

PAPER:

CIVIL SEARCH AND SEIZURE OF DIGITAL EVIDENCE: THE EXAMPLE OF THE THAI CENTRAL IP & IT COURT¹

By **Jumpol Pinyosinwat**,
Presiding Judge,
the Central Intellectual Property and
International Trade Court, Thailand

Introduction

The increasing need to gather and use digital evidence in court proceedings has raised many challenges for the procedural laws. The shift from physical evidence to digital evidence often leads to disputable issues of collection of evidence and the admissibility of evidence. In criminal proceedings, the argument for search and seizure of digital evidence usually leads to issues of probable cause, unreasonable search and seizure, and the scope of the criminal investigation. On the other hand, a search and seizure order in civil litigation is often tied to provisional measures or interim injunctions orders, which leads to issue of fair trial arguments. The request for provisional measure orders in civil proceedings has often been used and been developed in intellectual property litigation which also confronts to countless challenging questions.

This paper briefly considers the following: it examines the three main items of legislation related to digital evidence in Thailand; considers civil search and seizure in intellectual property litigation, comparing Article 50.1 of the TRIPS Agreement with the Thai Central IP & IT Court Rule; discusses the grant of a civil search order in some notable court cases; analyzes how the change from physical evidence to digital evidence could affect the civil search and seizure in intellectual property cases, and finally offers some concluding comments.

Thai digital evidence legislative

Major legislative initiatives relating to digital evidence and civil search and seizure in Thailand include the Civil Procedural Code, Rules for Intellectual Property and

International Trade Cases 1997, and the Electronic Transactions Act 2001.

Civil Procedural Code

There is no specific provision for digital evidence in Thai evidence law under the Civil Procedural Code. Most learned scholars view evidence law in Thailand in civil law proceedings, as providing a broad discretion for the admissibility of digital evidence. Parties can adduce digital or electronic evidence as part of scientific evidence, as well as a print-out as documentary evidence. The issue of most concern is the reliability of the digital evidence and any print-out. The parties should establish the proper source and the authenticity of any such data during the trial process.²

Rules for Intellectual Property and International Trade Cases 1997

In 1997, the Rules for Intellectual Property and International Trade Cases (IP Court Rules) established for the first time the principle of admission of computer evidence (rule 33-35). Rule 33 provides as follows:

The Court may admit data recorded in or processed by a computer as evidence in a case, if

- (1) The data recording or processing was done in the ordinary course of business of the user of the computer, and
- (2) The data recording or processing was result from proper operation of the computer according to its

¹ The author is grateful for the useful suggestions of Stephen Mason and insightful comments on an earlier draft by Narumon Saardchom.

² Sophon Rattanakorn, *Payan 382 (Niti Bannakam., Co.) (1996) (Thai)*.

due procedure and, even though the computer is out of order, the accuracy of the data contained therein is not affected.

The use of a computer in ordinary course of business as stated in (1) and the accuracy of the data recording or processing as stated in (2) shall be affirmed by the person involved in the recording or processing, or the person recording or processing the data.

Thus the party intending to adduce digital evidence has to establish that such data was created in the ordinary course of business of the user of the computer, and the data recording or processing was a result of proper operation of the computer accordingly to its due procedure.

These court rules provide modern regulations for adducing digital or computer evidence in Thai litigation. Such standards and rules are deemed to be applied in other specialized courts and general courts, besides the Central IP and IT Court.

Electronic Transactions Act 2001 and 2008

The basis of the Electronic Transactions Act is based on the UNICTRAL Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001), both of which aim to provide the legal framework necessary to support electronic and commercial transactions. The Electronic Transactions Act includes sections on contract formation and validity, and admissibility of data messages as evidence before the courts. The provisions of section 7 of the Act prohibit the denial of the effect and enforceability of evidence solely on the ground that the message is in the form of electronic data message. The integrity of such electronic data message is determined by having regard to its completeness and whether it has been altered, apart from the addition of any endorsement or record or any change that may arise in the normal course of communication, storage or display of the information, which does not affect the integrity of the information.³

Furthermore, the admissibility of a data message as evidence in all legal proceedings shall not be denied solely on the grounds that it is an electronic data message, as indicated by section 11, which has recently amended in 2008 as follows:

The admissibility of a data message as evidence in

the civil proceedings, criminal proceedings, or others, shall not be denied solely on the grounds that it is an electronic data message.

