ARTICLE:

DIGITAL WATERMARKS AS LEGAL EVIDENCE

By **Maurice Schellekens**[1]

Digital watermarks allow the invisible and indelible incorporation of information in an item of intellectual property, such as a digital picture or a digital movie. Digital watermarks can be used for the detection of copyright infringement. This article considers one particular application of digital watermarks: tracing the source of an illegal distribution. The evidential value of digital watermarks is considered. The article identifies areas of concern with respect to the legality of proof and with respect to the scientific aspects of proof by digital watermark. The article concludes with a few wider considerations concerning the use of digital watermarks for the purposes of enforcing intellectual property rights.

Introduction

A digital watermark is meta- information that can be added to a work such as a picture or a movie. The watermark is imperceptible to the user of the work and is difficult to alter or remove. Digital watermarking technology can be used for a range of legal applications, including copyright protection. In this context, the technology could be put to a number of uses, such as watermarks that identify the author or rights holder, or watermarks that carry information identifying the work, which could be used by playing devices, or by Internet Service Providers (ISP) for the purpose of recognizing copyrighted materials. This article will not address these applications, but focuses on a particular application of digital watermarks, that of tracing the source of an illegal work. It functions like this: a watermarked work is given to a limited number of licensees, for example movie theatres. After a while the work might appear on the internet without permission of the rights holder. With the help of the digital watermark in the internet-copy of the work, it is relatively easy to retrieve the code that indicates which of the licensees might be responsible for failing to secure the movie appropriately. This article investigates whether information deduced from digital watermarks could and should be used as evidence in legal proceedings. In particular, it will focus on the limitations that the right to privacy and the science underlying digital watermarks should impose. The focus will be on Dutch law.

In the following section of this article, the aims and context of the use of watermarks for copyright infringement protection purposes is explained. The third section analyses the legal issues arising when using watermarks for evidentiary purposes. Issues concerning reliability, legality and scientific validity of digital watermarks will be addressed. The fourth section analyses how contract law can be used to diminish the evidentiary risks associated with the use of watermarks and the limitations that watermarks impose in this context. Finally, the wider implications of the use of digital watermarks will be addressed, both for users of watermarked works, and for the enforcement of copyright.

The context of copyright infringement protection

Although the use of digital watermarks for copyright infringement protection purposes may take place in many different contexts, one such context – the movie industry – will be described here to set the scene for understanding watermarking as a means for copyright infringement protection. The movie industry has an elaborate business model for bringing movies to the market and to increase the revenue that a movie yields. Although the exact business model may differ from production company to production company and even between movies, a typical business model is provided. A new movie is first circulated among a number of reviewers who write comments on the movie and publish them in widely read periodicals and internet sites. The production companies hope

1 *This article has been written as part of the DaVinci project, a collaboration between VUB/ETRO and the Tilburg Institute for Law, Technology, and Society, funded by IBBT and ICTRegie. At the Department of Electronics and Informatics (ETRO) of the Faculty of Engineering Sciences in Brussels, a mathematical approach to lattice based watermarks is being developed. The author is indebted to professor Ann Dooms for the valuable comments she provided to an earlier draft of this text.*

that these reviews whet the appetite of the public to go and see the movie. When the movie is released to the public at large this is done exclusively in the profitable market of the movie theatres. The movie is later released on DVD for the rental market, such as hotels or airline companies. When this market is saturated, the movie is licensed for broadcasting on television or the internet. The business model is disturbed if pirated copies of a movie appear on the internet, especially if it happens in the earlier stages of the exploitation of the movie. Therefore, most production companies take measures against pirated movies appearing on the internet. The traditional response is to take action against the person that placed the content on the internet or the ISP that hosts the movie file. Typically, enforcement focuses on the links in the illegal distribution chain. It may, however, be more efficient to try and prevent the illegal distribution at the source, such as the reviewer who leaked the movie to the internet or the movie theatre that may not have done enough to stop members of the public from recording the movie in the theatre. In general, the source is the person or entity within the limited circle that rightfully has a copy at its disposal and whose copy somehow finds its way to an illegitimate distribution channel.

One reason for the rights holder to identify the source is to enable him to investigate whether the licensee has done enough to prevent the work from being distributed without authority. If the security measures in place are not sufficient, the rights holder may be able to take measures to prevent a leak from occurring again, such as future exclusion of the licensee or requiring the licensee to implement improved measures against leaks. The rights holder may also want to recoup damages from the licensee. The behaviour of the licensee may also constitute indirect copyright infringement or breach of contract. It might be that the licensee or their employee engaged in criminal behaviour, such as aiding and abetting copyright infringement. The rights holder may also want to pursue any legal remedies in this respect.

The traditional way of identifying the source of the illegal version of the copyrighted material is to identify the person who placed a work on the internet, and request a court to order the defendant or the person suspected of uploading the infringing work to make known his predecessor from which he obtained the infringing materials (compare article 1019f Dutch Code of Civil Procedure 'DCCivP').[2] This process can be a burden, because it might take some time before the rights holder identifies the person responsible for the breach.

Digital watermarking provides an easier way to identify the source of the breach. Upon distribution, each copy is digitally watermarked with a copyright infringement protection code. Each licensee obtains a copy with a unique watermark that identifies him as the licensee. In this way, it is possible to detect the relevant licensee quickly, once a pirated and watermarked copy has been discovered on the internet. Identification of the licensee by watermarking fulfills a pressing need, especially if other methods of identification, such as following the links of the chain, are impossible or uneconomical.

