RDS
ADVOCATES & SOLICITORS

In Business Collaboration:
AMT / ANDERSON MORI & TOMOTSUNE



Digital Evidence And The Limits Of Discovery In Intellectual Property Disputes

17 November 2026

For more information, please contact:

Datuk D P Naban
naban@rdslawpartners.com

Austen Emmanuel Pereira
austen@rdslawpartners.com

Bahari Yeow Tien Hong
bahari@rdslawpartners.com

Farah Shuhadah Razali
farah@rdslawpartners.com

Tan Sri Datuk Harmindar Singh Dhaliwal
harmindar@rdslawpartners.com

Kenny Lam Kian Yip
kenny@rdslawpartners.com

Lim Zhi Jian
jian@rdslawpartners.com

Michael Soo
michaelsoo@rdslawpartners.com

Rosli Dahlan
rosli@rdslawpartners.com

Steven Perian KC
speriankc@rdslawpartners.com

Vinayak Sri Ram
vinayak@rdslawpartners.com

Technology has fundamentally changed the way information is created, stored and exchanged. Documents, communications and business records that were once maintained in physical form are now predominantly stored and transmitted electronically, with computers and other digital devices forming an integral part of modern life. This shift towards a greater reliance on electronic devices has also reshaped the nature of intellectual property.

For instance, the source code of computer programmes and applications may constitute valuable copyright works; trade secrets such as customer information may be stored in digital folders or on cloud servers; patent drawings may exist entirely in electronic forms; and many more. In many modern businesses, some of the most valuable intellectual property may not exist in physical form at all for security and privacy reasons.

However, the digitalisation of intellectual property has also significantly changed the manner in which intellectual property rights may be infringed. For instance, copyrighted works such as computer software may exist entirely in digital form and can be copied, stored and distributed with considerable speed and ease, without the knowledge or authorisation of the copyright owner.

This digital nature of intellectual property also presents particular challenges in gathering evidence of infringement, which may be stored within computers, mobile devices, servers or online accounts that are inaccessible to outsiders.

Furthermore, these devices or systems may contain other unrelated, confidential or privileged information belonging to the suspected infringer. The challenge therefore lies not merely in identifying or establishing an infringement, but in obtaining and preserving the relevant electronic evidence without unjustifiably interfering with the legitimate rights and interests of the suspected infringer.

Obtaining Electronic Evidence In IP Litigation

Fortunately, the law does provide for avenues through which intellectual property owners may obtain and preserve evidence of infringement. Depending on the nature and circumstances of each case, intellectual property owners may apply to the court for an Anton Piller Order, a delivery up order or an order for discovery under Order 24 of the Rules of Court 2012. While these remedies serve different purposes and are subject to different legal requirements, they share a common feature: in appropriate circumstances, they may provide an applicant with access to electronic devices or data in the possession or control of the suspected infringer.

However, electronic devices are repositories of vast amounts of information. A computer may contain privileged communications, personal documents, private correspondence, confidential information belonging to third parties, trade secrets and commercially sensitive material accumulated over years of use. Unrestricted, *carte blanche* access may therefore expose information far beyond that which is relevant or necessary to establish the alleged infringement.

Hence, the courts are consequently required to strike a delicate balance between an applicant's legitimate need to obtain and preserve evidence and the respondent's proprietary rights in other unrelated information.

The High Court's Decision In *Bentley Systems, Incorporated*

In this respect, the decision in *Bentley Systems, Incorporated v PUSB Engineering Sdn Bhd* [2024] MLJU 1782 is instructive. The Plaintiff, Bentley Systems, Incorporated, is a software development company based in Pennsylvania, USA, and the owner of copyright in various computer software used in the design, construction and infrastructure industries, including an offshore structural analysis software known as "SACS Connect Edition" or the "SACS Computer Programs".

