Effective Applicability of Sections 65A and 65B of Copyright (Amendment) Act, 2012 using Case Study of Digital Watermarks

Prateek Chakraverty†
†Jindal Global Law School, OP Jindal Global University

Received 26 February 2015; accepted 12 August 2015

With increasing utilization of Technological Protection Measures (TPMs) to protect digital copyrighted works, legislative changes to counter their misuse become necessary. With this objective, Sections 65A and 65B of the Indian Copyright (Amendment) Act 2012 were introduced. Section 65A delineates the Anti-Circumvention Law for effective TPMs while Section 65B protects the associated Rights Management Information. Several digital watermarking techniques are widely used for different kinds of protection to digital images, video, audio, databases, websites and e-books. The “effectiveness” of digital watermarks is prone to subjective assessment, not only because of their sheer variety in types, techniques and applications but also due to rapid technological advancements that continuously reshape the standard of “effectiveness”. Given this malleability, a case-case analysis of “effectiveness” may involve expert technical knowledge that is beyond legalese, thereby inviting miscalculation in justice due to subjectivity. In this paper, the scope and remedies for effective legal applicability of the aforementioned provisions in the light of certain grey areas are discussed. These include lack of a specific standard of “effectiveness” and invitation of corresponding technical excesses, skewed quantum of punishment, and the need to bring into ambit certain transformations that can lead to infringement without violating existing laws.

Keywords: Section 65A, Copyright (Amendment) Act 2012, technological protection measure, digital watermark, Digital Rights Management

With the advent of the digital age, copyrightable works are increasingly being produced in digital formats. The proliferation of digital media has led to increasing violations of copyright and Digital Rights Management (DRM) through rampant online attacks, thus putting such works to risk of counterfeiting, fraud and theft. However, the demand for such media is overwhelming due to their ease of production, distribution, display and storage. In the backdrop of such paradox, owners of digitally encoded copyrighted works resort to Technological Protection Measures (TPM) to ensure their security against malicious or benign online attacks.

TPM includes a range of techniques such as digital locks, encryption, passwords and digital watermarks. These techniques enforce a variety of access controls, copy controls and DRM on the digital objects. The Indian Copyright (Amendment) Act, 2012 incorporates certain provisions to provide legal backing to TPMs. Section 65A makes circumvention of an effective technological measure that protects any of the copyrights a punishable offense with two years imprisonment and fine. Section 65B makes it an offense to remove or alter digital rights information without authorization and to distribute any copyrightable works from which the digital rights information has been removed.

Of all the TPMs that are in vogue, digital watermarking is the one most widely adopted for according a variety of protection to digital documents. The end result of watermarking is a transformed document produced when the watermark, which is a digital pattern, is inserted into an original document in a manner such that its usability remains practically unaffected. Digital watermarks are intrinsically linked to their host documents, thereby providing them a durable, persistent identity and permanent protection as opposed to other TPMs such as Cryptography.

Digitally watermarked images, audio and video have been used since long and are quite common. Of recent, digital databases, e-books and websites are also being watermarked for adding a layer of security when they are launched in the web-sphere. It is expected that the use of watermarks as a cost-effective TPM will increase manifold in future as we veer towards a knowledge society where besides
images and video, well-researched and carefully crafted databases serving as information repositories are produced copiously.

The predominant use of digital watermarks is in the context of Intellectual Property Rights (IPR) and copyright protection. Digital watermarking is also used for sending across secret messages in steganographic applications. For the purpose of this paper however, we restrict our discussion to its IPR applications. Watermarks aids in establishing ownership proof in legal disputes, owner identification, detection of illegal tampering, enforcing copy control and access control, carrying digital rights information, tracking the transaction path of a document, and authentication of content. Thus, watermarks cover the entire spectrum of copyright and DRM. The use of watermarks permeates to electronic governance, electronic commerce and creative works of individuals. In the light of such widespread applications and popularity, watermarking would definitely fall within the scope of Sections 65A and 65B of the Copyright Amendment Act.

Motivation

Section 65A qualifies technological measures with the term “effective”. In other words, those watermarks which are “ineffective” will not fall within the scope of Section 65A. However, the legal endeavor is a precise one and it is observed that “effective digital watermark”, in its technical sense, does not convey all kinds of watermark, thereby leaving it to the Courts to decide whether a particular kind of watermark fits the bill to be accepted as an “effective” TPM.