Mere identification of the licensee is one step. If measures are to be taken against the licensee and the licensee is not willing to comply, it is relevant to know whether the detection by watermark provides adequate evidence of the identity of the licensee. Although a degree of certainty about the identity of the registered licensee does not indicate what role, if any, he or she played in failing to control the intellectual property, it is an important first step in building a case to take further measures. Either the watermark and the infrastructure in which it is included provide direct legal proof of the identity of the licensee, or based on the detection of the watermark, further legal measures can be taken to arrive at a proof of the identity of the licensee. An example of the latter is the preliminary witness

2 *Article 1019f DCCivP is the Dutch implementation of article 8 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights OJ L 157, 30.4.2004 and OJ L 195, 02/06/2004 p. 16 – 25: Right of information 1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who: (a) was found in possession of the infringing goods on a commercial scale; (b) was found to be using the infringing services on a commercial scale; (c) was found to be providing on a commercial scale services used in infringing activities; or (d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services. 2. The information referred to in paragraph 1 shall, as appropriate, comprise: (a) the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers; (b) information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question. 3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which: (a) grant the rightholder rights to receive fuller information; (b) govern the use in civil or criminal proceedings of the information communicated pursuant to this Article; (c) govern responsibility for misuse of the right of information; or (d) afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right; or (e) govern the protection of confidentiality of information sources or the processing of personal data.*

statement (article 186 DCivCP),[3] that is the possibility to summon and hear witnesses before the actual proceedings have started. A rights holder may thus summon the identified licensee to provide witness evidence about the circumstances under which the watermarked intellectual property was copied to the internet.

In general, the standard of proof required for evidence in relation to such preliminary measures is low, and the quality of information derived from watermarks is generally adequate for such purposes. Nevertheless, there may be other circumstances that make the indirect route less attractive or even impossible. For example, the witness may deny any involvement or claim to have no recollection of the relevant circumstances. In criminal law, the authorities can use investigatory powers to obtain further evidence, but the use of many of these powers requires a suspicion of committing a criminal offence. Identification by watermark may be sufficient to found a suspicion of, for example, aiding and abetting copyright infringement. However, most powers can only be used if there is a suspicion of a criminal offence that is punishable with a prison sentence of at least four years (article 67 Dutch Code of Criminal Procedure 'DCCrimP'). This holds for example for the most useful power of claiming stored data (article126nd DCCrimP) that may, for example, be exercised against an ISP or a hotel. However, intentional copyright infringement is only punishable with a prison sentence of up to 6 months (article 31 Dutch Copyright Act 'DCA') and thus falls well short of the condition. Only if copyright infringement is committed in a professional or business capacity it is punishable with a prison sentence of up to four years (article 31b DCA). However, aiding and abetting such copyright infringement would then again fall under the four year threshold: it is punishable with up to 2 years and 8 months imprisonment (article 49 Dutch Criminal Code 'DCC'). This means the police have limited powers to investigate further on the basis of detection by watermark.

In conclusion, information derived from watermarks is generally adequate to obtain further evidence. In practice however, other circumstances may prevent the rights holder from taking further measures. Therefore, it is worthwhile to investigate the potential that watermarks themselves have as a direct means of evidence.

Proof by digital watermark

The preceding section raises the question whether, and if so under what conditions, the identity of the licensee can be proven directly with the help of digital watermarks. The rules of evidence differ between civil and criminal cases.

Formal means and assessment of evidence

The Dutch Code of Criminal Procedure has a closed system of formal means of evidence. If the results of the detection and further investigation of a watermark are laid down in a document, the document can be part of the proof as a 'geschreven bescheid' (a written document). The probatory value is to be decided by the court. The Dutch Code of Civil Procedure permits evidence to be provided by any means (article 152.1 DCCivP). There is no closed system of formal means of evidence. A court determines for itself what value it attaches to a watermark as a means of evidence (article 152.2 DCCivP). Evidence by digital watermark is basically possible in the Netherlands. Any evidence that can shed light on the probanda may be adduced in court. However, the court is free to evaluate evidence of the watermark. Naturally, a defendant can contest the evidence that the claimant deduces from a digital watermark.

Disputing evidence

A defendant can challenge the watermark in three ways: (i) he may contend that the evidence is unreliable, that is it is unfit to prove. This may be, for instance, because the digital evidence was not handled correctly; (ii) he may have legal objections against the evidence, for instance where the evidence is gathered or presented in an unlawful way; or (iii) he may question the scientific validity of the evidence. These categories are not mutually exclusive. Evidence may be both unreliable and unlawful. The third category could be said to be an instance of the first category. It is dealt with separately here because of its particular character.

Reliability of the evidence

The reliability of the evidence may be challenged in various ways. Examples include:

3 *For an additional discussion on Dutch law relating to electronic evidence, see Dr. Simone van der Hof, Réno Pijnen and Simone Fennell-van Esch, 'The Netherlands' in Stephen Mason, general editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

1. Whether the item in question was actually found on the internet.

2. The entire process of affixing, registering and detecting digital watermarks was not executed with the required care and attention and therefore the watermark is unreliable as evidence.

3. The integrity of the database containing the registrations of affixed watermarks is compromised so that the mapping from 'watermark' to identity has become unreliable (for instance as a consequence of criminals hacking into the database).

4. A licensee did not enrol under his own name. Hence, the data in the watermark is not necessarily sufficient to establish his or her identity.

Whether these contentions are successful depends on the extent to which the defendant can corroborate them with additional facts. The contentions can largely be preempted if the rights holder takes adequate measures beforehand. Such measures can include a combination of technical (firewall and virus protection of the database), procedural (identity checks at enrollment, procedures for registration of what picture was found where, when and by whom, safe storage of retrieved pictures, watermark detection in a safe environment, providing for possibilities for contra-examination) and institutional measures (outsourcing watermarking and detection to a third party). Where doubts continue to be raised with respect to the reliability of the evidence, even where it is proved that the rights holder took such measures, it will be for the court to decide whether it shares the doubts and if so, whether they make the evidence unusable. When rendering its decision, a court will look critically at the credibility of the doubts in view of the measures taken to safeguard the reliability of the evidence. In any event, the court is free to assess the evidence before it and to attach the value to it that it sees fit. The party relying on the watermark may try to reach an agreement with the licensee about the evidence in order to deal with any uncertainty relating to the court's discretion to assess the evidence. Such an agreement can resolve many of the uncertainties that exist under the statutory law of evidence. Agreements about evidence only affect the parties privy to the agreement and only in civil proceedings. These agreements will be dealt with below.