Sometime in 2022, the Plaintiff discovered that the Defendant had been using infringing copies of the SACS Computer Programs on 10 electronic devices, mainly computer or laptops, owned by the Defendant or its employees. The Plaintiff subsequently commenced an action against the Defendant for copyright infringement. Approximately two months before the trial, the Plaintiff filed an application under Order 24 rule 3 of the Rules of Court 2012 seeking discovery of various "documents". Amongst things, the application sought the delivery of 10 computing devices used by the Defendant's employees or former employees, softcopies of folders, files and documents relating to the SACS Computer Programs contained in those devices, employment records and activity logs from January 2022 to October 2022, as well as contracts between the Defendant and various third parties.

The High Court dismissed the Plaintiff's application. In respect of the 10 computing devices, the High Court held that the Plaintiff was, in substance, seeking an order for the unconditional delivery up of the devices "*without any attendant terms or conditions preserving and protecting the Defendant's rights*", and such an order would effectively allow the Plaintiff unrestricted access to, and extraction of, the contents of the devices. The High Court emphasised that an application of this nature should have incorporated appropriate safeguards, which are customarily imposed in applications for an Anton Piller Order or a delivery up order, to protect the interests of the party whose devices are being searched.

The High Court identified a non-exhaustive list of safeguards which may be appropriate, including an undertaking as to damages; the appointment of a supervising solicitor to oversee the execution of the order; the involvement of IT experts in the imaging and extraction of data; protocols governing the taking of possession, downloading, imaging and extraction of data; measures to preserve the integrity of the devices and extracted data; restrictions on the disclosure and use of any information obtained; protection of confidential and privileged information; protocols preventing the extraction or disclosure of irrelevant information; and procedures governing the subsequent use of the extracted data as evidence in court.

Importantly, the High Court held that the responsibility lies with the party seeking the order to propose the necessary ancillary safeguards. This responsibility cannot simply be delegated to the court by way of an omnibus prayer for such other relief as the court deems fit. The court may exercise its discretion to impose further safeguards where the terms proposed are inadequate or inappropriate, but the applicant must first identify and seek the protections necessary to ensure that the proposed order is proportionate.

The High Court also dismissed the Plaintiff's application for discovery of the remaining documents. The court considered the application to be an afterthought and was a fishing expedition undertaken to salvage the Plaintiff's case before the trial. This was particularly significant given that the trial had been fixed months earlier and the application was filed only one day before the deadline for filing the bundle of documents. The Plaintiff's application for discovery was dismissed on appeal; notably, the trial subsequently proceeded and was decided in the Plaintiff's favour.

Conclusion

The decision in *Bentley* serves as an important reminder that the pursuit of electronic evidence does not entitle a litigant unrestricted access to any devices of the opposing party. This principle applies equally to infringement actions involving the gathering of electronic evidence or evidence stored within electronic devices and is not confined to cases concerning the infringement of copyrighted software. While the court recognises the legitimate need of intellectual property owners to obtain evidence of infringement, any such access must be circumscribed by appropriate safeguards and protocols to prevent unnecessary intrusion into the proprietary, confidential and other legitimate interests of the party against whom the order is made.

Ultimately, the onus rests on the applicant to propose appropriate protective terms and ancillary safeguards to ensure that the relief sought strikes a proper balance between the need to preserve and obtain relevant evidence and the protection of legitimate interests.

This publication is for educational and informational purposes only and is not intended and should not be construed as legal advice.

KUALA LUMPUR
Level 16, Menara 1 Dutamas No. 1, Jalan Dutamas 1, Solaris Dutamas, 50480 Kuala Lumpur
T: +603 6209 5400
F: +603 6209 5411
enquiry@rdslawpartners.com

PENANG
Suite S-21E & F21st Floor, Menara Northam, No. 55, Jalan Sultan Ahmad Shah, 10050 Penang
T: +604 370 1122
F: +604 370 5678
generalpg@rdslawpartners.com

JOHOR BAHRU
8-35, Menara Delima Satu, Jalan Forest City 1, Pulau Satu, 81550 Gelang Patah, Johor Bahru
T: +607 585 6414
F: +607 509 7614
generaljb@rdslawpartners.com