ARTICLE:

EVIDENTIAL ISSUES FROM PRE-ACTION DISCOVERIES: *ODEX PTE LTD V PACIFIC INTERNET LTD*

By **Daniel Seng**

Introduction

There have been many pre-action applications by right holders against Singapore ISPs to discover the identities of internet users. Most of these applications are not contested, and the identities of the users are as a result disclosed. Consequently, the scope and issues pertaining to such applications have not really been subjected to close judicial scrutiny. It therefore came as a surprise to both the local legal and the internet communities in Singapore to read about the case of *Odex Pte. Ltd. v. Pacific Internet Ltd*.[1] This is the first reported decision in Singapore where an ISP challenged an application for pre-action discovery.

Odex is a private company that provided Japanese anime programmes to local television stations for broadcasting.[2] It also distributed authorized copies of these programmes to retailers for sale to the public.[3] Odex allegedly became concerned with internet piracy, particularly with the ease of obtaining DVD-quality movie files for free via P2P software. It alleged that its sales of anime video titles had begun to drop significantly and that television stations also bought fewer anime titles, because they were allegedly losing viewers to people who illegally downloaded files.[4]

To address this problem, Odex engaged the services of BayTSP.com Incorporated (BayTSP), an American company, to collect and track instances of unauthorized uploading and downloading of copies of Japanese anime video titles.[5] The High Court judge described BayTSP in the following terms:

> BayTSP.com [is] an American company which is the developer and owner of patented technology that tracks instances of uploading and/or downloading of digital files on the Internet in real time, and displays the internet protocol ('IP') address of the relevant users, to provide Odex with an online tracking solution that would enable Odex to collect details relating to instances of unauthorized uploading and downloading of copies of the video titles.[6]

Through BayTSP, Odex discovered that there had been more than 474,000 unique downloads over an 11-month period, 'based on searches conducted on only 50 out of more than 400 authorized titles', as described by the judge.[7] That these numbers were not only restricted to downloads in Singapore, but worldwide, could be discerned from the claim by Odex that Singapore was ranked tenth in the world for the total number of illegal downloads, and was ranked first based on the number of illegal downloads on a per capita basis.[8] Odex claimed that it approached the Intellectual Property Rights Branch (IPRB) of the Criminal Investigation Department, Singapore, to search the homes of those identified as having illegally down loaded files, but its request was declined. Instead, it was advised to gather evidence itself and apply for pre-action discovery.

In these circumstances, Odex applied under Order 24 Rule 6(5) of the Singapore Rules of Court [9] for the pre-action discovery of 'documents' from various local

[1] *Odex Pte. Ltd. v. Pacific Internet Ltd., [2007] SGDC 248 (District Ct. Sing.) (Odex (District Ct.)), rev'd on other grounds, [2008] SGHC 35, [2008] 3 SLR 18 (High Ct. Sing.) (Odex (High Ct.)); George Wei, Pre-commencement Discovery and the Odex Litigation: Copyright versus Confidentiality or is it Privacy? (2008) 20 SACLJ 591.*
[2] *Odex (High Ct.), [2].*
[3] *Odex (High Ct.), [2].*
[4] *Odex (High Ct.), [3].*
[5] *Odex (High Ct.), [4].*
[6] *Odex (High Ct.), [4].*
[7] *Odex (High Ct.), [5].*
[8] *Odex (High Ct.), [5].*
[9] *Rules of Court (Cap. 322, R 5, 2006 Rev. Ed., Sing.).*

Odex had argued that both the Practice Direction and the Regulations refer to an application made 'on behalf of a copyright owner', and in doing so, sanctioned its application as a licensee.

internet service providers, to identify individuals that illegally down loaded files, based on a selection of 981 IP addresses of internet users who were recorded as having carried out the highest instances of such uploading and downloading via the BitTorrent protocol.[10] Only the defendant Pacific Internet, a local internet service provider, resisted that application.