Legality of the evidence

The legality of the evidence can be disputed in various ways:

1. The evidence was obtained using a covert means (possibly) infringing human rights such as privacy.

2. Personal identifying information was registered at a moment that no suspicion of infringement existed, thus infringing privacy or data protection rules.

3. The combination of watermarking, registration and detection gave insight to patterns of communication or information such that it impinged upon the unencumbered exercise of the freedom of expression as meant in article 10 ECHR. Basically, it is contended that the evidence was gathered or presented in an unlawful way and that this unlawfulness should be a reason to apply the exclusionary rule, that is to disallow the evidence.

Two questions arise. First, it is necessary to know the conditions by which evidence was unlawfully obtained. Second, if evidence was obtained unlawfully, whether it should it be excluded.

With respect to whether the evidence can lawfully be admitted, criminal and civil law differ. In criminal law, the gathering and presentation of evidence is subject to the legality principle: the police and judicial authorities may only exercise powers that infringe upon human rights if they have been statutorily granted to them.[4] In defining the powers and the conditions under which they may be used, the legislator balances the benefits of exercising the power against the infringement of human rights such as privacy. Evidence gathered without an adequate legal basis infringes privacy and is basically unlawful. Other reasons for excluding evidence in criminal proceedings may be that, where there is a statutory power, the required formalities have not been

4 *In the Netherlands: Enquêtecommissie opsporingsmethoden (colloquially known as the van Traa Commission) Inzake Opsporing, 1996, available at: http://www.burojansen.nl/traa/index.htm.*

If watermark based evidence gathered by civilians is later used in criminal proceedings against an infringer, the gathering of evidence is mostly judged against civil standards

complied with or even if the formalities have been complied with, the exercise of the power may be disproportionate, in that no reasonable relation may exist between the costs of the exercise of the power and the purpose that is to be attained by it.

In civil law, the parties to the action gather the evidence. The gathering of evidence may not breach statutory rules, may not infringe upon subjective rights or may not lack due care. Providing evidence has been obtained lawfully, all methods may be used to collect evidence.

The actions of private persons are not governed by the legality principle. If watermark based evidence gathered by civilians is later used in criminal proceedings against an infringer, the gathering of evidence is mostly judged against civil standards. This does not hold if the police actively solicit the gathering of civil evidence in order to evade the constraints of public law. The use of digital watermarks for the purpose of enforcing intellectual property rights will mainly be used in a civilian setting. To the author's knowledge, there are no public policy documents in which watermarking is seen as a task for government. The failure to gather evidence lawfully is dealt with according to civil standards. If publicly funded institutions such as museums or archives use watermarking, they are not subject to the legality principle. This is not seen as exercising a typically public function, but merely as enforcement of their civil interests.

In practice, a breach of privacy is the most prevalent reason for the evidence to be refused admission into proceedings. For this reason, the discussion is restricted to whether watermarks could infringe privacy. The privacy implications are dependent upon the way in which copyright infringement protection is implemented using watermarks.

As a preliminary issue, it is relevant to know who or what is being registered as a licensee. A watermark may refer to a legal entity, such as distribution companies, or to individuals. In the former case, the identifying details of the company are registered. It is assumed that this does not raise a privacy problem. In case individuals (such as reviewers) are being registered, the question of privacy is self-evidently relevant.

For the purposes of analysis in relation to privacy, it is important to discern four stages of the watermark process:

1. Affixing the watermark to the intellectual property. This is the necessary preparatory act required to make it possible to trace the person responsible for breaching copyright later on in the process.

2. The presence of the watermark in the intellectual property. At this stage, it is relevant that people without authority do not obtain access to the data in the watermark. In essence, there are two options in respect of the information to be included in the watermark: the watermark comprises data that directly identifies a person or legal entity, such as name, address and dwelling place are placed in the watermark, or an indentifying code is inserted that in itself carries no information about the registered licensee. The first option requires the watermark to be encrypted in order to prevent unauthorized access to the information it contains. It is possible to encrypt the watermark only, while the rest of the picture is not encrypted.[5] The latter option requires the user of the watermark to maintain a database that enables the code to correspond to a physical identity. It is necessary for the database to be secured against unauthorized access.

3. Reading the watermark. This is relevant because it

5 For JPRG 2000 this has been standardised in JPSEC 2000 Security (Part 8 – JPSEC), ISO/IEC 15444-8:2007.

creates a relationship between the person or legal entity recorded in the watermark and the appearance of the work in a place where it should not be. The watermark can be read by the content provider, rights holder, or by a third party.

4. The use of the results of reading the watermark. The data from the watermark taken together with the facts of the circumstances in which the intellectual property is found, will give rise to information that can be used to take appropriate action by the rights holder, if it is deemed necessary.

A privacy analysis cannot focus on a single stage in isolation, but must assess the process as a whole. When taking data protection as the starting point of the analysis, the following picture may arise. Article 8 subparagraph f of the Dutch Data Protection Act (DDPA) provides that processing is justified as follows:

> 'Art. 8 WBP: Persoonsgegevens mogen slechts worden verwerkt indien: [...] f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.'

> 'where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the registered licensee.'

It is necessary to ascertain what legitimate interest the user of the watermark has in using a watermark and whether the process meets the requirements of effectiveness, proportionality and subsidiarity.

The first step is straightforward. A copyright owner has a legitimate interest in enforcing his copyright, and digital watermarks are a technology that is helpful in this respect. The second step is more elaborate and must take into account the different choices that can be made when implementing a watermarking scheme.

