

DISRUPTIVE (TECHNOLOGY) LAW? EXAMINING TPMS AND ANTI- CIRCUMVENTION LAWS IN THE COPYRIGHT (AMENDMENT) ACT, 2012

*Swaraj Paul Barooah**

This paper will explore in suitable depth, §65A which has introduced anti-circumvention provisions into the Indian copyright law. It will begin with an introduction into the relevant terminology and scope of DRMs, TPMS and RMIs, and the typical issues associated with the introduction of anti-circumvention laws. After identifying and examining these issues, this paper will undertake a legal analysis of the problematic phrases in §65A, namely, 'effective', 'purpose not expressly prohibited', 'intention' etc; and examine whether the Copyright (Amendment) Act, 2012 suitably addresses the issues that typically arise from the introduction of anti-circumvention laws. Next, the liability regime itself and the wisdom in introducing criminal penalties as opposed to civil statutory damages (paid to copyright owners) are discussed. This is followed by examining the politics associated with the Amendment including the lack of any international obligation to enact the same. Further, pressure groups and representations made by different stakeholders in the Standing Committee Report are given due consideration to understand the differing interests at stake. Finally, the paper undertakes an analysis of whether the balancing act sought to be achieved between industry and consumer interests has been realised through this Amendment.

I. INTRODUCTION

From its origins in the Statute of Anne¹ in England in 1710, to the various national and international legislations present today, modern copyright law has a fundamental nexus with information and knowledge. Though copyright law had its origins in censorship,² its purpose changed with time

* JSD Candidate 2013, LLM 2010, School of Law, U.C.Berkeley; B.A., LL.B.(Hons.) NALSAR University of Law. I would like to thank Prashant Iyengar for his generous comments and Tanaya Sanyal, 3rd year, W.B.National University of Juridical Sciences, Kolkata for her excellent research assistance. All errors remain my own.

¹ Statute of Anne, 1710, 8 Anne c.19.

² See Pamela Samuelson, *Copyright, Commodification, and Censorship: Past as Prologue-But to What Future*, available at http://people.ischool.berkeley.edu/~pam/papers/haifa_priv_cens.pdf (Last visited on June 1, 2013) (In order to have a method of controlling the print of seditious material, the English Crown was willing to grant the Publishers guild, control over printing of books in exchange for the promise to not print 'dangerous' material).

to encourage cultural and knowledge production³ by balancing the incentives given to creators, against the interests of society in accessing this information and building on it. Thus while society can and does benefit from the spread of information, the creator is granted exclusion rights for a specified duration so as to allow her to appropriate returns during this period.

While it is true that exclusion rights allow the creator to appropriate returns, it is not *necessarily* true that these returns are the incentive for creation,⁴ nor is it necessarily true that these exclusion rights are *required* to appropriate requisite returns.⁵ These are seemingly pedantic, yet crucial differences for policy purposes. The use of copyright as an *imperfect proxy* for creativity is important to keep in mind, so that focusing on a policy of encouraging creativity through copyright doesn't become an exercise in encouraging copyrights regardless of creativity.⁶ And it is within this larger framework that this paper examines one of the newest conceptual additions to the copyright regime in India – that of 'technological protection measures' (TPM), its addition and its implications in Indian copyright law.

The transition to a digital environment has made the proliferation of information much easier, with the cost of duplicating information coming close to zero. This has greatly increased the rate at which information has been copied and spread, copyrighted or not. The terms on which India's tremendous content creation and consumption industries operate are quickly changing with new digital technologies. The media and entertainment industry in India has been booming. KPMG expects revenues from Indian cinema to grow from \$ 2.3 billion in 2008 to \$ 3.6 billion by 2013. A report by E&Y on the Media and Entertainment Industry in India,⁷ noted that though theatres were

³ Information here includes literary, musical and artistic works, as well as any other tangible expression of ideas.

⁴ Along with economic enablement and/or incentive, creation may also occur due to any number of reasons including creators seeking reputational benefits, merely as a means of expression, serendipity, etc.

⁵ Even in the instances where the incentive is purely economical, evidence is required to show that exclusion rights are required to appropriate returns. Prior to this, evidence is also required to determine what the appropriate returns constitute. For instance, in many cases 'first mover' advantage may be more than enough to recover the appropriate returns, without imposing the social costs involved by conferring exclusion rights. It must be noted to all policy makers that while putting all works under the umbrella of copyrights, these unnecessary costs are also being incurred, so that copyright policy can be appropriately shaped for maximum benefit to all parties involved.

⁶ Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond and Intellectual Property Internalism*, May 11, 2012, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103821 (Last visited on November 11, 2012).

⁷ Ernst & Young, *Film Industry in India: New Horizons*, available at <http://www.ey.com/IN/en/Industries/Media---Entertainment/Film-industry-in-India---New-horizons> (Last visited on June 1, 2013); See Aparajita Lath, *Part II: Digitization – Growth Trends of the Film and Television Industry: Comparative Analysis*, February 3, 2013, available at <http://spicyipindia.blogspot.com/2013/02/part-ii-digitization-growth-trends-of.html> (Last visited on June 1, 2013).

still the primary sources of revenue (60%), other revenue streams such as pre-selling satellite, home video rights and revenue from new media are increasing. However, the Indian film industry allegedly loses around Rs. 50 billion per year due to piracy and India is one of the top countries in peer-to-peer file sharing infringements worldwide.⁸

Copyright owners, who'd been used to older distribution technologies, have struggled to keep up with technology and found it difficult to adapt to an evolving marketplace.⁹ The dominant players generally try to adapt rules towards maintaining their lead in the market, rather than allow the market to make efficient use of the new technology. In this case, dominant players were the middlemen between the content creators and their audience. Since establishing a distribution mechanism used to be a costly endeavor, their role enjoyed a boosted significance. However, the digital age, with its near zero distribution costs, is heavily cutting into the importance of that role.