Odex's application for a discovery order failed before the District Court, which held that Odex did not have sufficient connection to the case to make the application, since it was only a sub-licensee for most of the video titles (whose infringement Odex complained of).[11] However, for one title for which Odex was held to be the exclusive licensee (Mobile Suit Gundam Seed), the District Court was of the view that Odex had to show an extremely strong prima facie case of wrongdoing before the order sought would be made in its favour. As Odex had failed to establish such a case, its application was dismissed.[12]

Odex filed an appeal and sought to introduce additional evidence to establish sufficient connection to the case and an extremely strong prima facie case. The appeal court (the Singapore High Court) allowed the admission of such additional evidence.[13] However, the court rejected Odex's argument that it had the requisite connection to the case to apply for a discovery order, on the basis of a Practice Direction[14] issued by the Supreme Court and on the basis of the Singapore Copyright (Network Service Provider) Regulations 2005.[15] Odex had argued that both the Practice Direction and the Regulations refer to an application made 'on behalf of a copyright owner', and in doing so, sanctioned its application as a licensee. The court observed that the Practice Direction did not have the force of substantive law, and that Regulation 3(2)(b) did not pertain to discovery applications.[16] The court also noted that the Singapore Copyright Act did not have an equivalent provision to section 512(h)(1) of the U.S. Copyright Act, which would enable a copyright owner or 'a person authorised to act on the owner's behalf' to issue a subpoena to a service provider for identifying an alleged infringer.[17]

The court held that an agent of a copyright owner or an exclusive licensee could not apply in the agent's own name for pre-action discovery in order to identify infringers.[18] While the copyright owners could use the services of an agent to track down infringing parties, they had to use their own names to commence civil court proceedings, apply for pre-action discovery and take formal action for substantive relief.[19] Even if Odex were not relying on Order 24 Rule 6(1) for a discovery order but on the inherent jurisdiction of the court to issue a Norwich Pharmacal[20] discovery order, any connection to the case it might have was not sufficient to rely on the court's Norwich Pharmacal jurisdiction.[21] Nor could Odex merely claim that it would only use the information to initiate criminal proceedings (based on the decision of *Ashworth Hospital Authority v. MGN Ltd*. [2002] 1 W.L.R. 2033), because in seeking to file the current application as a mere agent (and not even as a licensee) for the right holders, it could not claim to be a victim and thus the party entitled to relief.[22]

The court reversed the decision of the District Court on the requirement for an extremely strong prima facie case of wrongdoing, holding that the court below had prescribed too high a standard of proof. Where there was evidence of wrongdoing, the court would consider the strength of the case by the applicant for discovery order as one of the factors to be considered in the totality of the facts before deciding whether to grant the

[10] *Odex (High Ct.), [12].*
[11] *Odex (District Ct.), [21].*
[12] *Odex (District Ct.), [36].*
[13] *Odex (High Ct.), [16].*
[14] *Practice Direction 4 of 2005 'Applications for discovery or interrogatories against network service providers in relation to specific intellectual property issues'.*
[15] *Copyright (Network Service Provider) Regulations 2005 (S 220/2005, Sing.).*
[16] *Odex (High Ct.), [37].*
[17] *Odex (High Ct.), [37]. See also In re Verizon Internet Servs., Inc., 257 F.Supp.2d 244, 259 (D.D.C.2003), reversed on other grounds, Recording Indus. Ass' n of America, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C.Cir.2003).*
[18] *Odex (High Ct.), [38].*
[19] *Odex (High Ct.), [40].*
[20] *Norwich Pharmacal Co. v. Customs and Excise Commissioners, [1974] A.C. 133.*
[21] *Odex (High Ct.), [43].*
[22] *Odex (High Ct.), [50].*

order in the interest of justice. Any duty of confidentiality, which the defendant ISP might owe to other parties, was another factor and should not, in itself, give rise to a higher standard of proof.[23] Nonetheless, the court concluded that it was inexpedient to have the copyright owners start the discovery application again, especially where on the current appeal, there was an application by some copyright owners to be added as plaintiffs. The court allowed these owners to be added as plaintiffs and allowed disclosure of the subscribers' information to these plaintiffs as copyright owners for their respective video titles.[24]

The duty of the court in an application for pre-action discovery

This case is the first case in Singapore where the court had the opportunity to rule on the issues regarding an application of a discovery order against an internet service provider to identify the allegedly infringing internet subscribers. Unlike the decisions from Hong Kong,[25] where the courts were only concerned with their Norwich Pharmacal jurisdiction to order pre-action discovery, the Singapore court also examined its jurisdiction to do so under the Rules of Court. Though the decision was not cited to the courts, the Hong Kong Court of First Instance in *Cinepoly Records Co. Ltd. v. Hong Kong Broadband Network Ltd. (No. 1)* had also dismissed the argument of the defendant ISP that its confidentiality obligations to its subscribers did not permit it to disclose its subscribers' details to the copyright right holders.[26]