The effectiveness of watermarking can be made plausible as follows: it is usually more effective to deal with enforcement at the point at which it occurs, that is by closing down a source of copyrighted material, rather than prosecuting all those who place a work on-line. In copyright cases, it is not unusual to require an infringing party to reveal the source of the infringing materials. Watermarks used for copyright infringement protection purposes are the ideal means to quickly identify a source, and are helpful in enforcing copyright. Effectiveness does not appear to be too large a hurdle to overcome.

Proportionality poses a more significant challenge. One issue is whether watermarks are a reasonable means to an end. Watermarks affect the privacy of the registered licensee. The information that can be derived from a watermark and the circumstances in which the intellectual property is found can be used to draw conclusions about the registered licensee and help the drawer of the conclusions to decide how to approach or treat the registered licensee. The presence of the watermark provides no information about the way in which the cover-work leaked to the internet; neither does it give information about the role of the registered licensee, if any. Hence, the privacy interests of the licensee make it necessary to consider how watermarking is implemented. For the sake of clarity, this analysis will be structured by distinguishing the different stages of the watermarking process.

At the stage of affixing the watermark and handing the marked item of intellectual property over to the licensee, it is necessary that the registered licensee be informed about the presence and contents of the watermark, especially since it is covertly present in the work, and he may not have any other way of knowing that his or her data are being processed (article 33 DDPA). For the second stage, the period between affixing and reading, the information that is actually put into the watermark is relevant. As noted above, there are two alternative options: first, including directly identifying information into the watermark, such as the licensee's name, address and dwelling place. Second, an identification code may be put in the watermark, such as a random number. In the latter case, the content provider or a trusted third party retains a database that provides a link between the identification code to the physical identity, such as name, address and dwelling place. Although the

latter implementation is more elaborate, it may have an advantage in terms of the amount of data included in the watermark. An identification code is more compact than a reference to the attributes of a physical identity, and a shorter watermark is easier to hide in a picture or other item of intellectual property. More importantly for data protection purposes, the consequences differ, depending on the approach adopted. In the first approach, the licensee becomes the custodian of his own data. The protection of the right holder's copyright and protection of the licensee's personal data are brought together. If the licensee does not share the work for privacy reasons, the right holder's copyright is automatically protected. The licensee must obviously be informed of the exact data present in the watermark; since the watermark is imperceptible he cannot see so for himself. With this knowledge, he can take adequate measures to protect the data against unauthorized access. Furthermore, it enables him to exercise his right to correct the data, should the data prove to be wrong. From a data protection perspective, this alternative seems to be straight forward. The second option is more complicated from a data protection perspective. Here, the content provider or a third party is responsible for the personal data, and will have to take the measures necessary to protect the data against unauthorized access.

In the third stage, who reads the watermark is relevant: the user of the watermark or a trusted third party (TTP). In the latter case, extra care towards the registered licensee can be built into the process by stipulating the conditions under which the TTP may provide data to the user of the watermark. A possible condition could be that the user of the watermark can obtain access to the data where a registered licensee is involved in more than one breach of the licence. In the absence of a TTP, the care due to the registered licensee may be implemented in another way, such as by formulating conditions for the use of the data.

Finally, in the fourth stage, the use of the data could be regulated by self-imposed rules. In this instance, it is important to know that the data are being used for a purpose for which they are fit. The risk of misinterpretation is significant. The item of intellectual property may have been revealed on the internet by somebody other than the registered licensee. The item of intellectual property may even have left the possession of the rightful licensee involuntarily, perhaps because his computer was hacked. Any conclusions about the involvement of the registered licensee in a disclosure of the intellectual property have to be dealt with the utmost care and attention. Subsequent actions towards the registered licensee should be based on adequate information about the evidence, partly derived from the watermark, but preferably supported by information from other sources.

Finally, watermarking should pass the subsidiarity test. It will be necessary to establish whether there are other, less burdensome means to trace the source from which infringing materials originate. The existing alternative mentioned above is to obtain court orders obliging infringing parties to disclose the identity of person from whom they obtained the work, thus advancing one link in the chain and to repeat this until the first source in the distribution chain has been reached. This method is particularly onerous, not just for the user of the watermarks, but also for all intermediate links in the illegal distribution chain. In the traditional way, each person and the relationship between each person must be identified. Digital watermarks bypass all the intermediate links and only implicate the privacy of the source. In this respect, digital watermarks are a very useful method of identifying a licensee.

In conclusion, data protection legislation does not prevent the use of watermarks. It is necessary to provide guarantees to protect the interest of the registered licensee at each stage of the watermarking process. The extent to which the user of a watermark has to go to protect the interests of registered licensees depends on the particular circumstances of the watermarking application, such as the value of the works, the efficiency of reducing the ability of the licensee to deal with the intellectual property other than in accordance with the terms of the licence, the consequences attached to positive identification and the nature of the information revealed about the source through positive identification.

It might be that the legitimate interest of the controller does not justify the processing of the data of licensees. This means another justification to process data must be considered. Of the justifications

mentioned in article 8 DDPA, consent is the most promising. When the registered licensee consents to their data being viewed, processing the data can be justified, but the DDPA is careful to regulate how consent should be obtained. The consent should be given in such a way that any doubt that the controller may have about the consent is excluded. If there is any doubt, the controller is obliged to verify whether the registered licensee has actually given their consent.[6] This seems to exclude that consent is obtained through a provision included in the general terms and conditions that go with the license. A more conspicuous mention of the data processing must be made, such as through a pop-up message when agreeing to a license. Sufficient information about what the registered licensee agrees to must also be made available. Another concern with respect to consent is that the party using the watermark will need to be able to prove the consent. This means that the necessary legal, technical and organizational measures must be taken to safeguard this.