It is contended that the choice of a watermarking technique for any given application involves a careful consideration of the possible trade-offs between various conflicting factors. For example, it is possible to use a highly secure watermark, but this may result in a compromise on efficiency. Some other factors include minimizing the degradation of image quality, eliminating false positive rates that deceive users into thinking certain works are watermarked when in-fact they aren’t, and robustness to withstand alterations. With so many factors coming into play, no watermarking scheme can be perfectly full proof. Indeed, it is difficult to assess the overall “effectiveness” of watermarks considering all qualitative factors.

Furthermore, as new watermarking techniques are developed, the very same technological advances can be tapped by adversaries to counter these TPMs and render them ineffective. This poses a challenge to the legal mind: how to define and interpret contextually the term “effective technological measure” as enunciated in Section 65A in a scenario where technological innovations as well as watermarking techniques and applications are constantly in a state of flux?

Contributions

In this paper, a re-look at the Articles 65A and 65B is taken in the context of watermarking as a TPM. Arguments are illustrated like how on one hand, it cannot be said for certain that a given watermark falls within the scope of Section 65A, as different kinds of such watermarks have different levels and standards of effectiveness. On the other hand, there is no clear, legally codified criterion for determining “effectiveness” of digital watermark. In fact, not even the minimum acceptable level of effectiveness is articulated. Thus, there remains a void in determining the standard of “effectiveness”. In light of such ambiguity, we propose to delineate the legal scope of “effectiveness” of Technological Protection Measure and propose remedies for the highly popular digital watermarks to fall within the purview of the provisions.

Some other aspects of Sections 65A and 65B are looked upon that can lead to ambiguity in dispensing justice. Firstly, difficulty in establishing the intention behind the very act of circumvention is examined and then deciding the quantum of punishment this entails. Secondly, highlighting the analog hole problem and some other transformations that can circumvent watermarks without leaving a trace, but these commonly occurring scenarios have not been considered. Suitable changes in these sections are presented so as to bring these situations into the ambit of law.

Overview of Digital Watermarking

In order to understand the benchmarks for assessing the effectiveness of different watermarking schemes, the variety of watermarks that exist must be appreciated, along with their security applications and their vulnerabilities. A brief tour of the domain of digital watermarking is present here.

The Watermarking Process

The process of watermarking begins with the selection of a watermark that is to be inserted within a document sought to be protected. The watermark itself is simply a digital pattern of zeros and ones.
which can be derived from any digitally encoded text, image, audio or video clip chosen or prepared by the document's owner. Though it can be any arbitrary pattern, a watermark usually carries meaningful information about the identity, origin and copyrights associated with the owner and the document. This pattern is superimposed on the original document by an embedding device called encoder, in a manner such that the quality of the document is hardly degraded and it remains useful. Now, the watermarked document is ready to be launched into the web-sphere for its intended application. The embedded watermark may need to be extracted later by another device called decoder.

The process of watermark insertion as well as extraction involves a set of secret parameters known only to the owner. The parameters depend upon the watermarking algorithms employed and can include one or more encryption keys. Though not mandatory, it is best to register the watermark and the secret parameters with a trusted legal entity so that legal succor can be obtained without any hitch, if a dispute arises later due to infringement.

Types of Digital Watermarks

Unlike paper watermarks, digital watermarks are of various kinds with different characteristics and applications. Watermarking techniques designed for images and video are broadly classified as perceptible (or visible) and imperceptible (or invisible) watermarking. Invisible watermarks are further sub-divided into robust, fragile and semi-fragile types. For digital databases and books, watermarking schemes can be grouped into two major categories: robust and fragile. Various classifications of digital watermarks are:

Classification According to Degree of Perception

- A perceptible (or visible) watermark is unobtrusively noticeable in the watermarked image or video. Visible watermarks can be destroyed or removed by active human intervention with image editors. An effective watermarking scheme must be robust against such attacks.
- Imperceptible (or invisible) watermarks are completely indistinguishable from the original cover images into which they are embedded. Unlike visible watermarking where removal involves human intervention, invisible watermarks in images are particularly susceptible to malicious attacks with common signal processing techniques. Hence, their design entails specialized algorithms that can resist alterations in the watermark due to signal processing.