But in seeking to resolve the application on the narrow issue of whether the applicant had the requisite connection to the case, the Singapore court missed the valuable opportunity to link the consideration of whether the applicant had demonstrated the strength of his case to an assessment of the evidence tendered by the applicant to support his pre-action discovery application. The judgment of the High Court alluded to the requirement to show the connection between BayTSP and the applicant, as well as the qualifications and expertise of the expert tendering evidence required to show how the BitTorrent protocol works,[27] with the judge claiming, without elaboration, that the new affidavits address these points (raised previously by the lower court).[28] The lower court itself even asserted that it was not necessary for the applicant to satisfy the Evidence Act provisions for computer output for the application.[29] But the judgments did not record any detailed substantive examination of the evidence tendered by the applicant's.

It is difficult to see how these observations, together with the absence of a detailed assessment of such evidence, can be reconciled with the court's duty in any Norwich Pharmacal discovery application, as held in the Singapore Court of Appeal decision of *Kuah Kok Kim v Ernst & Young*, 'to ensure that the application was not frivolous or speculative or that the applicants were on a fishing expedition'.[30] In *Cinepoly Records Co. Ltd. v. Hong Kong Broadband Network Ltd. (No. 1)*, the Hong Kong High Court summarized the applicable principles in a discovery application against the ISPs regarding the identities of its subscribers as follows:

a. There must be cogent and compelling evidence to demonstrate that serious tortuous or wrongful activities had taken place.

b. The alleged wrongdoer was a person whom the applicant believed in good faith to be infringing his rights in the sense that he could be reasonably be assumed to be the wrong doer vis-à-vis the applicant.

c. It must be demonstrated that the order would or would be likely to reap substantial and worthwhile benefits for the applicant.

d. The ISP, the innocent party against whom discovery was sought, had been caught up or become involved in such activities, which facilitated the perpetration or continuation of the activities.[31]

After establishing these elements, the applicant must further demonstrate that it was just and convenient in all the circumstances for the court to exercise its discretion to grant the relief. And where the innocent party was the only practical source of information, or if the innocent party was subject to a duty of confidentiality, imposed by contract or otherwise, the court will take into account these competing interests in ordering or refusing disclosure.[32]

[23] *Odex (High Ct.), [61].*
[24] *Odex (High Ct.), [76].*
[25] *Cinepoly Records Co. Ltd. v. Hong Kong Broadband Network Ltd. (No. 1), [2006] HKCFI 547, [2006] HKCU 191, [2006] 1 HKC 433 (Ct. of First Instance H.K.) (Cinepoly (No. 1)) and Cinepoly Records Co. Ltd. v. Hong Kong Broadband Network Ltd. (No. 2), [2006] HKCFI 1028, [2006] HKCU 1500 (High Ct. H.K.) (Cinepoly (No. 2)).*
[26] *Cinepoly (No. 1).*
[27] *Odex (High Ct.), [63].*
[28] *Odex (High Ct.), [64].*
[29] *Odex (District Ct.), [31].*
[30] *Kuah Kok Kim v Ernst & Young, [1997] 1 SLR 169, [59].*
[31] *Cinepoly (No. 1), [19].*
[32] *Cinepoly (No. 1), [20]. Similar principles were advanced in Sony Music Entertainment Inc. v. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y., 2004).*

Evidential issues

It is suggested that establishing the cogency and compelling nature of the facts that show an alleged infringement and the good faith of the applicant's complaint involve demonstrating the evidential chains of proof and observance of the rules of evidence. Courts have disallowed the pre-action discovery applications when either the evidential links are not established or rules of evidence are breached. And notwithstanding the interlocutory nature of these applications, rules of evidence must still be observed,[33] particularly since these discovery applications are ex-parte in nature and are not subject to the challenges of the adversarial process. There is no suggestion that affidavits may be made on the basis of inadmissible hearsay evidence, or contain information made without prejudice by the other party.[34] After all, an affidavit may contain only such facts as the deponent is able of his own knowledge to prove.[35] It is suggested that a component of the balancing exercise is built into an evidential assessment of the quality of the good faith case tendered by the applicant.