Many privacy issues can be avoided if watermarks are used to register companies or institutions rather than individual persons. Assuming that the companies are so large and the other circumstances are such that spontaneous recognition of individual persons can be excluded, data protection problems may not be relevant. An example may be the case where a hotel is registered in a watermark database instead of individual hotel guests, or where a movie theater is registered instead of individual visitors.

Exclusion of unlawfully obtained evidence

If it is not possible to prove consent, or the notice of registration of personal data was inadequate, or privacy is infringed in some other way, the evidence is considered to be unlawfully obtained, even though the evidence may be perfectly reliable. Where evidence has been improperly obtained, it is useful to consider whether the evidence should be excluded, or whether it can be admitted. If the evidence is admitted, perhaps the unlawfulness can be dealt with in another way.[7] Dutch civil courts have hitherto been reticent in excluding unlawfully obtained but reliable evidence.[8] However, if watermarks are being used systematically, privacy infringement may have a structural character. Every work released with a watermark may be infringing privacy. In such cases, a court may be more inclined to set an example by excluding unlawful evidence. In such circumstances, it is not just a single case, but the general practice by the user of the watermark that is at issue. At the time of writing, two criminal cases in the court of Haarlem have excluded evidence that the Dutch security services obtained through illegal interception of the telephone of a journalist.[9] This indicates that the possibility of applying the exclusionary rule is far from purely theoretical. Another implication of privacy infringements may be that the privacy commissioner, in the Netherlands the 'College Bescherming Persoonsgegevens', steps in and forbids the further use of watermarks until such time as the privacy concerns are adequately addressed. This is, however, outside the realm of the law of evidence and will not be dealt with here.

Scientific disputation

A scientific disputation of the evidence may take the following forms:

False positives

A defendant could claim that detection software has found a watermark in a picture that was never put into it. Perhaps no watermark was ever placed in the picture, perhaps another watermark had been placed in it. That this could occur by coincidence, for example as a consequence of compression, resizing or other normal processing acts, is very unlikely. The length of a watermark is so great that the chance that random changes in bits would produce something that could be recognized as a watermark is statistically negligible. False positives through human intervention such as collusion are more likely. Collusion could work as follows. Suppose two licensees have the same picture, but each has a different watermark. Then the licensees could, by comparing the two pictures, discover the bytes making up the watermark by finding out where the bytes that make up their pictures differ. They could

6 C. M. K. C. Cuijpers, C. W. J. Ebbers, A. C. M. de Heij, P. J. D. J. Muijen and J. E.J. Prins (eds.),Voorschriften Privacybescherming, The Hague: Elsevier Overheid 1980, A 4.2-Wbp-article 8-4.

7 Compare J. B. H. M. Simmelink, 'Bewijsrecht en bewijswaardering', in: M. S. Groenhuijsen and G. Knigge, Het onderzoek ter zitting: Eerste interimrapport onderzoeksproject Strafvordering 2001, (Gouda Quint, 2001) p 423 for the Belgian law. Article 154, 189 and 211 BCCrimP: 'regularly obtained' means that the evidence is obtained through honest means and without deception. If that is not the case then the evidence must be excluded.

8 M. Kremer, Onrechtmatig verkregen bewijs in civiele zaken (PhD research Groningen), Deventer: W.E.J. Tjeenk Willink 1999.

9 District Court of Haarlem 14 July 2010, LJN: BN1195, 15/700461-09 and District Court of Haarlem 14 July 2010, LJN: BN1191, 15/700462-09.

then make up a third copy of the picture that is in every respect the same as the two copies they already have, apart from the bytes that make up the watermark. If they give the bytes the average value of the byte values found in their original pictures, something could be created that might be recognized as a watermark. This means that the watermarking algorithm must make sure that no watermark is given out that is capable of being an 'average' of any two other watermarks that have been given out. When the number of watermarks in circulation is limited, this can easily be done, but when the number of watermarked copies of the picture becomes larger this becomes increasingly difficult.

Partial retrieval

By the time an item of intellectual property is retrieved from the internet, its watermark may have been damaged. It may be that the watermark can only be partially read.[10] The problem shows some semblance with the use of DNA for identification purposes. Sometimes DNA found at crime scene has deteriorated, so that only a partial profile can be derived from it. This has not given rise to a question of interpretation, because a forensic scientist can explain what it statically means: that, for instance less Short Tandem Repeats (STR) are used. In other words, they can indicate the level of reliability of their findings. What has given rise to discussion is how to report partial DNA findings. In the past, a profile that was so incomplete as to be useless for positive identification purposes was not reported at all by the forensic scientist.[11] Later, it proved to be important that the court should be made aware of the presence of the deteriorated DNA, since it pointed to the presence of somebody else other than the suspect; it may not have been fit for a positive identification, but it could still be used for the purpose of excluding the suspect. This raises the question how digital evidence specialists should report about partially retrieved watermarks. The problem with digital watermarks is even more complicated because there are many algorithms and applications available for watermarking. A watermark embedded by one company can usually not be detected by software of another company.[12] This means it may even be more difficult to determine whether there are any partial watermarks that may be present in addition to the one a digital evidence specialist may have been asked to identify.

Authenticity of the watermark

The watermark may be a fabrication after the fact. Given a picture, theoretically a watermarking algorithm and key could be made that reads any code from the item of intellectual property. For this reason, it is especially important that the watermarking techniques used are registered with a trusted third party before handing out watermarked intellectual property, or at least well before any conflict about the watermark arises. Only by fixing the algorithm and key before the event, can it be proven that a watermark found in intellectual property was actually placed in the work before the dispute arose. The key in this respect has the function of coding where the watermark is located in the intellectual property. It must thus be distinguished from a possible key used for encrypting the message contained in the watermark.