Classification According to Degree of Robustness

- Robust watermarks can withstand repeated attacks with malicious intent to destroy the embedded watermark. However, hard an attacker may try to destroy it, the watermark still remains intact. Robust watermarking is used for establishing ownership of the watermarked document.

Robust watermarks are susceptible to a variety of attacks. Image based watermarks can be exposed to modification attacks, geometric attacks, cryptographic attacks and protocol attacks. Increased robustness ensures the watermark survives many image edits and file format conversions. Watermarks in digital databases can be attacked by tuple addition, deletion and alteration, attribute deletion, addition and re-ordering, randomization attacks, rounding off attacks, bit based attacks and linear transformation. Robustness is achieved by inserting the watermark in profusion all over the database.

The Self-Help Property of Robust Watermarks

If at all the attacker succeeds in destroying the watermark after massive attacks, he/she lands up with a highly degraded, unusable version of the original document. For example, an invisible watermark can be robustly embedded in the most significant region(s) of the host image such that tampering that portion with an intention to remove or destroy the watermark will degrade the aesthetic quality and value of the image. Likewise, in a digital database, the attacker is forced to delete, modify or add several records just to spoil the embedded watermark that invariably spoils its utility. Herein lies the technologically enabled “self-help” features of robust watermarks; they need not rely upon law to prevent circumvention as the very act of circumvention defeats the purpose of infringing copyrights. Nevertheless, legal backing puts in place necessary deterrents.

- A fragile watermark achieves just the opposite of robust watermarks - even the slightest change made to a document alters the watermark immediately. The watermark is essentially a “signature” of the original document which is
embedded in it discreetly. Fragile watermarks are used to detect tampering attempts to change the contents of the watermarked document. A problem with fragile watermarks is that it is not possible to distinguish between malicious attacks and unintentional benign attacks.\textsuperscript{14}

- A semi-Fragile watermark is “midway” between a robust and fragile watermark as it involves trade-offs from both of them. Such watermarks are more robust than semi-fragile watermarks and they carry the content's signature.\textsuperscript{14,15} They also show enhanced resistance to image processing based attacks.\textsuperscript{10} Since robustness requires an attacker to make several attempts to be able to infringe the watermark, semi-fragile watermarks can distinguish between malicious and benign attacks.

Both fragile and semi-fragile watermarks are subject to certain identified frequent attacks such as information leakage wherein the attacker tries to obtain information about the authentication key by a random walk through the image and protocol attacks.\textsuperscript{10} Thus, semi-fragile and fragile watermarks have a very high risk of circumvention.

**Classification According to Type of Copyright Protection**

Each combination of the visibility feature and the robustness feature gives certain unique properties to the watermarks which can be used for protecting the copyrights in different ways.

- Visible-Robust for displaying copyright: They are used for publicly released images and video to show the copyright-holder's logo and copyright information. The primary aim is to provide copyright protection by deterring unauthorized use of publicly released images and safeguarding the commercial interests and brand image of the organization associated with the digital image content.\textsuperscript{7}

- Invisible-Robust for ownership proof: An invisible watermark is content-rich, holding specific information about copyright, owner ID, address and details of the image document. Therefore, invisible robust watermarks can be used for establishing the identity of the owner of the work in case a legal dispute arises.\textsuperscript{10} Thus, such watermarks are valuable to gather unambiguous evidence of ownership and deserve legal backing against their circumvention. Furthermore, the watermark can also include biometric identification such as the owner's fingerprint or prerecorded voice.\textsuperscript{9} This helps in authenticating the contents of the watermark document.

- Robust-Invisible for access/copy controls: Robust-invisible watermarks are specially used in professional video to enforce copy control by writing a “no-copy allowed” diktat. Likewise, access control can be enforced by recording the allowed usages of the video and enlisting players that are allowed to access the video. The watermark can be read by a detector so that it knows whether the player is authorized to access, read or copy the content and where the source of the content originated.\textsuperscript{17} Thus, robust-invisible watermarks are useful in implementing DRM.