In *BMG Canada Inc. v. John Doe*, the Federal Court of Appeal of Canada had the opportunity to examine this issue. In that case, the music producers as right holders tendered affidavits to establish the following chain of proof:

a. The right holders provided a list of the songs over which they claimed copyright to MediaSentry, the company that provided services for the online automated detection of unauthorized distribution of copyrighted materials on the internet.

b. MediaSentry through its computer program searched the internet and identified IP addresses from which large numbers of the sound recordings (comprising the songs) were being offered for copying. Screen captures were made of these files that were offered.

c. MediaSentry's program then requested copies of the files and received them from the identified IP addresses. The files were provided to a representative of the right holders who confirmed that the contents of the files corresponded with the right holders' songs.

d. MediaSentry's program matched the IP addresses to the specific ISPs who were administering the IP addresses at the relevant time.[36]

In *BMG Canada v. John Doe*, these identified ISPs were then served with the discovery request, in an attempt to identify the relevant subscribers. Although there was a clear chain of proof tendered by the right holders and by MediaSentry in the affidavits, the application by right holders was ultimately rejected, because the court held that the affidavits from MediaSentry were made by its President based upon information gained from his employees, and not by the employee investigators themselves, and as such, constituted largely of hearsay.[37] As the Federal Court of Appeal observed:

> Much of the crucial evidence submitted by the plaintiffs was hearsay and no grounds are provided for accepting that hearsay evidence. In particular, the evidence purporting to connect the pseudonyms with the IP addresses was hearsay thus creating the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted. Without this evidence there is no basis upon which the motion can be granted and for this reason alone the appeal should be dismissed.[38]

This aspect of its reasoning by the Federal Court of Appeal of Canada deserves greater elaboration. It is only by understanding which aspects of the evidence is 'crucial' will the right holders be in a better position to establish a case of good faith against the infringing parties that will entitle them to the discovery order.

Proof of ownership of the works

First, there must be proof of copyright ownership to the works in question, which are the subject of the investigation. It follows that reliance may be had to the

[33] *See Rules of Court (Sing.), Ord. 38 r. 2(2), r. 2(5) (Cap. 322, R 5, 2006 Rev. Ed. Sing.) (Sing. Rules of Court) ('Nothing in this Rule shall make admissible evidence which if given orally would be inadmissible.'); Supreme Court Practice Directions (Sing., 2007 ed.), Para. 43 (applications for discovery or interrogatories against network service providers to be made as originating summons applications).*

[34] *Evidence Act, s. 2(1) (Cap. 97, 1997 Rev. Ed. Sing.) (Sing. Evidence Act). But see Butterworths Annotated Statutes of Singapore: Evidence 2-3 (J. Pinsler, Y.L. Tan, V. Winslow, M. Hor, H.L. Ho, D. Seng, eds., 1997) (explaining that s.2 envisaged the use of affidavits where they are not used in lieu of oral testimony, and that this rule has been overridden by Sing. Rules of Court, Ord. 41, r. 5).*

[35] *Sing. Rules of Court, Ord. 41, r. 5 ('an affidavit may contain only such facts as the deponent is able of his own knowledge to prove').*

[36] *BMG Canada Inc. v. John Doe, [2005] F.C.A. 193, [12] (Canada Federal Ct. of Appeal) (BMG Canada), upheld on different grounds, BMG Canada Inc. v. John Doe, [2004] 3 F.C.R. 241 (Canada Federal Ct.).*

[37] *BMG Canada, [15].*

[38] *BMG Canada, [21].*

presumptions in copyright legislation as to the subsistence and ownership of copyright.[39] But it should be noted that some of these presumptions may have limited application in the digital environment, particularly where they operate on the premise that the name of the author or publisher is 'marked' or 'labelled' on a copy of the work. Other practical considerations would be whether proof of copyright ownership requires the proof to be adduced by the copyright owner, or whether it would suffice to have a licensee, a representative or an agent make the declaration.[40] Much would turn on the procedural requirements as prescribed in the copyright legislation of the relevant country.[41]

In addition, proof of copyright ownership does not merely go to the issue of whether the applicant as the right holder or exclusive licensee has the necessary connection to the case to commence discovery proceedings against the infringing parties,[42] it is also an issue as to whether the third party investigating company (such as MediaSentry or BayTSP) has been supplied with the correct works, titles or information for its investigation. In this regard, it should be noted that in some jurisdictions, it has been held that the use of a third party investigator to conduct infringement investigations is not legal.[43]