With the easy and cheap means that consumers today have to reproduce works without loss or damage to their own purchase, rights holders have lost a measure of control over their works. This has led to them turning to new digital technology to deal with this. These digital techniques to ensure continued enjoyment of their exclusion rights are referred to as Digital Rights Management ('DRMs').¹⁰ The two most common forms of digital rights management are Technological Protection Measures ('TPMs')¹¹ and Rights Management Information ('RMIs').

⁸ *Piracy, a Serious Threat to the Indian Film Industry*, FINANCIAL EXPRESS (India) March 19, 2010, available at <http://www.financialexpress.com/news/piracy-a-serious-threat-to-indian-film-industry/592752> (Last visited June 1, 2013).

⁹ Jane C Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101, Colum. L. Rev. 1614 (2001)(For example, until the advent of the photocopier, copyright owners substantially controlled the production and dissemination of copies of works of authorship... Before mass market audio and video recording equipment, copyright owners also controlled access to works made publicly available through performances and transmissions... With the arrival of these technologies, the de facto, and often de jure, balance substantially shifted to users); See also Yochai Benkler, *The Battle over the Institutional Ecosystem in the Digital Environment*, Comm. of the ACM, Feb 2001, 84, 86.

¹⁰ Julie E. Cohen, *DRM and Privacy*, 18 Berkeley Tech. L.J. 575-617 (2003); See also Kapczynski *supra* note 6, 1015-8.

¹¹ Ian R. Kerr, *Technological Protection Measures: Part II - The Legal Protection of TPMs*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=705081 (Last visited on June 1, 2013)(Discussing the Canadian policy objectives behind implementing TPMs. The author also highlights the international experience with TPMs and argues a balanced approach towards the introduction of such measures till the cultural norms of the country so necessitates); Urs Gasser, *Legal Frameworks and Technological Protection of Digital Content: Moving Forward Towards a Best Practice Model*, Research Publication No. 2006-04, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=908998(Last visited on June 1,2013).

TPMs are measures that allow a copyright holder to restrict what can be done with a file so as to protect the interests of the rights holder.¹² This can be through preventing or restricting a computer or machine from altering, copying, converting (format), examining, sharing, distributing, saving or using the digital media in which the copyright holder's interests lie. Unfortunately, TPMs are a very slippery slope from merely protecting against infringement of copyrighted content, to protecting and encouraging rents that may arise from all content, copyrighted or not. They are especially risky because they need to be *extremely well designed* to ensure that they do *not* overstep the rights granted by copyright law,¹³ and the burden of ensuring they do not overstep these rights lies on the makers of these TPMs, who happen to be (or who are hired by) the copyright holders which shows a clear conflict of interest.

RMIs on the other hand are an additional 'note' embedded in or along with the file which conveys information such as the identity of the rights holders and/or other information such as terms and conditions regarding the copyrighted material.¹⁴

While the lay person may or may not always be able to circumvent, alter or remove these TPMs and RMIs, it is often not difficult for anyone with some relevant computer knowledge to do so. With the pace at which such computer knowledge accelerates and grows, it also does not take long for this relevant computer knowledge to become more widespread and commonplace. Thus for TPMs and RMIs to be effective, their source of power must be externally derived and this is where anti-circumvention laws come into play. Anti-circumvention laws make it illegal to tamper with, alter, or otherwise work around the technical (software or hardware) implementations of TPMs or RMIs. For the purposes of this paper, I will be discussing only the TPM aspect of DRMs.

¹² WIPO Performances and Phonograms Treaty, Art. 18 provides "...adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law". See also WIPO Copyright Treaty, Art. 11 which provides for similar legal protection and legal remedies against the circumvention of effective technological measures used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that which restrict unauthorized acts of the nature already mentioned.

¹³ This is because technical measures by default are applied across the board. Extra consideration needs to take into account the exceptions and limitations of copyrights.

¹⁴ WIPO Performances and Phonograms Treaty, Art. 19 (2) defines RMIs as "... information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication or making available of a fixed performance or a phonogram to the public".

II. THE NEW AMENDMENT

The Copyright (Amendment) Act 2012, ('Amendment') for the first time, explicitly recognized legal protection for Technological Protection Measures in the Indian copyright law through § 65A, and Rights Management Information through § 65B.

As far as anti-circumvention provisions go, § 65A¹⁵ seems to be a well thought out provision. The primary part of the provision is taken almost directly from the equivalent WIPO Copyright Treaty ('WCT') provision (Article 11) with several exceptions and limitations recognized. Nonetheless, there are certain some problematic portions. In the following paragraphs, I shall break down those portions and examine the text of the same.

A. FIRST PORTION

First, I shall analyse the following part of the provision:

“Any person who circumvents an *effective* technological measure applied for *the purpose of protecting* any of the rights conferred by this Act, with the *intention* of infringing such rights, shall be *punishable with imprisonment*¹⁶ which may extend to two years and shall also be liable to fine.”

This is the central part of the provision, which states that certain anti-circumvention measures are illegal. The insertion of the word 'effective'

¹⁵ The provision is as below (emphasis provided by the author):

65A. (1) Any person who circumvents an *effective* technological measure applied for *the purpose of protecting* any of the rights conferred by this Act, with the *intention* of infringing such rights, shall be *punishable with imprisonment* which may extend to two years and shall also be liable to fine.

(2) Nothing in sub-section (1) shall prevent any person from,—

(a) doing anything referred to therein for a *purpose not expressly prohibited by this Act*.
Provided that any person facilitating circumvention by another person of a technological measure for such a purpose shall maintain a complete record of such other person including his name, address and all relevant particulars necessary to identify him and the purpose for which he has been facilitated; or (b) doing anything necessary to *conduct encryption research* using a lawfully obtained encrypted copy; or

(c) conducting any lawful investigation; or

(d) doing *anything necessary for the purpose of testing the security* of a computer system or a computer network with the authorisation of its owner; or

(e) operator; or

(f) doing anything necessary to *circumvent technological measures intended for identification or surveillance of a user*; or

(g) taking measures necessary in the interest of national security.