- Invisible-fragile for tamper-proof: Invisible and fragile watermarking schemes are used to establish whether a watermarked digital media was illegally tampered with in any way.\textsuperscript{13} This has immense value for collecting evidence of illegal copyright infringement and therefore must be brought under the ambit of anti-circumvention provisions.

- Invisible-Semi-fragile for tamper-proof with intent: Just like fragile watermarks, the main use of such watermarks is integrity verification/tamper detection.\textsuperscript{16} However, a certain degree of robustness is added so that a few attacks will not alter the watermark but more intensive attacks will destroy it. This helps to show the intent of the attacker, whether it was malicious or unintentional.

**Generic Features of Watermarks**

As discussed in the previous sub-section, different kinds of watermarks have specific characteristics that can be used to enhance their individual efficiency.\textsuperscript{3} However, there are certain common features that can be applied to evaluate their general effectiveness, such as:

- **Embedding efficiency**: This is the probability that a watermark is correctly detected in a watermarked document immediately after embedding, \textit{i.e.} before being exposed to attacks. Ideally, this probability should be 100%, but practical considerations of efficiency and fidelity requirements may necessitate a compromise.

- **Detection probability**: Probability that a watermark that is embedded within a document is correctly detected and extracted without knowing any of the secret parameters.\textsuperscript{10} For a watermark to
be effective, such probability should be extremely low.

- **Fidelity**: It refers to the perpetual similarity between the watermarked and the original versions of the cover work.\(^{18}\) A good watermarking method retains high fidelity.

- **Robustness**: It is the ability to withstand alterations caused by transmissions over a lossy channel or by malicious attacks that try to remove the watermark or try to make it undetectable.\(^{10}\)

- **Payload**: In order for more information to be included in a watermark, a bigger payload needs to be embedded.\(^{10}\)

- **False positive rate**: False positive rate is the frequency with which a watermark is expected to be detected in a non-watermarked document.\(^{18}\) It must be kept low.

- **Cost**: A watermarking scheme can be considered effective if the cost of extracting the watermark through unauthorized means far exceeds the cost of purchasing the watermark legally from the copyright holder by paying royalties. Note that the economic model of watermarking is highly complex and application-specific.

The above features can be used to measure the robustness, efficiency and quality of watermarks by observing results of experimentation using standard benchmarks. For example in the case of robustly watermarked images, the degradation in the quality of the image and the extracted watermark before and after being subjected to different kinds of attacks, can be measured in terms of the Peak Signal to Noise Ratio (PSNR) of the watermarked image/extracted watermark when compared with the original cover image/watermark.\(^{8}\)

### Applicability of the Relevant Law

The overview in the previous section brings home certain points about the applicability of Sections 65A and 65B in the context of watermarking as TPM. A discussion ensues:

**Watermarks Satisfy the Copyright Protection Criterion**

Section 65A requires that technological measure used should be meant for protecting any of the rights conferred by the Copyright Act. Emphasis is made on a point that all watermarks satisfy the copyright protection criterion. As discussed in the above subsection, robust watermarks mainly provide evidence on the ownership of a document and fragile watermarks help prove whether its contents were tampered with or not. Semi-fragile watermarks further allow discrimination between malicious and benign tampering efforts. These are all evidence-oriented and help establish copyright violations, rather than directly enforcing copy or access controls. Thus, they undoubtedly serve the purpose of protecting copyrights and are admissible from that point of view. Invisible robust watermarks carry DRM information and enforce copy and access controls. Visible watermarks deter copy attacks by direct human intervention. Hence, it is found that all kinds of watermarks pass the test of protecting copyright either by direct enforcement or by providing strong evidence or by carrying DRM information.

A distinct advantage of digital watermarks is that, being embedded within their host documents, they provide permanent protection as long as the document is live. This contrasts other TPMs such as passwords and digital locks which are separate from the document.

### Difficulty in Assessing Effectiveness

Section 65A positions the word “effective” before technological measures. It is this clause that turns out to be a grey area in the proclamation of the Act. Section 1201 of the Digital Millenium Copyright Act that clearly spells out circumvention of “effective access controls” as an offense.\(^{19}\) Thus, whereas the circumvention of access control TPMs is culpable (barring specified exceptions), one is legally allowed to circumvent copy-control TPMs. This is in sharp contrast to the Indian legislation, which is silent on any specific type of TPM that cannot be circumvented.