The *Odex* case also illustrates one other point in this regard. The original affidavits tendered by the applicant did not make it clear as to whether the investigations were carried out by the investigator or by the applicant.[44] The fresh affidavits filed before the High Court on appeal showed that the applicant had actually engaged the investigator to provide it with 'an online tracking solution' which the applicant had operated to track the alleged infringers. However, the district judge hearing the application at first instance observed that while the 'tracking solution' was operated by the applicant, the tracking reports it generated were compiled by the investigator.[45] Thus it was not apparently clear, at least from the judgments, as to whether the tracking reports were produced by the applicant or the investigator. This lack of clarity as to the respective roles and functions of the investigator and the applicant actually prejudiced the applicant's discovery application in the court below.[46]

Identifying the infringing works and confirming their availability

Supplying the wrong information to the investigator will in turn point the investigations in the wrong direction. Given that many works that are illicitly shared on-line do not have rights management information contained in them, the problem is how the works are to be identified as 'infringing' works belonging to the right holders or exclusive licensees. Identification of the works shared by users as 'infringing' works by their titles is neither conclusive nor reliable. For instance, it has been widely reported that to prevent widespread instances of illicit file sharing, right holders have included misnamed, decoy or fake files (known as 'spoofing') into P2P networks to discourage users who are looking for copyrighted content based on the names or titles of the files.[47] The alternative is the use of digital fingerprinting technology to uniquely identify the right holders' works. This point was alluded to in the lower court's judgment in *Odex* but it was not clear if the applicants' works in question had been so fingerprinted.[48]

In this regard, the extra step taken by the right holders in *BMG Canada v. John Doe* is most certainly to be lauded. MediaSentry, the investigator in that case, actually downloaded the files in question from the alleged infringers' computer systems and provided them to the right holders to confirm that they corresponded with the right holders' works in question. This assessment goes some way towards addressing concerns that digital fingerprinting may yield false positives, in that works which are not related to the right holders' works have been identified as infringing. If there is a visual or aural assessment that is conducted through a human agency, this will also address concerns that works that are 'remixed' or adapted from existing works as permissible 'fair use' or 'fair dealing'[49] will not be tagged as infringing works.

[39] *For example, see the U.K. Copyright, Designs and Patents Act 1988 (c. 48), ss. 104, 105; Australian Copyright Act 1968 (Cth.), ss. 126-128; Copyright Act (Cap. 63, 2006 Rev. Ed. Sing.), ss. 130-132.*

[40] *For example, see the Malaysia Copyright Act 1987, s. 42.*

[41] *For example, see Rock Records (M) Sdn. Bhd. v. Audio One Entertainment Sdn. Bhd., [2005] 3 MLJ 552 (Msian. High Ct.).*

[42] *In Odex, the applicant tendered various letters of authorization from the right holders to act, but the court rejected them on the basis that this did not constitute the applicant as an exclusive licensee to pursue the discovery application.*

[43] *For example, see Foundation for the Protection of Rights of the Entertainment Industry in the Netherlands (Brein) and Ors. v UPC Nederland B.V. (Chello) and Ors., 194741/KGZA-05-462/BL/EV (12 July 2005), at [4.25]-[4.27] (Utrecht Court, 12 July 2005) (Brein v. Chello (Utrecht Ct.)).*

[44] *Odex (District Ct.), [26]. Cf. Odex (High Ct.), [11]-[12].*

[45] *Odex (District Ct.), [28(c)].*

[46] *Odex (District Ct.), [28] (the court finding the affidavits filed by the applicant not relevant as regards explaining how the online tracking solution worked).*

[47] *See BMG Canada Inc. v. John Doe, [2004] 3 F.C.R. 241, [19] (describing the service called MediaDecoy which distributes bogus or inoperative files over the Internet); TorrentFreak, MPAA Caught Uploading Fake Torrents, at http://torrentfreak.com/mpaa-caught-uploading-fake-torrents/.*

[48] *Odex (District Ct.), [28(d)].*

[49] *For example, see the U.K. Copyright, Designs and Patents Act 1988 (c. 48), s. 29; Australian Copyright Act 1968 (Cth.), s. 40; Copyright Act (Cap. 63, 2006 Rev. Ed. Sing.), s. 35.*

Actually downloading the complete files is also part of the process of proving that there has been substantial infringement of the right holders' rights. In *HKSAR v. Chan Nai Ming*, the officers from Customs and Excise Department downloaded three entire movies from the accused's computer before commencing criminal investigations to track down the accused based on his IP address.[50] In *Winny I*, the Kyoto Police Department likewise successfully downloaded two movies from the accused's computer before he was arrested and charged with the criminal offence of copyright infringement.[51] The fact that a work appears to be available is no confirmation that it is actually available for download. The distributed nature of P2P networks and distributed file sharing systems such as BitTorrent mean that indexes or Torrents that show that certain files are available may be outdated because the source files have been removed.