Discussion before a court about these issues involves digital evidence specialists explaining reports they prepared about an investigation into a marked item of intellectual property. The requirements that an expert witness must meet under Dutch law are very general. In the Netherlands, scientific expert evidence should conform to the criteria set out in the Schoenmaker case:[13]

1. What is the profession, the education and experience of the expert?

2. Does the expertise relate to the subject on which the expert is giving an opinion?

3. What method did the expert use?

10 *This type of problem has been investigated by Dieter Bardyn, Ann Dooms, Tim Dams and Peter Schelkens, Comparative Study of Wavelet Based Lattice QIM Techniques and Robustness against AWGN and JPEG Attacks, Proceedings of the 8th International Workshop on Digital Watermarking, (Springer-Verlag Berlin, Heidelberg, 2009) pp 39-53.*

11 *Rechtbank Rotterdam 27-04-2005, LJN: AT4777, 10/010049-04 and Gerechtshof 's-Gravenhage 22-11-2005, LJN: AU6566, 2200301205.*

12 *Jong-Nam Kim and Byung-Ha Ahn, MPEG Standards and Watermarking Technologies, in Juergen Seitz, editor, Digital watermarking for digital media, (IGI Publishing, 2005), pp 182-214.*

13 *HR 27 January 1998, NJ, 404. Dossier no. 106416. This decision of the Dutch Supreme Court is not yet available from a free digital open source, although it has been assigned a reference number (ZD0917) in the free on-line case law collection 'rechtspraak.nl'.*

4. What is the reliability (validity) of the method used?

5. Was the expert able to apply the method in a competent fashion?

Of the five criteria, the fourth criterion is the most significant in respect of digital evidence: the expert must be able to show that the method he used for arriving at his conclusions is reliable. As a consequence of the Schiedam park murder case, the trend in the Netherlands is to have healthy scepticism towards the results of investigations and the science involved in obtaining them.[14] It is not enough to show the findings. If necessary, the court must be able to verify the steps the expert took for arriving at his conclusion.

In this respect, it is important that there are standards that codify the shared opinion in the scientific community to which digital evidence specialists can refer in their reports and testimonies.[15] In the field of digital watermarking, there have been several initiatives to arrive at standards, such as in the context of Copy Protection Technical Working Group and Digital Audio-Visual Council (DAVIC). The Moving Picture Experts Group (MPEG consortium) helped to develop a standard that has the greatest relevance in this respect, a standard about the evaluation of persistent association technologies.[16] This standard is part of the extensive framework of MPEG 21. Part 11 of the standard does not state a specific aim for the evaluations it standardizes because it is not specifically written with forensic purposes in mind. It should be used by content providers to select a watermarking technology that best fits their functional requirements. The standard indicates a number of best practices for defining a test configuration and the actual evaluation of digital watermarks. These best practices should be implemented in working procedures and benchmark tools used for evaluation. Examples of such tools are computer programs such as Stirmark,[17] Checkmark,[18] Optimark,[19] and WET (Watermark Evaluation Testbed).[20] However, the standard leaves many details about the implementation of an evaluation open. For instance, it does not prescribe in detail how to perform an evaluation, nor does it provide boundary values for the parameters it distinguishes. Such details can only be given if it is known how the watermark is applied, because only then the characteristics of the watermark are known. The approach of indicating best practices does have the obvious advantage that the standard is reasonably independent from the technology and will not easily become outdated.[21] At the same time, this means that an adequate technical evaluation of, for example, the authenticity of a watermark retrieved from a picture found on the internet depends on the quality of the benchmarking programs used and the experts involved in performing the evaluation. As indicated above, it is also not specifically aimed at forensic use. The parties and courts that need to evaluate recovered watermarks must therefore be critical about how the best practices have been implemented. In this respect, additional work geared towards standardisation of forensic procedures and certification of benchmarks and forensic experts or investigation institutes would provide much needed help for courts. This does not take way the relevance of less formal mechanisms such as experts being able to refer to scientific findings; in fact, in common law countries these mechanisms carry more weight than standards and certification.[22]

Contracts and evidence

A court has discretion in assessing the evidentiary value of a watermark. This causes some uncertainty as to the extent to which a content provider can rely on a watermark as a means of evidence. In the license between the rights holder or distributor and the

14 *Rechtbank Rotterdam 27-04-2005, LJN: AT4777, 10/010049-04 and Gerechtshof 's-Gravenhage 22-11-2005, LJN: AU6566, 2200301205.*

15 *For a more detailed discussion, see Stephen Mason, general editor, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010), Chapters 3, 4 and 5, especially section 4.04, p 86.*

16 *ISO/IEC TR 21000-11:2004 Information technology -- Multimedia framework (MPEG-21) -- Part 11: Evaluation Tools for Persistent Association Technologies.*

17 *F. A. P. Petitcolas, 'Watermarking schemes evaluation', IEEE Signal Processing, Volume 17, Issue 5, September 2000, pp 58–64.*

18 *S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet and T. Pun, 'Second generation benchmarking and application oriented evaluation,' Information Hiding Workshop III, Pittsburgh, PA, USA, April 2001.*

19 *V Nikos Nikolaidis, Sofia Tsekeridou, Anastasios Tefas, Vassilios Solachidis, Athanasios Nikolaidis and Ioannis Pitas, 'A benchmarking protocol for watermarking methods,' in IEEE International Conference on Image Processing, volume 3, October 2001, pp 1023–1026.*

20 *Hyung Cook Kim, Hakeem Ogunleye, Oriol Guitart, and Edward J. Delp, 'The watermark evaluation testbed (WET),' in Edward J. Delp III and Ping W. Wong, editors, Security, Steganography, and Watermarking of Multimedia Contents, VI (Proceedings Volume), Proceedings of SPIE Volume 5306, pp 236-247.*

21 *See Section 6 'Use Cases for Evaluation of Persistent Association Tools' of ISO/IEC TR 21000-11:2004 Information technology -- Multimedia framework (MPEG-21) -- Part 11: Evaluation Tools for Persistent Association Technologies.*