This may imply “presumably, TPMs could not be used to restrict access, only to restrict copying, communication to the public, and that gamut of rights…” as pointed out in the reputed cyber expert Pranesh Prakash’s post.\(^{23}\) The writer implies that a TPM applied for the purpose of preventing access to a copyrightable work is not admissible under Section 65A. However, we note that the access control TPMs prevent illegal access to a copyrighted work. If its circumvention is allowed, then an attacker can access the work without paying royalty and subsequently sell or distribute it. Therefore, it is concluded that the absence of any particular TPM in Section 65A actually broadens the applicability of the clause to all effective technological measures that protect rights accorded by the Copyright Act. It includes watermarks providing access-control, copy-control
CHAKRAVERTY: EFFECTIVE APPLICABILITY OF SECTIONS 65A AND 65B OF COPYRIGHT ACT, 2012

and DRM protection either directly or by dint of their ability to gather evidence on ownership, tampering or authenticity as the case may be.

This generic qualification would inevitably create problems as it is near impossible to find a universal standard for measuring “effectiveness” as observed in the case of digital watermarks. The next point further dwells upon this aspect. Discussion in the previous section brings home the point that the overall effectiveness of a watermark can involve trade-offs along different qualitative parameters. There are different levers such as robustness, fragility and payload size that can be tweaked to adjust the overall effectiveness of watermarks. Some illustrative examples are as follows:

- Robustness versus fragility: These two goals are recognized to be mutually contradictory. Therefore, if one desires both proof of owner using robust watermarks as well as proof of tampering using fragile watermarks, a dilemma arises. One may have to reduce the degree of robustness in order to incorporate fragility and vice versa.

- Encrypted versus plain watermarks: The security of a watermark can be enhanced by encrypting it with a secret key before embedding, thus making it extremely difficult to “crack” the watermark contents randomly. However, the price of enhanced security reduces the speed of watermark extraction because an extra decryption step is required. For real time applications such as streaming video-on-demand, this may be harmful.

- Payload versus fidelity/robustness: A robust watermark may include owner-specific and document-specific details in it. Now if the watermark length increases significantly, it may have an adverse effect on the degree of robustness or fidelity. For example, the owner likes to add his/her biometric information such as fingerprint, voice, face image or iris image into a watermark to authenticate the contents. But this would invariably bloat its size and if the content-to-watermark ratio exceeds a limit, the document’s fidelity to original will suffer for a desired degree of robustness. If however fidelity is maintained, then the level of robustness may reduce.

- Effectiveness—a composite measure: Effectiveness is a composite measure of several factors with different metrics for each. Thus, the factor PSNR indicates image quality, the correlation factor indicates correspondence between original and extracted watermark, and the factors precision, recall and accuracy assess biometric identification in authentication based applications.

- The technology-driven race: A prevalent paradox is that the very same technologies that are used to develop innovative watermarking schemes are available to attackers who can tap them to create circumvention tools. This triggers a race between developers and attackers and a result, the benchmark standards for “acceptable effectiveness” need to change with time to remain relevant.

In all the above cases, application-specific trade-off considerations would force a compromise along different qualitative dimensions. The moot point is, does this render them ineffective?

The interpretation of effectiveness is contextual, depending upon the intended application and the relative priorities of different quality features that it demands. It is found that there is no fixed standard of effectiveness as the permutations and combinations of various parameters for specific kind of watermarks do not conform to a single reference point. Hence, it would be the task of the court to determine effectiveness of a digital watermark. Unfortunately, in the situation when a digital watermark is found to be “ineffective” due to lack of technical foresight, Sections 65A and B would not be attracted and the rights of the claimant would not be secured. Thus, the concerned legislation in its current form is not without lacunae.

Transformations Ignored in Section 65B

Section 65B prohibits deletion and alterations to the digital rights information carried by a TPM. It may be noted that digital watermarks are intrinsically embedded within the cover document and can suffer mutilation whenever the watermarked object itself is changed in any way. Now the document can be attacked by the same methods such as deletions, additions and modifications. More significantly, its contents can be “transformed”, i.e. changed from one form to another. Classic transformational attacks on multimedia objects are JPEG compression for images and MPEG compression for video. An image can also be rotated, skewed etc. In digital databases, a particular field (attribute) can be linearly transformed from one unit to another, say centigrade to fahrenheit for temperature field. The watermark can be
destroyed in the process of such simple or complex transformations. However, Section 65B in its current form, is amiss in not including such a possibility.