¹⁶ This portion will be covered in Part III which discusses the rationale for introducing criminal liability in this provision.

is initially confusing. Taken literally, can a truly ‘effective’¹⁷ technical measure be circumvented in the first place? Strictly interpreted, the dictionary definition would mean that if a TPM can be circumvented, it is not an ‘effective’ measure. However, such a definition would be contradictory to the purpose of the legislation. Looking at the rest of the sentence, there is nothing else which helps in understanding the scope of the word ‘effective’. In fact, the corresponding provisions in the WCT and the WIPO Performances and Phonograms Treaty (‘WPPT’) have also left these terms undefined so that their member countries could contextualize them according to their domestic needs. In US, § 1201(a) (3) of the Digital Millennium Copyright Act, 1998 (‘DMCA’), defines technological measures that ‘effectively’ control access to a work, as measures that require application of information, process or treatment in ordinary course of operation, with authority of the copyright owner, to gain access to the work. In the EU, European Directive 2001/29/EC of the European Parliament defines ‘effective’ technological measures as those that are protected by access control or protection processes such as encryption, scrambling, or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective. The Indian legislation however has left it completely open with no guidance from the text other than specifying that it will only cover actual circumvention.

In this context, I propose the following method of interpretation: ‘effective’ should be interpreted as being against an ordinary or average consumer - ordinary with respect to technical proficiency. This is problematic in that it may be difficult to ascertain who the ‘average’ consumer is. It may be argued that technical knowledge of computers is growing at a very rapid rate, with technical measures getting outdated very quickly. So an ‘effective’ measure against an average consumer in 2012, may be quite ineffective by 2015. However, this can be countered by proposing that the ‘average’ customer is calculated as per the date of the alleged anti-circumvention law violation.

Looking at the provision again, it is seen that not all anti-circumvention measures, even when against ‘effective’ measures, are illegal. The circumvented TPMs also need to have been applied for the specific ‘purpose of protecting’ copyrights, and this circumvention needs to be done with the ‘intention’ of infringing upon these rights. This is important as it does not grant any legal sanction to technical measures that a company may include in its goods which simply provide the company with an extra measure of control over the goods after sale rather than protecting copyright. Furthermore, inserting the ‘intention’ requirement means that the accused must have both the knowledge and desire to infringe upon the copyright.

¹⁷ BLACK’S LAW DICTIONARY 532-533 (1999) defines *effective* as “ That which is produced by an agent or cause; a result, outcome, or consequence; To bring about; to make happen”; MERRIAM-WEBSTER, available at <http://www.merriam-webster.com/dictionary/effective> (Last visited on November 19, 2012)(Defines *effective* as “producing a decided, decisive, or desired effect”).

However, what constitutes ‘intention’ is not clear, and may even be circular, especially when taken in context of ‘conversion and interoperability’ issues. With the vast array of devices and gadgets, platforms and applications to view and engage with digital content, the advantages that come with interoperability have nearly become a fundamental requirement for fully utilizing digital content.¹⁸ However, TPMs usually limit the movement, and restrict the usage of a file from the device, platform and/or application of first usage, and this is often done without informing the user of such restrictions. This can cause a variety of unnecessary and problematic issues to legitimate usage. As Samuelson and Schultz point out in their paper (as an example), ‘users of Apple’s iTunes Music Store (iTMS) and iPod music player are precluded from interoperating with other digital music devices and vendors’ despite there being no indication anywhere on Apple’s site or on its products regarding such restrictions for its purchasers or exactly what these limitations are.¹⁹ Disallowing the conversion of content to compatible formats, while also restricting the interoperability of the content, leads to a narrow scope of usage for the consumer. As the consumer and the supplier of content are often not in the same bargaining positions, even in the rare instances where complete information is given, the consumer is not in a position to negotiate with the content provider to allow non-infringing personal usage. For instance, the purchaser of a song from the iTunes store cannot play that song on a Sony device. If the purchaser wants to convert the iTunes purchase to a compatible format for the Sony device despite knowing that it is not permitted by iTunes, does this mean he has the intention to infringe? Another problem that can arise from TPMs is region coding. This limits the usage of the content to devices that are recognized as being from a certain region. This prevents or restricts the usage of the users’ legitimately purchased content when the user tries to engage with the content in another geographical region.²⁰ Such restrictions unnecessarily hamper access and use of information goods by consumers.

In this context, I would opine that with the expansion of fair dealing under § 52 (1)(a)(i) to include sound recordings and cinematograph films, a purchaser of content cannot be held liable for infringing copyrights in that content when he is using it for his own personal use, even if he indulges in space-shifting or format-shifting. The question of ‘intention’ to infringe copyright ought not to arise in such cases of personal use. Even so, this still leaves much uncertainty as to when conversion and interoperability are permissible, and when they aren’t. Case law would probably be required to settle this point.

¹⁸ See Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L.J. 1575 (2002).

¹⁹ Pamela Samuelson & Jason Schultz, *Should Copyright Owners Have to Give Notice about Their Use of Technical Protection Measures?*, UC Berkeley Public Law Research Paper No. 1058561, 48, available at <http://ssrn.com/abstract=1058561> (Last visited on June 1, 2013).

²⁰ This problem commonly arises in DVD encryption as DVD players may not be encoded at the same region as the source of the DVD, which may have been bought during a visit to another country, for instance.

B. SECOND PORTION

“(2) Nothing in sub-section (1) shall prevent any person from,—

- a) doing anything referred to therein for a *purpose not expressly prohibited by this Act: ...*”.

Provided that any person facilitating circumvention by another person of a technological measure for such a purpose shall maintain a complete record of such other person including his name, address and all relevant particulars necessary to identify him and the purpose for which he has been facilitated.

This exception provides much of the required balance to this provision. By explicitly denying the applicability of this provision to anything not expressly prohibited by the Indian Copyright Act, 1957 (Copyright Act), it ensures that all the restrictions and limitations to copyright law continue to operate when TPMs are used. This is further supported by the phrase in the main provision - that TPMs must be for the “purpose of protecting” rights conferred by the Copyright Act. Thus the provision makes it quite clear that TPMs can be protected by legal sanction *only* when they are for the purposes of protecting rights conferred by the Copyright Act. To put this statement into context, one must remember that copyright is a delicate balance²¹ between creators’ rights and public interest.²² This balance is achieved by ensuring exceptions and limitations to copyrights even when TPMs are in place.

