if an approach to resolving TPM overreach involves compelling rightsholders to disclose source code that forms part of a TPM, this may conflict with digital trade obligations, particularly where such disclosure is a requirement for market access.

While the approach most likely to produce progress among EU Member States involves empowering users and institutions to carry out lawful circumvention directly, there still may be a need for rightsholders’ cooperation and engagement on occasion. If the sophistication of TPMs has or will become such that greater user access to circumvention tools or services is insufficient, it may be necessary to preserve the Information Society Directive-style approach that obliges rightsholders to take positive steps to permit circumvention. It is foreseeable that a solution along these lines may take the shape of a mandatory scheme where rightsholders are obliged to provide access or disclosure of the means of circumvention at the time of sale or market entry. But again, in such a scenario, national governments may find that international trade source code obligations significantly restrict their capacity to compel this type of action. Though these source code provisions vary in their inclusion of carveouts that may ease these limitations on TPMs, overall, they risk impairing the ability of national governments to take more involved and proactive steps to enable circumvention for lawful uses in the future.

<sup>93</sup>. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018) (CPTPP), Art 14.17.

<sup>94</sup>. Supra note 114 at Art 19.16.

<sup>95</sup>. Maurizio Borghi & Benjamin White, “Data extractivism and public access to algorithms” in Maurizio Borghi & Roger Brownsword, eds, *Law, Regulation and Governance in the Information Society* (London: Routledge, 2022) at 122–125.

<sup>96</sup>. European Commission, “Digital Trade”, online: [https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade\\_en](https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en)

<sup>97</sup>. See e.g. EU-Mexico Agreement, Chapter 16 (Digital Trade), Article 9(1), “No party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party”. Similar provisions exist in bilateral and regional trade agreements between the EU and Canada, Singapore, Vietnam, Japan, the United Kingdom, Chile, and New Zealand.







## PART FOUR: RECOMMENDATIONS

**The foregoing reveals a significant gap across European jurisdictions between the practical effects of TPMs on research, education, teaching, and preservation, and the user rights provided by exceptions and limitations to copyright law. Contributing to this gap is a lack of harmonisation with respect to complaint bodies and administrative review tribunals within Member States that are intended to require that rightsholders provide access to TPM-protected works on a case-by-case basis. Where Member States have created such bodies under their national laws, they impose relatively lax time constraints on rightsholders to follow through on these obligations.**

The relatively few reported instances where complaint bodies and administrative tribunals have intervened evidence their lack of effectiveness in delivering upon the objects and purposes articulated in Article 6(4) of the Information Society Directive. On the one hand this points to an opportunity to improve these processes, while on the other calling into question this approach more broadly. The lack of efficacy of these complaint bodies and administrative tribunals calls into question whether users should be burdened with identifying and contesting TPM overreach to begin with, or whether an alternative approach would yield better results.

The EU approach to TPMs and anti-circumvention prevents opportunities for productive reforms should there be sufficient legislative will to do so. Finally, there remains a missed opportunity for European jurisdictions to place greater emphasis on the legality of offering circumvention services and so-called “trafficking” in circumvention tools. Greater emphasis on these capabilities as part of EU Member States’ obligations to “take appropriate measures” to ensure that rightsholders make available the means of benefiting from copyright exceptions could be crucial in allowing circumvention to be carried out in the absence of cooperation.

Based on the findings in the foregoing, the following recommendations are put forward:

- 1/** The Information Society Directive’s Article 6(4) should be amended to include all research-related copyright exceptions, including the temporary copying exception in Article 5(1) and the quotation right in Article 5(3)(d). This would ensure that the permitted grounds of TPM circumvention would extend to all research-related exceptions to copyright. This recommendation is consistent with the legal proposals put forward by the DG RTD Report;
- 2/** EU Member States should implement all non-mandatory exceptions to copyright that relate to research and education, including Articles 5(1) and 5(3)(d) of the Information Society Directive as noted above. This would further reinforce the efficacy of recommendation (1) above;
- 3/** European jurisdictions should adopt a broad and purposive interpretation of taking “appropriate measures” to ensure that rightsholders give effect to copyright exceptions by expanding the scope of permitted circumvention to include so-called “preparatory acts”, including offering circumvention services and the sale, distribution, or manufacture of circumvention tools. Relying on rightsholders to take action to facilitate access to TPM-protected works is insufficient, even at the behest of an administrative tribunal or complaint body. Technical knowledge, expertise, and capability should be diffused throughout research communities and related organisations across Europe to give practical effect to the guarantees provided by research exceptions in various Directives;