It should also be noted that MediaSentry in *BMG Canada v. John Doe* also made records of the downloading process. The images displayed on the screen were captured, and served as evidence that identified the infringing works, the identities of the users and the successful downloading process. Sometimes, the entire process of searching and downloading is under the control of a computer program. This process, together with the records generated, is automated.[52] Where this occurs, it is important that such evidence be tendered with proof of the proper operation of the computer program and the system and the corresponding accuracy of the computer printouts.[53] This evidence was actually called for by the court below in *Odex*. Unfortunately, because the applicant, rather than the investigator as the developer of the solution offered the affidavits seeking to establish the reliability of the on-line tracking product, the court found the affidavits irrelevant.[54]

Identifying the infringers

This is probably the most contentious aspect of the process, because identifying users on the internet by way of their IP addresses poses both legal and technical challenges. In some jurisdictions, the IP addresses of users are held to be personally identifiable information and their disclosure will be strictly regulated by privacy or data protection legislation.[55] There may also be confidentiality obligations as between ISPs and their users. While courts may take the view that data protection and confidentiality obligations are no bar to the public interest in favour of disclosure of the identities of users for reasons of enforcing copyright laws,[56] ultimately this involves a balancing exercise between the protection of personal data (and the private life) of users and protecting the property rights of the right holders by affording the latter an effective remedy.[57]

Another legal and technical impediment will be the lapse of time between the recording of the infringing activity and a request made for the identity of the subscriber who allegedly committed that activity. The longer the lapse of time, the greater is the risk that the information as to identity may be inaccurate (for instance, if existing records are overridden or corrupted) or even missing.[58] For this reason, legislation may be passed which prescribes how long ISPs are obliged to keep their IP address records.[59]

Given the fact that these identification reports contain technical information such as IP addresses, date and time stamps, names of files that are shared or their identifiers (hash numbers) and other miscellaneous information, many of these reports will be computer-generated.[60] This in turn raises valid questions such as whether they contain hearsay evidence or fall within a permissible hearsay exception,[61] are primary or

[50] *HKSAR v. Chan Nai Ming, [2007] HKCFA 36, [2007] HKCU 849, [2007] 3 HKC 255 (Ct. of Final App. H.K.).*

[51] *Winny I, 2004 (Wa) No. 2018 (Kyoto District Ct., 30 Nov. 2004).*

[52] *Brein v Chello (Utrecht Ct.), [2.9].*

[53] *For example, see The Statue of Liberty [1968] 1 W.L.R. 739, [1968] 2 All E.R. 195; R v. Wood (1982) 76 Cr. App. R. 23; Castle v. Cross [1985] 1 All E.R. 87; PP v. Ang Soon Huat [1991] 1 M.L.J. 1 (High Ct. Sing.); R v. Shephard, [1993] A.C. 380; R v McKeown, [1997] 1 W.L.R. 295, [1997] 1 All E.R. 737.*

[54] *Odex (District Ct.), [28].*

[55] *Brein v Chello (Utrecht Ct.), [4.22], upheld on appeal, Foundation for the Protection of Rights of the Entertainment Industry in the Netherlands (Brein) and Ors. v UPC Nederland B.V. (Chello) and Ors. 1457/05 KG (Netherlands Ct. of Appeal, 13 July 2006), at [4.8] (Brein v. Chello (Ct. of Appeal.)); Productores de Música de España (Promusicae) v. Telefónica de España SAU, Case C-275/0-6 (European Court of Justice, 29 Jan. 2008), [45] (Promusicae v Telefónica) (holding that European Community law did not require member states, in order to ensure the effective protection of copyright, to lay down an obligation to disclose personal data in the context of civil proceedings).*