§ 52 provides the fair dealing exceptions in the Copyright Act, which now extend to all works, including sound recordings and video.²³ This

²¹ See William Landes & Richard Posner, *An Economic Analysis of Copyright Law*, 18 J. Leg. Stud. 325 (1989) (explaining that the central difficulty in copyright law is to find the balance between access and incentives); Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Right Management Systems*, (2001) 15 Harv. J.L. & Tech. 41 at 49-51.

²² Information is a public good, thus it is non-rivalrous and non-excludable. A non-rival good is one wherein one person’s usage of that good does not reduce the ability of another person to use the same good. A non-excludable good is one which does not discriminate as to who gets access to that good. This means that granting any exclusion rights (such as copyrights) over this information is inefficient. The reason this inefficiency is accepted is because it can serve as the incentive for creation. This is a delicate balance and requires much tailoring to ensure that true balance is achieved. See Paul A. Samuelson, *The Pure Theory of Public Expenditure*, Review of Economics and Statistics 36 (4): 387-9 (1954); See generally Pamela Samuelson, *DRM (AND, or, VS) the LAW*, available at http://people.ischool.berkeley.edu/~pam/papers/acm_v46_p41.pdf (Last visited on June 1, 2013).

²³ This is opposed to the pre-amendment version which covered only literary, dramatic, musical or artistic works.

includes exemptions for research, criticism, reporting of current affairs,²⁴ reproduction by teacher to pupil in course of instruction,²⁵ accessible formats for persons with disabilities²⁶ and more.²⁷ Thus, concerns as to space-shifting and format-shifting are likely to be addressed by this provision.

To the extent that hindrance of ‘fair dealing’ is concerned, the amendment adequately addresses legal concerns regarding possible sanctions against legitimate usage as per the fair dealing provisions of the Copyright Act.

The proviso is perhaps one of the few legislations worldwide that explicitly mentions third parties who help circumvention, and seems to exempt them from liability provided they fulfill certain conditions. These conditions include maintaining records of who seeks such help and the reasons they are circumventing the TPM. Unfortunately, these conditions carry privacy concerns.²⁸ It is important to realise that the anonymity that the internet brings, builds great value for the information produced when one removes this cloak of anonymity. There are primarily two privacy related concerns with TPMs. *Firstly*, in order to associate (digital) content with a purchaser, companies often require some sort of registration or submission of personal information. This allows companies to keep track of their user base, but also forces users to disclose their identity, which they may not always want to. The lack of viable alternatives to anonymously purchase such goods often means that the user does not have a ‘real’ choice as to whether she wants to disclose her identity or not.²⁹

Secondly, companies often introduce tracking mechanisms to follow up with the information gathered from step one. Tracking allows them to gather more information over their target audience as well as keep some measure of control over the digital file, thus allowing them to maximise rents.³⁰ In addition to this, users who want to circumvent TPMs for fair dealing purposes or other legitimate reasons need to supply their personal details and/or reasons in order to be able to circumvent the TPM. In other words, personal information is required to be given to private companies, for an individual to take legitimate action that is outside the purview of copyright law.

²⁴ The Indian Copyright Act, 1957, §§ 52(1)(b) & 52(1)(m).

²⁵ See Indian Copyright Act, 1957, § 52(1)(h)(i).

²⁶ See Indian Copyright Act, 1957, § 52(1)(zb).

²⁷ See generally Indian Copyright Act, 1957, § 52(1) for exceptions to copyright infringement under the Act.

²⁸ See generally Julie E. Cohen, *DRM and Privacy*, 18 Berkeley Tech. L.J. 575, 585 (2003).

²⁹ Lemley, Mark A., *Intellectual Property and Shrinkwrap Licenses* (Stanford Public Law Working Paper No. 2126845) (“Software vendors are attempting en masse to “opt out” of intellectual property law by drafting license provisions that compel their customers to adhere to more restrictive provisions than copyright (and even patent) law would require. These software license agreements are of two types: bargained agreements for custom software, and unbargained “shrinkwrap licenses” imposed on mass-market purchasers. As software has become a mass-market commodity, the shrinkwrap license has tended to predominate”).

³⁰ Samuelson & Schultz, *supra* note 19, 48.

These issues are particularly problematic for persons with disabilities, who are likely to be the biggest group of non-infringing circumventors. Private companies would be recording practically every work they access, throwing up particularly large privacy concerns. Additionally, it is simply impractical to expect all third parties in a country as large as India to have knowledge of this provision requiring them to maintain such records, especially considering that there is (rightfully) no regulation of who these third parties can be.

This impracticality may prove to be quite troublesome for certain circumventors, as the provision explicitly states that it will not prevent them from doing anything expressly not prohibited by the Copyright Act *provided that the third party maintains certain records*. This will be more closely examined in part III of this paper.

C. THIRD PORTION

“2) Nothing in sub-section (1) shall prevent any person from,—

- (b) doing anything necessary to *conduct encryption research* using a lawfully obtained encrypted copy;
- (d) doing *anything necessary for the purpose of testing the security* of a computer system or a computer network with the authorisation of its owner; or
- (e) operator”.

These two highlighted phrases provide welcome relief to programmers and computer engineers, as well as users who take an interest in discovering and fixing security issues within TPMs as it explicitly provides them with a safe harbour. When it is read together with the fair dealing exceptions of research (§ 52), this allows one to not only examine and look into these security issues, but also to disclose and publish their research findings.