- 4/ Drawing upon the New Zealand and Singaporean approaches, and consistent with recommendation (3) above, EU Member States should, as furtherance of their “appropriate measures”, empower research organisations and institutions (such as libraries) to facilitate circumvention of TPMs for lawful purposes on behalf of users and researchers; and
- 5/ With only a few exceptions, EU Member States should impose clearer and shorter timelines in relation to rightsholders’ obligation to provide the means of accessing TPM-protected works in furtherance of an exception or limitation to copyright. Empowering research organisations and institutions to facilitate circumvention may fall short of a comprehensive solution, particularly where TPMs are novel or emerging technologies for which there are no commonly known circumvention techniques. In these cases, there must remain a procedure by which rightsholders can be compelled to provide the means of circumvention to give effect to exceptions and limitations. These procedures must be accompanied by teeth. Namely, tasking administrative bodies to effectively and efficiently resolve complaints and disputes arising from rightsholders’ failure to comply with these timelines, and the ability to prescribe penalties and remedies.

## CONCLUSIONS

This report has explored the multifaceted landscape of TPMs and their implications for copyright law across various jurisdictions. The legal and technical dimensions of TPMs have evolved substantially over the past two decades. Initially driven by the imperative to protect digital content from infringing activities, anti-circumvention law has since been significantly influenced by international treaties, including the WIPO Internet Treaties and successive FTAs embodying the DMCA anti-circumvention approach. Within the European Union, anti-circumvention law has been unsurprisingly strongly influenced by harmonising instruments such as the Information Society Directive and the DSM Directive, but significant variation in national approaches nevertheless remains. Furthermore, rapid advances in digital technologies – particularly the transformation from independently executable digital files embodying works to clouds and streams – have accelerated the use, implementation, and potential impacts of TPMs on non-infringing uses of works and access to information. Given these changes, anti-circumvention frameworks intended to permit users to make use of exceptions and limitations to copyright (particularly those in European countries) appear ill-equipped to provide such guarantees in this new paradigm.

The legal conceptualisation of TPMs varies quite significantly across jurisdictions. At a very general level, the jurisdictions studied fall into one of two categories in either treating TPMs as measures intended primarily to prevent infringing activities or measures that “effective control access” to copyright works. This distinction tends to have larger implications for the scope and character of anti-circumvention regimes across jurisdictions, with the former group more likely to bring general exceptions and limitations to copyright within the scope of lawful grounds for circumvention. The latter “effectively controls access” group of jurisdictions, on the other hand, tend to enact standalone and inconsequential exceptions and limitations permitting circumvention only for narrowly prescribed activities.



The overwhelming majority of jurisdictions studied place strong restrictions (or outright prohibit) offering circumvention services or dealing in circumvention tools. This is identified as a significant challenge in creating more effective schemes for enabling users to give effect to exceptions and limitations. This is because exceptions permitting private circumvention presume or require technical expertise that is often beyond the means and capabilities of users, requiring access to specialised knowledge or equipment. In this regard, the approaches of Singapore and New Zealand in particular stand out for showing the greatest potential to devise meaningful solutions for users to circumvent TPMs. More particularly, this is achieved by allowing circumvention services or dealing in tools for the sole purpose of permitted acts (i.e. lawful grounds for circumvention). New Zealand's approach in prescribing certain individuals and organisations with the authority to circumvent TPMs on behalf of others for these purposes also shows promise for offering a reasonable balance of interests and its lack of reliance on rightsholders to take cooperative and positive action to aid in circumvention efforts.

With respect to flexibilities and opportunities for future exceptions, this report identifies potential avenues forward that could be leveraged to introduce new anti-circumvention exceptions or expand the practical utility of existing ones. Across all jurisdictions studied, this is probably best achieved through expanding exceptions and limitations permitting preparatory acts to circumvention (namely, offering services or dealing in circumvention tools). The doctrinal avenue for implementing such an expansion, however, varies in feasibility given the entanglement of anti-circumvention law with various international trade obligations and the limitations on flexibilities as prescribed by European Union directives. Irrespective of jurisdiction, however, solutions aimed at giving greater effect to exceptions and limitations to copyright law must place a greater emphasis on empowering users and prescribed organisations with the practical means to circumvent TPMs. Lawful grounds for circumvention, in the absence of the practical means and assistance to do so, are unlikely to yield productive results or meaningful application of public interest exceptions and limitations to copyright.