22 *Stephen Mason, general editor, Electronic Evidence, p 86.*

licensee, provisions concerning evidence may be incorporated. Such provisions strengthen the position of the rights holder or distributor in civil cases considerably, if the defendant is a contract partner or licensee. That the person identified by the watermark is a licensee is probably the default situation since a watermark is used to identify the 'buyer' of a copy of the work and digital copyrighted works are usually only distributed under an (End User) License Agreement (EULA). The rights holder or distributor may incorporate contractual provisions in the EULA that indicate what the evidentiary value of digital watermarks is. The provisions may, for example, indicate that a watermark provides cogent proof of certain facts (such as the identity of the licensee) between the parties. By declaring certain evidence to be cogent between parties, the discretion of the court in assessing the evidentiary value of the proof is removed; the court must accept the evidence as proof. Provisions in a contract may also bypass the issue of evidence altogether and directly impose certain consequences upon positive identification. An example may be a provision that allows the rights holder to obtain access to the records of the person identified by the watermark or even to obtain access to the buildings in order to check relevant business procedures (such as those involving measures aimed at preventing copyright infringement).

An important question is whether such agreements about evidence are valid. In accordance with the provisions of article 6:233 DCivC, such an agreement when included in general conditions can be nullified if it is unreasonably burdensome for the party subject to the general conditions. The main question is whether an agreement declaring watermarks to give cogent proof is unreasonable. If an agreement does not allow the licensee to adduce proof of the opposite, such is the case (article 6:236 sub k DCivC only applies to business to consumer transactions, and at best analogously applicable in business to business transactions). If an agreement allows proof of the opposite, and only takes away the assessment discretion from the court (cogent proof), the agreement could be allowed. The agreement could also be unreasonable if the evidence provided by a digital watermark is unreliable and chances are that the unreliability is to the detriment of the party subjected to the general terms. In the context of contracts between banks and their clients, it is, for example, stipulated that the administration of the bank provides cogent proof. When arguing the acceptability of this provision, the general confidence that can be placed in banks is mentioned (this argument is perhaps a little weakened in contemporary times). It is often observed that banks are subject to many legal rules regarding their administration, and that compliance with these rules is controlled by supervising institutions.[23] With respect to watermarks, there are no legal rules governing watermarks and supervising institutions. This does not mean that evidentiary provisions in contract are invalid because trust in the reliability of watermarks could be organized in a different way. For example, standardization and certification could play an important role in this respect.

A second issue is that a watermark can never prove more than that a certain copy of a work entered an illegal distribution channel. It provides no proof that the person registered as the legitimate holder of that copy actually introduced the copy into the illegal distribution network. Additional evidence is necessary to prove the identity of the person who entered the copy in the illegal channel. If a provision about cogent proof is included in a contract and is found to be acceptable, this does not mean that the content provider need not prove anything. He still will have to show that, according to his registration of events, no irregularities are apparent.[24]

General implications of proof by watermark

The discussion has focused as to whether and if so under what conditions digital watermarks may be used for copyright infringement protection purposes under Dutch law. The wider implications of using watermarks for copyright infringement protection purposes have not been addressed. Additional concerns include how digital watermarks will affect businesses; whether it will revolutionize copyright enforcement, and what effect, if any, it will have on society and individual citizens. The breadth of these questions precludes that they will be dealt with exhaustively here. Therefore, some tentative observations of will be made about the most

23 *W. H. G. A. Filott, Algemene bankvoorwaarden, Serie Bank- en Effectenrecht nr. 3, Deventer: Kluwer 2000, pp 70-75, W. J. Slagter, Commentaar op de Algemene Bankvoorwaarden, NIBE Bankjuridische reeks nr. 38, Amsterdam: Nederlands Instituut voor het Bank- en Effectenbedrijf 1999, pp 120-123.*

24 *Compare HR 26 April 1996 RvdW 1996, 101c (Honig/WUH).*

striking elements.

Evidence based on digital watermarks is part of copyright enforcement. Enforcement of copyright on the internet has been a problem for as long as the internet has been available to the public at large. However, it seems that the momentum is gathering to deal with the problem more actively. On the international level, negotiations about an Anti-Counterfeit Trade Agreement are well underway. On the Dutch national level, a parliamentary working group recommended that the government support copyright enforcement with new initiatives if right holders improve the availability of legal offerings of works on the internet.[25] In France and the United Kingdom, legislation has been introduced allowing for the disconnection of internet subscribers from the internet if and when they have proven to be repeat offenders.[26] Given these developments, the climate for digital watermarks is not unfavourable. The trend seems to be to involve more participants in the enforcement of copyright. HADOPI and the Digital Economy Act 2010 enlist the cooperation of internet service providers, who are in the best position to terminate subscriptions. Likewise, digital watermarks enlist the help of companies and organizations that are legitimate users of copyrighted works. At the same time, there seems to be a trend for individuals to be less concerned with their privacy, in the sense that they openly share data about themselves. This could be interpreted as not unfavourable to the use of watermarks registering individual persons. In short, there are many developments and trends that are not unwelcome to the use of watermarks for copyright infringement protection purposes.

Nevertheless, content owners and rights holders have to be careful when considering the introduction of watermarking schemes. Companies and organizations making use of licensed works may not be too enthusiastic about works with identifying watermarks. This is especially the case if it is not clear whether 'leaks' can be prevented, and the watermark increases their exposure to liability for breach of license conditions, or even copyright infringement. The prevention of leaks may require companies and organizations to implement costly measures, while they cannot guarantee that their systems will prevent intellectual property from being stolen.

If the identity of individual persons is to be registered, the introduction of a watermark will have to take place with even more circumspection. The individual will have to be informed of the presence of the watermark and the fact that it contains or points to information that personally identifies him. It is not certain how the legitimate user of the work will react. In an ideal scenario, the user of a work internalizes the idea that his identification data are engrained in the work, and this knowledge alone will be sufficient to keep him from sharing the work and spur him on to take adequate measures to ensure that a work does not leave their possession unintentionally. The proof by digital watermark is then no more than a credible threat that the rights holder need not actually effectuate.