As TPMs are externally ‘imposed’ technical measures which aren’t always disclosed to the consumer, it is possible that the consumer may be using software/technology which may render them vulnerable to security risks without their knowledge.³¹ If the TPMs are properly disclosed to the consumer, this security risk can be reduced. The addition of a potential security risk to the previously mentioned privacy and interoperability concerns, is undesirable

³¹ Mulligan, Deirdre K. and Perzanowski, Aaron, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, Berkeley Technology Law Journal, Vol. 22, 1157, 2007.

to say the least. Furthermore, as they attach liability to those who circumvent TPMs, anti-circumvention laws pose threats to those who seek to display the existence of, or solutions to security breaches caused by DRMs, thus disallowing means to address these concerns. In summary, there are three categories of security related concerns here:

- a. Technical measures which aren't disclosed to the consumer, possibly exposing the consumer to risks without his knowledge.³²
- b. When these measures are disclosed, the consumer may not be in a position to address them, as tinkering with them may lead to attachment of liability under anti-circumvention laws.
- c. Persons may not be allowed to discuss or analyse security risks in TPMs as anti-circumvention laws may render them liable for this reason.

This part of the provision partly addresses these security concerns in circumstances where computer users are trying to address or display (for others to address) security lapses. However, it still leaves unaddressed the potential security risks caused by TPMs that haven't been disclosed in the first place.

The word 'operator', i.e., § 65A(2)(e) is curiously separated from § 65A(2)(d) even though it seems to be in continuation. Interestingly, the previous draft version³³ of the Bill did not have this distinction, indicating that perhaps the legislators want to emphasise the distinction between 'operator' and 'owner'. This distinction would ensure that persons beyond just the owner of the machine are protected by the provision.

D. FOURTH PORTION

2) Nothing in sub-section (1) shall prevent any person from,—

- (f) doing anything necessary to *circumvent technological measures intended for identification or surveillance of a user*.

The legislative intent to prioritize privacy over copyrights is evident in this provision. As mentioned above, DRMs by their nature, tend to require identification and/or surveillance. When a software or hardware is linked to an authorization of some sort, then personal information of the user is required for the purpose of identification. However, it is possible to ensure that

³² See generally Samuelson & Schultz, *supra* note 19.

³³ The Copyright (Amendment) Bill, 2010, available at <http://copyright.gov.in/Documents/CopyrightAmendmentBill2010.pdf> (Last visited on November 26, 2012).

there are multiple layers of anonymity between the user and the authorization check, which allow a user to show that she is authorized without necessarily revealing details of her identity. As an example, all authorized persons can have a login key, which are coded a certain way when entered. This can be made more secure by, for instance, combining a login key with a machine specific serial number of an authorized machine in a way that, when combined, they cannot be correctly separated³⁴ into their two component parts once again.

This ensures that companies must provide such multi layered levels of security, anonymity and protection, if they want to insert TPMs. This provision puts the onus on TPM makers to do so, if they wish to use §65A against circumventors. This current portion of the provision directly addresses the privacy concerns listed above, and to the extent of the privacy issues *not* created by the third party proviso mentioned above, this successfully addresses them.

E. A FAIR BALANCE? A SUMMARY OF THE TRADE-OFFS TAKING PLACE

We have broken the Amendment down into examinable parts. Let us now sum up which problem areas have been addressed and which areas have not.

- (i) Restrictions on legitimate fair use - This is more or less adequately addressed as explained in Part II, Section B, by § 65A (2)(a) and by the corollary found to this in the main part of § 65A.
- (ii) Privacy concerns - They are partly addressed as explained in Part D which refers to § 65A (2)(f). However, as mentioned in Part II, Section B, the proviso in § 65A (2)(a) creates certain privacy concerns. Thus the provision in total, partly assuages privacy concerns, and partly creates them.
- (iii) Conversion and interoperability restrictions - Part A explains that § 65A (1) partly addresses these concerns, but still leaves scope for uncertainty for the consumer as to whether conversions and interoperability are permitted or not.
- (iv) Security Concerns - As explained in Part C, §§ 65A (2)(b), 65A (2)(d) and 65A (2)(e) address 2 out of the 3 security concerns that arise. The issue of content suppliers inserting TPMs with possible security

³⁴ For instance, if the two numbers are multiplied by each other, there is no correct way of finding the two constituent numbers by only examining the resultant number. Of course, this is a simplified example just being used to demonstrate the point.

risks, without disclosing this to the consumer is one that has not been addressed.

- (v) Transaction costs and social costs - This is not addressed anywhere nor is it expected to be addressed within a provision. It is possible that well crafted anti-circumvention laws may allow for enough exceptions and limitations, that all (otherwise) legitimate action is not hindered by the presence of such laws. However, the fact remains that even in these cases, the user must internalise the transaction costs and other costs involved in getting legal sanction to bypass the TPMs.

This extra cost is justified³⁵ only when the following two circumstances are fulfilled:

- (a) TPMs and anti-circumvention laws are well crafted enough to allay the concerns mentioned above;³⁶ and
- (b) The benefits provided by way of such well-crafted TPMs and anti-circumvention laws outweigh the transaction costs that consumers must internalize due to the existence of such anti-circumvention measures.

Hence, first, it needs to be seen how much the provision contributes to these costs. As explained in Part II, Section A there are 3 conditions for application of the liability on circumvention of a TPM. The 3 requirements are 'effective', 'purpose of protecting any of the rights conferred' and 'intention'. This allows for a total of seven situations where liability is not attached and only one where liability is attached.³⁷

As the Copyright Act merely lays down that certain acts are not illegal, but does not address the practical problems of users as to circumvention in other cases, these 7 situations attract costs of either (a) circumventing the measure, and possibly attracting legal trouble; or (b) not having access to legitimate uses/measures of accessing the content that is 'protected' by the TPM,

³⁵ That is to say, it is justified in the utilitarian perspective which values efficiency and 'maximum good for the maximum number', which is generally accepted as a justification for IP. This, however, is not the only accepted justification for IP. Other schools of thought may require a different version of this condition. See generally William Fisher, *Theories of Intellectual Property* in *NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY* 168, 184-89 (2001).