**Questionable Quantum of Punishment**

There are several situations wherein an unwary user may infringe the watermark such as when unauthorized parties insert watermarks in case of fragile watermarks and an innocent party fall his hands on the damaged protected content. In such cases, “intention” may be hard to prove. Therefore, imposing criminal sanctions would be an excess quantum of punishment as circumvention with intention may not be possible “beyond a reasonable doubt”.

**No Provisions for the Analog-Hole Problem**

The Analog-hole problem refers to a frequent occurrence in mainstream commercial media protected by a digital watermark. A pirate can simply sneak in a camcorder into a poorly monitored room where a movie is being screened, record the analog output in this analog device and then re-converted it to digital form. This process can completely obliterate the watermark and at the same time, the attacker escapes the liability of direct circumvention of a TPM. Pirates can also use analog signals audio from loud speakers and video on a display to dishonestly market them by digitizing them and then distributing the files. Sections 65A and 65B do not include any explanation or even a reference to the analog-hole problem to highlight it as a special case of circumvention.

**Recommendations**

The Indian Copyright Act 1957 vests in the person holding a copyright a bundle of rights including, *inter alia*, rights of reproduction, communication to the public, adaption and translation of the work. The discussion so far clearly indicates that the legislation related to TPMs needs ironing out in order to seamlessly accommodate within its ambit, the highly popular digital watermarks, in order to bring to justice unauthorized circumventors and to prevent imposition of disproportionate liability on innocent infringers. In this context, the following solutions have been proposed-

**Define the Scope of the Word “Effectiveness” in Sections 65A and 65B**

It is observed that problems may arise if the word “effective” is left undefined in the Act. Therefore, following alternative routes have been suggested-

- Enumerate the different kinds of TPM explicitly in Section 65A so that the qualifier “effective” can be applied to each watermark according to its specific combination of features.
- Define the word “effectiveness” such that it is universally applicable for all cases involving TPMs.
- Remove the word “effectiveness” altogether from the impugned sections.

Now, taking into consideration all the aforementioned proposals, the solutions can be contretized as follows:

(a) Explicitly enumerate different kinds of TPMs: It is contended that the traditional distinction made between access-control and copy-control TPM/digital watermark is redundant. Firstly, a person who bypasses a TPM to gain access to a work, would in all likelihood copy as well as distribute the work, after circumvention of the TPM. Secondly, current technology allows a common watermarking scheme to be used for access as well as for copy control. We also believe that both direct controls as well as TPMs that serve to provide evidence are “effective” protectors of copyright. Each of the evidence-oriented watermarks effectively serve the course of law by serving as useful evidence in case of dispute and indirectly deters infringers from distributing the concerned work. The recognition that circumvention of both kinds of TPM whether access-control or copy-control by circumvention tools is found in Canadian Bill C-32 – the counterpart Canadian statute that aims to prevent circumvention of works protected by TPMs. In the light of these arguments and in order to remove any confusion about the admissibility of a watermark before its effectiveness is evaluated, Section 65A can explicitly state “effective access control, copy control and evidence based technological measures”. This will enable each type of protection measure to be evaluated according to its own set of features.

(b) Universally applicable effectiveness criteria: Theoretically speaking, an effective watermark would be one which is unobtrusive, discreet, easily extracted and robust or fragile as the case may be. However, it has been seen, practically the investigation for measuring “effectiveness” would involve a consideration of wide-ranging factors, differing in case of different kinds of watermarks. Instead of venturing to forge a universal standard of
“effectiveness”, certain simple criteria can be laid out. One of them can be the requirement of a *secret key* to extract the TPM. The existence of key ensures that an attacker would find it difficult to guess it randomly and hence a minimum acceptable level of security is ensured. Encryption, passwords and locks require a key in any case. With such a stipulation, owners of watermarks will also encrypt it with a key before embedding. Another condition can be that the quality of the watermarked document should not fall below an acceptable level when compared with the original. These two simple criteria can effectively resolve the judicial process in analyzing the word “effectiveness” of a digital watermark.