But users may not be so docile. Users may reject marked works altogether, and simply not buy them. They may not want to pay for a legitimate copy of a work and be responsible if something untoward happens with their copy. Furthermore, they could frame their personal dislike in legal arguments that have wider ramifications. They may feel inhibited in their freedom to deal with the watermarked works. Could a picture be shared digitally among members of a family without fear that one of the family members puts the picture on the internet? Could a picture be used in a legal way on the internet without fear that other internet users copy the picture and make it available in an illegal way? These consequences are not elaborated here, but could prove relevant for the acceptance in society of digital watermarking technology for copyright enforcement purposes.

But it is not just users refusing to buy watermarked products. Ignoring watermarks could also be a problem. If marked works appeared in large numbers as pirated copies on the internet, it is not known how right holders might react. Prosecuting some licensees as an example to others may upset public opinion. It is risky because it targets the very users of the work that actually paid for a legal copy. A less threatening reaction may be to demand better measures to prevent a leak from occurring again in the future. Although it is different from making a licensee liable for (indirect) copyright infringement or breach of license conditions, it still has its own problems. How could it be enforced without invading the privacy of

25 *A. Gerkens, P. Smeets, F. Teeven and N. van Vroonhoven-Kok, Auteursrechten, een rapport, Werkgroep uit de vaste commissies voor Justitie en voor Economische Zaken in de Tweede Kamer van de Staten-Generaal, 2010, available at: http://www.boek9.nl/www.delex-backoffice.nl/uploads/file/Boek9% 20/Andere% 2 ostukken/Eindrapport% 20parlementaire% 20wer kgroep% 20auteursrechten_tcm118-189136.pdf.*

26 *In France, Loi favorisant la diffusion et la protection de la création sur Internet (law promoting the distribution and protection of creative works on the internet) (HADOPI is the acronym of the government agency created to administer the law: Haute Autorité pour la Diffusion des ?uvres et la Protection des Droits sur Internet); in the UK, the Digital Economy Act 2010.*

somebody's home or personal sphere? A tough approach to enforcement also does not seem to be viable. In short, the use of digital watermarking in the sphere of consumers is fraught with difficulties. Therefore, it is more likely that digital watermarks will find use in a professional context, at least where it concerns copyright infringement protection.

Conclusion

This article assesses how digital watermarks can be used as evidence in the context of copyright infringement protection. The legal systems for proof in civil and criminal cases in the Netherlands basically allow for the introduction of evidence by digital watermark. The use of digital watermarks for copyright infringement protection purposes affects the privacy of those licensees that can be identified by the watermark. The identification in relation to the circumstances in which a marked item of intellectual property is found provides information about the licensee: it possibly identifies him as the source of a 'leak' and may give away information about the persons with whom he maintains contacts. However, the watermark neither gives information about the circumstances under which the 'leak' occurred nor about the role the registered licensee played in it. This requires restraint from those interpreting positive identifications. Deriving information from identification by watermark is thus a sensitive process and must take place under adequate privacy safeguards. Informing the licensee and protocols for dealing with identification information are important instruments. Privacy problems can be avoided if only companies or organizations are registered as licensees within watermarks.

It is relevant that courts have an adequate understanding of the scientific aspects of proof by watermarks. These aspects are both relevant for the assessment of the evidence as for the viability of (license) clauses dealing with the evidentiary value that is to be accorded to digital watermarks. Information about scientific aspects reaches a court though an expert witness. However, it is not easy for a court to assess the knowledge of the witness or the scientific adequacy of his testimony or report. Standards and certification can help a court in its assessment. There exists a standard for the evaluation of persistent association technologies, such as watermarks. However, the standard is not designed for forensic applications, it leaves many implementation details open and there is no certification infrastructure in place for benchmarking tools or experts. Hence, there is room for improving the support given to courts in assessing watermark evidence.

Although not strictly a legal issue, the success of watermarking may also depend on the acceptance by the people who will be involved in watermarking. In general, there is a development towards greater involvement of third persons in the enforcement of copyrights. This does not mean that those who are registered in watermarks are prepared to accept watermarked works. Their position seems to become weaker when watermarked works start being used. A positive identification at least morally places them in a defensive position, where they may be pressed to provide an explanation for the leak. This may dampen their willingness to buy works that have watermarks in place. It is unclear how and to what extent licensees will use a possible bargaining position they have to negotiate restrictions upon the use of watermarks. The introduction of new watermarking schemes will in this respect require a delicate hand of rights holders.

Dr. Maurice Schellekens is an assistant professor at the Tilburg Institute for Law, Technology, and Society at Tilburg University.

http://www.tilburguniversity.edu/webwijs/show/?uid=m.h.m.schellekens

Literature of interest not cited

R. Dekkers and A. Verbeke, Handboek Burgerlijk Recht, Deel III, Verbintenissen, Bewijsleer, Gebruikelijke contracten, Antwerpen: Intersentia 2007.

M. C. D. Embregts, Uitsluitsel over bewijsuitsluiting. Een onderzoek naar de toelaatbaarheid van onrechtmatig verkregen bewijs in het strafrecht, het civiele recht en het bestuursrecht (PhD research Tilburg), Kluwer 2003.

T. R. Hidma and G. R. Rutgers, Pitlo, Het Nederlands burgerlijk recht, Deel 7, Bewijs, Deventer: Kluwer 2004.

M. Natarajan and Gayas Makhdumi, Safeguarding the Digital Contents: Digital Watermarking, DESIDOC Journal of Library & Information Technology, Volume 29, Number 3, May 2009, pp 29-35.

J. F. Nijboer, Strafrechtelijk bewijsrecht, Nijmegen: Ars Aequi 2008.