³⁶ If TPMs and relevant legislation are not crafted to allow for the previously mentioned issues (privacy, interoperability & security), then it would be required to also take into account the unnecessary transaction costs, social costs and opportunity costs involved in the causation of all those issues. *Prima facie*, it appears to be a reasonable assumption that in sum total, all these costs would be much greater than the potential benefits to the rights holders.

³⁷ Let us refer to these 3 conditions as A, B and C. The 3 situations of no liability are [(A+, B-, C-); (A-, B+, C-); (A-, B-, C+)]. The 3 situations with only one condition fulfilled are [(A+, B+, C-); (A+, B-, C+); (A-, B+, C+)]. And finally, there is the one situation where all three are not fulfilled [i.e., (A-, B-, C-)].

despite the TPM not having legal sanction (and the costs associated with this lack of access).

In one situation where liability is attached, there are again exceptions within it, such as fair dealing, research and security exemptions, privacy exemptions, etc. So, within this situation, there are ‘sub-situations’ which again negate liability but still attract costs of either (a) circumventing the measure and possibly attracting legal trouble; or (b) not having access to legitimate uses/measures of accessing the content that is ‘protected’ by the TPM, despite the TPM not having legal sanction (and the costs associated with this lack of access). These costs may be tremendous or negligible depending on the TPM associated with it, as well as on the knowledge and skill of the person who seeks to circumvent it.

To clarify again, these ‘sub-situations’ exist and have existed in other areas where copyright law applies too. However, in those situations, the costs were limited to possible legal tangles and nothing more, as no special ‘measures’ were needed to access or use the non-copyrighted content.

III. THE LIABILITY REGIME AND CRIMINAL PENALTIES

Aside from the tradeoffs involved in the introduction of the anti-circumvention provision, the other noticeable factor is the introduction of criminal penalties³⁸ for its violation. The penalty includes a term of two years imprisonment along with a fine, the limits of which have not been set. Presumably, limits have not been set on the fine amount to allow flexibility in damages.

By providing a range of exceptions in § 65A (2), the Indian provision has been careful to ensure that, in terms of violations and penalties, the Act only punishes when there is both circumvention as well as infringement of copyrighted content. However, as pointed out earlier, there is a certain absurdity present in the provision. § 65A (2) (a) lays down that nothing in the provision shall prevent anyone from doing anything not explicitly prohibited by the Act *provided* that any person facilitating the circumvention maintains records which can identify the person and the purpose for which he has been facilitated.

This therefore requires a third party (the facilitator) to maintain records in order for the accused to be relieved of liability. In other words, a person may fulfill the three conditions laid out in clause (1), but may still be not

³⁸ § 65A (1) “Any person who circumvents ... shall be *punishable with imprisonment* which may extend to two years and shall also be liable to fine”.

infringing (i.e., may be fair dealing, for instance).³⁹ An example may prove useful here. A common man may not care much about copyright infringement and may be willing to take his chances at circumventing a TPM on his legitimately purchased region coded DVDs, so that he can play them in his own DVD-player, which happens to be set at another region's code. In order to do so, he asks his son's friend, who works in IT, to help him circumvent the region lock on the DVD. In this case, he may have circumvented an 'effective' TPM, which was set for the 'purpose of protecting' its copyright and it may even be argued that he had the 'intention' of infringing such right. It's important to note that clause (1) does not require actual infringement. If taken to court, his lawyer would advise him that it is not infringement and that it falls under the fair dealing exception. However, now, with the proviso under clause (2), he may have to rely solely on his son's friend's records for the penalty of imprisonment and fine to not apply, despite the fact that there was *no actual infringement* here.

Such a strict standard of liability is clearly against the purpose of the provision as well as the Copyright Act, which clearly recognizes the limitations and exceptions to copyright. Thus, hopefully, it will be interpreted as a proviso which helps in proving innocence through means of acceptable evidence (i.e., the records maintained), rather than proving guilt, which should require the actual act of infringement as well.

Another major cause for concern is the mandate of criminal sanctions (along with a fine), rather than the option of civil remedies or criminal sanctions for violations. Criminal sanctions are normally reserved for situations involving great harm to society as a whole. Neither the WPPT nor the WCT, from which the main part of the provision seems to be taken, recommend criminal sanctions over civil remedies. Article 61 of the TRIPS Agreement refers to questions of 'commercial scale' when it states that:

"Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale... Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale."

While some violations may be on a large and commercial scale, some may also be individual 'not-for-profit' infringements. It is simply a disproportionate 'punishment' to mandate criminal sanctions for infringing activity that is not even on a commercial scale. The clear distinction between these two cases, though not made in the Copyright Act, makes it irrational and

³⁹ § 65A (1) requires intention to infringe, but not the actual act of infringement.

unreasonable to impose criminal sanctions against such individuals who may be involved in minor non-commercial based infringing activity. The threats of criminal sanctions may also force overt self regulation and prevent legitimate non-infringing use of copyrighted data. Thus the effect could be to raise the floor of copyright protection and cut into the exceptions and restrictions placed on it.

The provision is in dire need of some sort of minimum ‘commercial scale’ standard in order to impose such criminal penalties and a separate civil sanction for smaller / lesser cases of violation. In Samuelson’s telling words, “The rhetoric of piracy lends itself to increased use of criminal penalties to enforce copyright interests”.⁴⁰

IV. HOW DID ANTI-CIRCUMVENTION LAWS MAKE THEIR WAY IN?

India has a curious presence on the international stage with respect to copyrights. While US’ Special 301 report⁴¹ puts India on its priority watch list a few times in the recent years, Consumers International have placed India in the top 3 consumer friendly copyright regimes⁴² for four years in a row now. This ‘mysterious’ mix is easy to explain. US’ Special 301 report looks at copyright regimes as compared to their own industry friendly ideal standard for a developed country. Consumers International ranks copyright regimes based on how consumer friendly they are. The ability to spread, grow and develop knowledge and technology is more beneficial to development than strong protection of intellectual property.⁴³ Thus it is important to have a copyright regime that encourages the spread of information and knowledge by being strong enough to incentivize innovative activity while being weak enough to not interfere with the flow of culture and information.⁴⁴ Given the socio-economic status of India’s populace, a consumer friendly regime is more beneficial. There has been no pressure on the Government by civil society for the introduction of TPMs. Thus, it is curious that India has implemented this TRIPS plus measure despite no necessity or obligation, urgent or otherwise. While it is true that the WIPO’s WCT and WPPT require the protection of TPMs and RMIs, as has already been noted, India is not a member of either.