[56] *See In re Verizon Internet Servs., Inc., 257 F.Supp.2d 244, 259 (D.D.C.2003), reversed on other grounds, Recording Indus. Ass' n of America, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C.Cir.2003); Sony Music Entertainment Inc. v. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y., 2004); BMG Canada, [36], Cinepoly (No. 1); Cinepoly (No. 2); Odex (High Ct.), [61].*

[57] *For example, see Promusicae v Telefónica, [65].*

[58] *BMG Canada, [43].*

[59] *For example, see Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13/04/2006 P. 0054 - 0063, Art. 6 (' Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.').*

[60] *Sing. Evidence Act, ss. 35, 36.*

[61] *Sing. Evidence Act, s. 32.*

secondary evidence,[62] or have been authenticated accordingly by the respective parties.[63] There will also be additional issues such as who (the applicant or the investigator) was actually responsible for producing the computer-generated reports and whether special expertise is required to interpret and support the reports. For the lower court in *Odex* to therefore offer the opinion that it is not necessary for the evidence tendered to satisfy the evidential provisions regarding computer output (which will be generally how these reports are produced) is therefore disingenuous.[64] Section 35 of the Singapore Evidence Act would have required the applicant to demonstrate that there was no reasonable ground for believing that the output was inaccurate because of improper use of the computer and that no reason exists to doubt or suspect the truth or reliability of the output, and that there was reasonable ground to believe that at all material times, the computer was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the accuracy of the output was not affected by such circumstances.[65] However, the lower court in *Odex* was certainly right in questioning whether the applicant's officer, who tendered the first sets of affidavits to assert that the computer-generated reports showed evidence of infringement, had the necessary computer expertise and expertise to both operate the tracking software and decode its data to the conclusions maintained in the affidavits.[66]

That there is every reason to scrutinize the evidence in this regard is best brought out in the Netherlands decision of the *Foundation for the Protection of Rights of the Entertainment Industry in the Netherlands (Brein) v UPC Nederland B.V. (Chello) (Brein v. Chello)*.[67] The foundation for the discovery applications by Brein and the collecting societies was a report generated by MediaSentry, which stated the P2P alias of the user, the date and time and the IP address from which the music files belonging to the right holders were made available on the internet.[68] In transpired, however, that MediaSentry's reports had errors as regards the dates and times of the infringement.[69] The Dutch court rejected Brein's discovery application for other reasons. But it also had the following to say as regards this error:

> If a claim such as the present one is to be awarded, it must be beyond a reasonable doubt that the IP addresses relate to the users who actually illegally offer music or other files on their computer. In order to determine from which computer the unauthorized music files are offered, the date and the time of the infringement must be accurately determined. This implies that it must be indicated at what moment third parties downloaded files from the computer in question. The service providers called into doubt the accuracy of the data collected by Brein on the infringers and the infringement. Brein has been unable to remove this doubt to a sufficient degree.[70]

The Dutch decision demonstrated a high degree of understanding of the technical complexities behind associating the IP address with the ISP's subscriber. Both the Utrecht court as well as the Court of Appeal correctly noted that most retail customers of ISPs are assigned IP addresses dynamically at the beginning of every session on the internet, and for this reason, the date and time of infringement must be determined with great accuracy in order to determine which user or subscriber committed the infringement under that IP address.[71] The Court of Appeal stated that in a pre-discovery application,'[t]he key requirement is that there can be no reasonable doubt about whether the IP addresses relate to subscribers who are illegally offering music files from their computer's shared folders'.[72] In the words of the Court of Appeal, if it could not be properly established in advance whether the investigations were carried out with sufficient accuracy and due care, it could not serve as the basis for allowing the application.[73] In fact, the Utrecht court offered the opinion that it was the duty of the ISP to scrupulously guard against any unlawful request to release the personal details of its subscribers, and a failure to do so will expose them to legal liability.[74] The court also noted that the release of such information was irreversible, in that if the names and addresses of the subscribers were released, this information could not be reversed later.[75]