(c) Remove the qualifier “effective” altogether: It is alternatively proposed that the word “effectiveness” in the Section 65A of the Act be removed as the same is redundant. It may be noted that the distinction between access control and copy control TPMs is now blurred.24 This has been recognized to be a problematic distinction in critics of the DMCA Act.24 Such a distinction does not exist in the Indian Copyright Act, 2012. It is suggested that the main purpose of the inducted provision is protection of rights vested by the Act. The liability of the infringer is with respect to the damage done to the protected work including damage done to the TPM/watermark itself. The circumvention of a TPM, howsoever ineffective, should not be a ground for the infringer to escape liability in case he has intentionally infringed upon the rights of the copyright owner. The point holds further substance in light of the fact that it is practically impossible to arrive at a legal standard of “effectiveness”, as observed above.

**Modify Quantum of Punishment**

The quantum of punishment as specified in the impugned sections is very high considering the fact that the infringement of digital watermark may be miscalculated on grounds of questionable ownership claims, questionable intent behind infringement and vastly frequent occurrence of infringement thereby inviting undesired deterrence on consumers from accessing works. In order to appreciate the probability of miscalculation, each of the aforementioned grounds is discussed below-

(a) *Questionable Ownership Claims*

Digital watermarks may have variable ownership claims. This may occur when unauthorized parties may leave their mark on a fragile watermark. Further, the ‘deadlock problem’ is a frequent occurrence wherein a pirate inserts a watermark in publicly available content and claims he or she is the legitimate owner of the copyright-protected content.26 Current watermark-based copyright schemes are unable to establish who watermarked the data first.24 The basic essence of such problem is that multiple ownership claims cannot be factored to the real identity. Thus, notwithstanding the methodology of insertion and its effectiveness, the factual problem of ownership remains. Other ownership based problems include situations when attackers remove embedded watermarks, cause embedded watermarks to be undetectable, replacement of existing watermark with a false one and insertion of an additional watermark into copyright-protected content.24

(b) *Questionable Intent Behind Infringement*

It is quite probable that an innocent attacker may incur liability. This may be due to duplicity of ownership claims as observed above, when a person unknowingly tampers with a digital watermark, or in other such innumerable situations where it is improbable to calculate the intention behind an “accidental” infringement of digital watermark. Given the popularity of the technique in media, documents and works, it is quite probable that hundreds of claims may arise with respect to circumvention of digital watermark, with questionable intent behind infringement. In light of the vast scale of use of digital watermark, as observed above, there would be an undesired deterrence on consumers of information protected by digital watermarks due to apprehension of accidental tampering and thereby incurring punishment of two years and fine. In other words, the criminal provision’s standard of proof is ‘beyond a reasonable doubt’. In effect, this situation brings out several contradictions, namely: one, low scope of convictions due to the ambiguous nature of the word “effective” and questionable intent behind circumvention, thereby defeating the purpose of Section 65A which is protect the rights vested in the Act. Two, the high quantum of punishment acting as deterrence to consumers of information protected by digital watermarks, as observed above.

In view of the above miscalculations in adjudication of claims of infringement of digital watermarks, it is proposed that the quantum of punishment for circumvention of TPM be reduced to the standard of 'preponderance of probabilities' as
opposed to 'beyond a reasonable doubt'. In other words, in case intent is questionable, as would be the case due to the high rate of usage of digital watermarks in mainstream media, and the preponderance of probabilities tilts towards the defendant, punishment may only be restricted to fines. Further, in case of proven malicious intent behind circumvention, penal fines may be awarded.

Include Provisions for Tackling the 'Analog-Hole' Problem

The investment put in by the owner of a work in putting of TPM such as digital watermark must not be let down by an instance of analog-hole based bypassing of the TPM. To curb the malpractice of tapping the analog-hole, the US Congress introduced the “analog-hole” legislation, also known as the Digital Transition Content Security Act 2005, which is not yet enacted but promises to act as an effective deterrent on such malpractice of circumvention of TPM.

It has been argued above that the word "effectiveness" is redundant in the context of Section 65A. Thus, it would be prudent to consider including provisions that specifically deals with the analog-hole problem. This is further substantiated by the fact that such problem is persistent for all TPM, regardless of their effectiveness.