⁴⁰ See generally Pamela Samuelson, *supra* note 22.

⁴¹ Office of the United States Trade Representative, *2012 Special 301 Report*, April 2012, available at http://www.ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf (Last visited on November 26, 2012).

⁴² See *Consumers International IP Watchlist Report 2009 to 2012*, available at <http://a2knetwork.org/watchlist> (Last visited on November 26, 2012) (India ranked 1st in 2009 and 2010; and 3rd in 2011 and 2012 as per this report).

⁴³ See SIVA VAIDHYANATHAN, *COPYRIGHTS AND COPYWRONGS- THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY* 4 (2001).

⁴⁴ Neil Weinstock Netanel, *Copyright and Democratic Civil Society*, 106 *Yale L.J.*, 283 (1996).

Looking into the Parliamentary Standing Committee Report,⁴⁵ the department acknowledges that this section has been inserted to provide for prevention of circumvention while also keeping in mind the public interest in providing access to works. After this, the Committee Report notes views of various stakeholders. The Indian Broadcasting Federation⁴⁶ expressed the most extreme viewpoints, asking for much harsher punishments as well as shifting the burden of proof to the alleged infringer. With the exception of Google India and Yahoo India (who emphasised the importance of fair use and reasonable restrictions on copyright), majority of the stakeholders represented in the Parliamentary Standing Committee Report asked for a more stringent provision to be made. Many even asked for the mere act of interfering with a TPM to be made punishable. These stakeholders namely, the Motion Pictures Association, RPG Enterprises-Saregama, Indian Music Industry and The Indian Performing Right Society are all right holders. In response, the department took a strong stance and noted that TPMs often come in the way of fair dealing and have a significant impact on freedom to use work as permitted by law.⁴⁷ The Committee noted the abuse of anti-circumvention provisions in developed countries such as US, EU, Japan and clarified that § 65A would be given limited legislative guidelines for the following purpose:

“...allow the judiciary to evolve the law based on practical situations, keeping in mind the larger public interest of facilitating access to work by the public. The Committee takes note of the fact that many terms have been consciously left undefined, given the complexities faced in defining these terms in the laws of developed countries. The Committee would, however, like to emphasize that a constant watch would have to be kept on the impact of this provision and corrective measures taken as and when required.”⁴⁸

The strong pressure by the right-holder groups as well as the push back by the Committee, combined with the lack of any international obligation to bring in such a provision, make it very likely, in my opinion, that these groups had much to do with the lobbying efforts to bring the provision into existence. Having said that, lobbying efforts in India (and Bollywood) are very different from that of USA (and Hollywood). In Bollywood, despite the large

⁴⁵ Parliamentary Standing Committee on Human Resource Development, Two Hundredth and Seventy-Seventh Report on the Copyright (Amendment) Bill, 2010, ¶ 20.2 (The Report was tabled before both the Houses of the Parliament on November 23, 2010); See Amlan Mohanty, *Copyright Act Standing Committee Report: Technological Protection Measures*, December 26, 2010, available at <http://spicyipindia.blogspot.com/2010/12/copyright-act-standing-committee.html> (Last visited on June 1, 2013) (For an overview on the report as it pertains to TPMs).

⁴⁶ *Id.*, ¶ 20.3.

⁴⁷ *Id.*, ¶ 20.7.

⁴⁸ *Id.*

amounts of piracy, a large number of production houses and producers simply remain indifferent to efforts aimed at tackling it – and this could well have to do with the concurrent increase in revenues.⁴⁹ It is relevant to note though, that several Hollywood studios such as Sony, Universal and Fox Corporation, have entered the Indian market⁵⁰ and unlike their Indian counterparts, have a history of heavy lobbying to change copyright legislation.⁵¹ Fortunately, the Committee has made it amply clear that it is taking a cautious approach with regards to anti-circumvention and is attempting to pay due regard to public interest and local context.

V. CONCLUSION

Under the law as per the Copyright (Amendment) Act, anti-circumvention laws would lead to unnecessary transaction costs and security risks while raising unfair restrictions and privacy concerns. These provisions are likely to have the dubious distinction of being harsher towards certain marginalized groups such as the visually disabled. As discussed, of the people affected by anti-circumvention laws, only a small group may be involved in actual copyright infringing activity. Failure to recognize the difference in types of infringing and non-infringing activity is a definite cause for concern. Recently, the Delhi High Court had the opportunity to decide the first case⁵² recognizing the introduction of the TPM provision in India. In my opinion, the Delhi High Court failed to clarify whether the protection was extended to that which Sony (the petitioner) did not permit or to which the Copyright Act did not allow. It's also important that the ambiguous boundaries of fair dealing are carefully demarcated so that there is no confusion on this front.

As mentioned before, the segment of society that would be most affected in terms of transaction costs is likely to be the visually disabled or print disabled.⁵³ For the 285 million print disabled persons in the world,⁵⁴ only tiny segments of print material are accessible due to conversion to accessible

⁴⁹ See *supra* note 7 and accompanying text.

⁵⁰ Ayan Roy Choudhury, *The Future of Copyright in India*, Journal of Intellectual Property Law and Practice, 3 (2), 2008, 102 – 114.

⁵¹ See AJ Scott, *A New Map of Hollywood: The Production and Distribution of American Motion Pictures* (Regional Studies, Vol. 36.9, 2002) 957–975.