[62] *Sing. Evidence Act, ss. 35(10)(b), 67.*
[63] *Sing. Evidence Act, s. 36(4).*
[64] *Odex (District Ct.), [31]. Perhaps the honourable District Judge had in mind s. 2(1) of the Sing. Evidence Act.*
[65] *Sing. Evidence Act, s. 35(1)(c). The other modes of admissibility are not likely to be applicable, namely that there is an express agreement between the applicant and the ISP not to dispute the authenticity nor accuracy of the output (s. 35(1)(a)), or that the output was produced pursuant to an approved process for document capture (s. 35(1)(b)).*
[66] *Odex (District Ct.), [32], [34]-[35].*
[67] *Brein v. Chello (Ct. of Appeal.).*
[68] *Brein v. Chello (Utrecht Court), [2.11].*
[69] *Brein v. Chello (Utrecht Court), [2.12].*
[70] *Brein v. Chello (Utrecht Court), [4.30]. The translation from Dutch into English was commissioned by SOLV Advocaten, made by Hendriks & James and made available by Christiaan Alberdingk Thijm of SOLV Advocaten, and is available on-line at http://www.digitalrights.ie/wp-content/TranslationVzrvs.Brein.pdf.*
[71] *Brein v. Chello (Utrecht Court), [4.31].*
[72] *Brein v. Chello (Ct. of Appeal), [4.2].*
[73] *Brein v. Chello (Utrecht Court), [4.4].*
[74] *Brein v. Chello (Utrecht Court), [4.28].*
[75] *Brein v. Chello (Utrecht Court), [4.32].*

This observation by the Dutch court also affirms the fact that it would be extremely unlikely for such manual records of P2P infringement activities to be made. Combining the large numbers of allegedly infringing activities that are monitored by the investigators and the fact that the bulk of retail IP addresses are dynamically generated, only automated processes will be able to keep up with the speed of such monitored activities and record such activities to the necessary accuracy as to date and time. There is therefore, in this regard, all the more reason to check and validate the accuracy and reliability of the computer programs developed by the investigators for this purpose. Had the timing errors not been accidentally revealed by MediaSentry in *Brein v. Chello*, the names and addresses of the wrong subscribers would have been disclosed by the ISPs. In countries where there are strong data protection laws, these subscribers may have some plausible redress against the offending ISPs and perhaps even against the right holders and investigators. In other countries, these subscribers would arguably be placed in the invidious position of having to prove their innocence.[76]

Yet there will invariably be some circumstances where subscribers will have to raise sufficient evidence to demonstrate that the evidence adduced that purports to prove their guilt is, in fact, not accurate. This is in the case where the infringing party is someone whom the subscriber has allowed or granted access to his internet account. Prior to the proceedings in *Odex*, based on information provided by the other ISPs, the licensee had pursued action against various infringing parties, who were the parents whose children had used the internet accounts for downloading the titles in question. In *Cinepoly Records (No. 1)*, the Hong Kong court dealt with this objection by observing that in discovery proceedings, the applicant was not required to prove that the subscribers were the infringing parties, only that they could reasonably be assumed to be the infringing parties. The court also offered the opinion that in any event, an internet subscriber was not supposed to authorize others to use his account for infringing purposes.[77] What this illustrates is that the balancing exercise between the interests of the right holders and the interests of the users does not unjustifiably favour one or the other party. Establishing a case based on good faith against the subscriber as the alleged infringer based on circumstances within the control of the right holder is all that the law calls for. Beyond that, a subscriber who enables another to use his internet account for infringing purposes is probably estopped from contending otherwise, if he does not exercise the necessary supervision over his internet account, since that is a matter that is within his control and management.

Conclusions

Pre-action discovery applications against network service providers are both technical and complex. Successful applicants have to demonstrate a clear and careful understanding of both the technical requirements for proving a case based on good faith of infringement against alleged infringers, as well as the evidential rules for doing so with cogent, compelling and admissible evidence. The *Odex* litigation demonstrated these pitfalls very clearly. Any application for pre-action discovery has to at the very least satisfy the courts as to the copyright ownership or exclusive licence in respect of the identified works in question, demonstrate that the alleged infringers had infringed them and provide accurate and reliable information for identifying the infringing parties. There has to be a clear allocation of responsibility for the assertions in the affidavits if the investigations are not personally conducted by the applicant but through the agency of a specialist investigator. Where special expertise is necessary, this has to be amply demonstrated, instead of requiring the court to make suppositions and draw conclusions. There is no reason for computer output not to be subject to close judicial scrutiny for its accuracy or authenticity, in the way the computer and its software were used and operated. Only then could it be said that it is in the interests of justice and convenient in all the circumstances for the court to exercise its discretion to aid the applicant in granting the discovery application as against the ISP as an innocent third party.

Professor Seng is a member of the editorial board.

[76] *For example, see BMG Canada, [21].*
[77] *Cinepoly (No. 1), [29].*