In order to include provisions regarding the analog-hole problem, we may take cues from US' Digital Transition Content Security Act 2005. A detailed scrutiny of the proposed legislation may find relevance in the Indian Copyright (Amendment) Act 2012 as an Explanation to the Section 65A, including the analog-hole problem within the scope of the word 'circumvention' as follows: Circumvention of a TPM includes usage of an analog video input device or related technology for the purpose of converting into digital form an analog video signal that is read from a prerecorded medium containing digital copyrightable work protected by a TPM. In other words, if a person knowingly converts a copyright-protected work with TPM such as digital watermark into an analog signal and then reconverts it to digital format using an analog video input device, he would be liable for circumvention of the TPM, notwithstanding the fact the conversion from an analog signal did not include a TPM as the prerecorded version was obtained from the original work protected by TPM.

In order to allow for protection of Rights Management Information, due to the analog hole problem, the word “transform” may be added to the words “removes” and “alters” in Section 65B(i). The word “transform” is different from the word “alters” as the former refers to conversion of signal from one medium (digital/analog) to another (digital/analog) whereas the latter refers to change in content of the protected work after circumvention of the TPM (digital watermark).

Lastly, the legal framework is built on incentives and deterrents. In this case, the analog-hole problem usually occurs in the entertainment sector. The sector enjoys a huge public outreach. Therefore, a substantial deterrent may be in place in the form of substantial fines exceeding the cost of the concerned digitally-watermarked work, taking cues from the US legislation. Such penal provision may be appended to Section 65A circumvention of TPMs in digital works that have artistic value by the convenient analog hole would incur liability to the tune of multiple of the cost of the original work.

Conclusion

Digital watermark is an important TPM that protects all aspects of copyrights and DRM through evidence collection, access controls, copy controls and carrying DRM information. It is highly popular in the movie industry as well as the State for protecting the copyrights of their digital content. However, since it is transmitted and spread over a network, it has a high vulnerability towards attacks/circumvention thereby attracting the scope of Sections 65A and 65B of the Copyright (Amendment) Act, 2012. Taking a closer look at the Section 65A, it is observed that it lacks clarity on the words "effectiveness" and "circumvention". The standard for measuring effectiveness of a TPM such as digital watermark is highly subjective to context and kind of watermark. Further, the technical benchmarks of measuring such effectiveness may be beyond the effective scrutiny of a court of law. In the same vein, the word "circumvention" needs explanatory footnotes which clarifies to the reasonable person not ordinarily schooled in technical knowledge to include specific instances of tamper-detection and analog-hole problem, as such do not directly involve infringement of the concerned TPM but in effect is able to bypass the protection afforded by the concerned TPM.

Particularly, the analog-hole problem is an important situation which occurs on a large scale due to proliferation of digital media, and needs redressal in the legislation by inclusion of the word "transforms" in addition to the phrase "removes or alters" in...
Section 65B(i) of the Act. Lastly, in light of the frequent usage of works protected with TPM causing high probability of accidental circumvention coupled with the fact that it would be difficult to ascertain "intent" behind the technical circumvention, the quantum of punishment may be different from the one for ordinary copyright infringement which involves both imprisonment and fine. It is proposed that the subject to a case-case basis by delineating civil damages for general circumvention and criminal penalties for circumvention with proven malicious intent.

References
16. Different kinds of watermarks are “effective” for different reasons and circumvention may not be the criteria for measuring efficiency (ref. Invisible watermarks), as opposed to the central theme of the legislation i.e. Sections 65A and B.
19. Access control technologies are technological protection measures which are used by Copyright owners to control access to their content. http://www.smartcopying.edu.au/copyright-guidelines/hot-topics/technological-protection-measures (accessed on 8 July 2015).
20. To illustrate, “Regardless of any digital or software copy control mechanisms, if sound can be heard by an ear, it can also be recorded by a microphone, and either stored by analog means (e.g. magnetic tape), or recaptured digitally. And if images (static images or video/film), including text, can be seen by the eye, they can also be recorded by a camera. In the case of text the image can be converted back to text using optical character recognition.” Overview, https://en.wikipedia.org/wiki/Analog_hole (accessed on 8 July 2015).