⁵² Sony Computer Entertainment v. Harmeet Singh, CS(OS) 1725/2012; See Amlan Mohanty, *Sony Playstations To Be Illegal in India? - First Test of Newly Inserted S.65A of the Indian Copyright Act, 2012*, February 6, 2013, available at <http://spicyipindia.blogspot.com/2013/02/jailbreaking-sony-playstations-to-be.html> (Last visited June 1, 2013) (For an overview of the case).

⁵³ Print Disability defined: Any person who cannot effectively read print due to any type of disability or handicap is said to be Print Disabled.

⁵⁴ WHO, *Visual Impairment and Blindness*, June 2012, available at <http://www.who.int/media-centre/factsheets/fs282/en/> (Last visited on June 1, 2013).

formats – 7% in richer countries and about 1% in poorer countries. Any policy that exacerbates this exclusion needs to be carefully checked.⁵⁵

The question of enforcement is also important. Out of the ‘guilty’ group, how many will be actually caught? And how many innocent parties will be harassed by it? As it currently stands, India’s legal interaction with the digital world has been very sketchy. While the news of two young female facebook users preposterous arrest⁵⁶ was spread to the public which immediately lead to their release, two other Air India employees were in jail for 12 days as well as suspended from their jobs for a similar reason,⁵⁷ before they too were released. Unfortunately, these incidences are not surprising anymore. According to Google’s transparency reports,⁵⁸ the Indian government has the second highest incidences in the world of user surveillance requests. It seems that the unfortunate truth is that India is yet to adapt to the digital era without resorting to censorship and surveillance as methods of governmental control. The mandate of criminal sanctions for any type of infringing activity, commercial or not, is in dire need of correction. It is hopeful that an alert civil society ensures that abuse of the system is kept in check. However, equally crucial is that laws are appropriately made, worded and interpreted so as to not allow such abuse to occur in the first place. This is especially relevant given the vague implications of third party actions.⁵⁹

And finally, there is the question of whether the provision will be effective in achieving its goal of reducing copyright infringement regardless of costs. Looking at other markets is not very helpful as the concept is still relatively young world over. Thus the question remains open and its answer will depend on the amount of resources that go into enforcing the provision.

⁵⁵ Swaraj Barooah, *Not just a Trophy Treaty*, December 21, 2012, available at <http://spicyipindia.blogspot.com/2012/12/not-just-trophy-treaty.html> (Last visited on June 1, 2013).

⁵⁶ A student had questioned the city wide shut down over the passing away of a politician on her facebook profile, and another student had ‘liked’ the message. The two girls were arrested and later released on bail. The charges were made under the loosely worded §66(A) of the Information Technology Act, 2000 for offensive and hateful speech; *See Police who made Facebook Arrests Suspended*, November 27, 2012, available at <http://india.blogs.nytimes.com/2012/11/27/police-in-mumbai-facebook-arrests-suspended/> (Last visited on June 1, 2013).

⁵⁷ Prasant Naidu, *Two Air India Staff Arrested for 12 days for their Post on Facebook under Section 66(A)*, November 26, 2013, available at <http://www.business2community.com/facebook/two-air-india-staff-arrested-for-12-days-for-their-posts-on-facebook-under-66a-0340664> (Last visited on June 1, 2013).

⁵⁸ Heather Kelly, CNN, *Google: ‘Government Surveillance is on the Rise*, November 14, 2012, available at <http://www.cnn.com/2012/11/13/tech/web/google-transparency-report/index.html> (Last visited on June 1, 2013).

⁵⁹ *See* Pranesh Prakash, *Technological Protection Measures in the Copyright (Amendment) Bill, 2010*, April 29, 2010, available at <http://cis-india.org/a2k/blog/tpm-copyright-amendment> (Last visited on June 1, 2013)(For a discussion on the uncertainties posed by the section).

The Indian provision is a more balanced provision than most others;⁶⁰ while it may still not be a ‘desirable’ policy, it still does a better job of providing for fair dealing and other exceptions than other jurisdictions. However, the fact remains that India has a population of 1.2 billion people and a large portion of that population is at or below the poverty line. The most likely hypothetical situation in my mind is that regardless of resources put into the effort of ensuring that sales of private companies are not harmed, circumvention can and will continue to occur unchecked to a large extent. This will only lead to more wastage of resources, since the whole process is simply inefficient, while negatively affecting non-infringers. As shown above, DRMs affect how legitimate purchasers access their content, more than they affect piracy. This is because communication technology has continued its pattern of becoming increasingly efficient and smooth. In Kim Dotcom’s words,⁶¹ “What will Hollywood do when smartphones and tablets can wirelessly transfer a movie file within milliseconds?”

If this were the only way in which rights holders could protect their interests, it might hold stronger moral ground. However, developed countries have experienced that DRMs in fact affect legitimate users harshly as opposed to restrictions on piracy by way of changing business models to more user friendly ones.⁶² In fact, it is not difficult to conceive that DRMs often drive users to seek pirated products, rather than products with DRMs attached, as they are unnecessarily hindered by such measures, achieving the opposite of their intended effect.

On balance, seeing the large unjustified costs it incurs, its negative effects on non-infringers, the unlikelihood of effective enforcement along with its potential for abuse, and the presence of alternate options to protect rights-holders, it appears that anti circumvention laws are quite unnecessary and undesirable in India. The best-case scenario, in my opinion, would be the repealment of the relevant provisions. However, given that they are now present, it is important that the judiciary takes note of the Standing Committee’s report wherein they made clear that limited legislative guidelines were laid out so that the judiciary could play a more active role, taking into consideration public interest and local context.

⁶⁰ See generally Swaraj Baroah, *DRMs in the draft Copyright Amendments*, March 29, 2010, available at <http://spicyipindia.blogspot.com/2010/03/drms-in-draft-copyright-amendments.html> (Last visited on June 1, 2013).

⁶¹ *Kim DotCom’s Open Letter to Hollywood*, available at <http://opnltr.com/letter/kim-dotcoms-open-letter-hollywood> (Last visited on June 20, 2013).

⁶² Alvisi, M., Argentesi, E., Carbonara, E., *Piracy and Quality Choice in Monopolistic Markets* (German Working Papers in Law and Economics).