Civil search and seizure in intellectual property cases

In general civil cases, the Thai Civil Procedure Code provides several measures for search and seizure. One important civil search order are the provisional measures before judgment that allows the plaintiff to request a court order to seize or attach the property in dispute or the defendant's property, including any money or property falling due to the defendant by a third person, as provided in section 254(1), which reads:

In a case other than a petty case, the plaintiff is entitled to file with the Court, together with his plaint or at any time before judgment, an *ex parte* application requesting the Court to order, subject to the conditions hereinafter provided, all or any of the following protective measures;

- (1) the seizure or attachment before judgment, of the whole or part of the property in dispute or the defendant's property, including any money or property fell due to the defendant by a third person

Civil search and seizure orders have been widely applied in intellectual property litigation. When enforcing intellectual property rights through civil litigation in most countries, including Thailand, rights holders have enjoyed the faster and more efficient results of civil search and seizure orders. Moreover, the TRIPS Agreement has established an international obligation for all member countries to provide prompt and effective 'provisional measures' to prevent any intellectual property infringements and to preserve relevant evidence in regard to the infringement. Section 3: Provisional Measures, provides, in Article 50(1):

1. The judicial authorities shall have the authority to order prompt and effective provisional measures:
 - (a) to prevent an infringement of any intellectual property right from occurring, and in particular to prevent the entry into the channels of commerce in their jurisdiction of goods, including imported

³ Section 7 Electronic information shall not be denied legal effect and enforceability solely on the ground that it is in the form of electronic data message.

goods immediately after customs clearance;

(b) to prevent relevant evidence in regard to the alleged infringement.

Accordingly, all members of the TRIPS Agreement need to change their domestic laws to provide such provisional measure orders.

Akin to the international standard, the Thai legislation provides special rules of civil searches and seizures for intellectual property enforcement. Rule 12-19 of the IP Court Rules provides provisional measures that allow holders of intellectual property rights to request protection prior to the institution of an action. The Central IP and IT Court grants the order if it is satisfied that there are reasonable grounds as well as sufficient reasons to grant such an application. The applicant also needs to show the nature of the damages, or the prospective defendant is not in a position to compensate the applicant for his damage, or it might be difficult to enforce the judgment against the prospective defendant after the litigation ends. These types of provisional measures are based on the same foundation of the TRIPS Agreement, Article 50.1 (a).

Alternatively, the TRIPS Agreement, Article 50.1 (b) is identical to the IP Court Rules, Rule 20-22—application for taking of evidence in advance. For this court order, the application must state the facts showing the necessity for taking of evidence in advance. In cases of emergency, the motion is required to state the facts showing the emergency situation in which such evidence will be damaged, lost, destroyed or difficult to be adduced at a later stage.

Accordingly, civil searches and seizures in intellectual property cases in Thailand are fully equipped with prompt and effective provisional measures, both provisional measures and applications for taking of evidence in advance. Additionally, the Central IP and IT Court provides a very speedy inquiry process, in that such orders will usually be granted within a few hours after the filing.

An example of how a court will provide for the search and seizure of evidence is illustrated in the Vilsco B.V. case.⁴ Vilsoco, a Netherlands company, claimed to be the copyright holder of certain textile designs. Later, Vilsco found that a Thai company had copied their designs, produced, and distributed copies of textiles in the market. Vilsco requested the Central IP and IT Court

to issue a provisional measure order under Rule 12, to stop the infringement by seizing the infringing textiles, documents related to sales and distribution, and shutting down the manufacturing plant. Vilsco showed reasonable grounds and sufficient reason for the application by adducing videotapes produced by a private investigator that that worked as an undercover worker. He videotaped some areas in the plant, including the infringing textiles. Also, Vilsco contended that such a small sized plant could be shut down and moved rapidly, which meant it was therefore an urgent matter to stop the infringement, as well as seize all the related evidence in advance under Rule 20-22. The Central IP and IT Court granted the provisional measures to stop the infringement by temporarily shutting down the printing machines, as well as ordering civil searches under Rule 20-22 to enable Vilsco to examine and temporarily seize all related sale orders, receipts, and related documents. Additionally, the court ordered Vilsco to present a guarantee of damages.

In the Thai Petrochemical Industrial (TPI) case,⁵ TPI announced their insolvency status and petitioned to begin the restructuring process. At the same time, a property investigation was performed by the comptroller in bankruptcy. During this processes, TPI made a request of the Central IP and IT Court for a provisional order under Rule 20-22 to inspect a private website operated by TPI's former CEO, as well as to print all the web pages and related information. TPI claimed that the former CEO intentionally published wrong and fallacious information with the purpose of defaming TPI and the current board of executives. Also, TPI submitted that it was necessary to take evidence in advance, because the alleged web site was a private web site and could be altered or modified at any time. The alteration would be technically difficult to recover at a later date. The Central IP and IT Court finally granted the civil searches under Rule 20-22 to enable TPI to inspect the alleged web site, as well as produce related documents in the form of print-outs.

In the UBC Broadcasting (UBC) case,⁶ UBC—a cable operator—received a report from its private investigator that the owner of a middle size apartment in Bangkok illegally received the UBC signal and re-transmitted the signal to its lessees. The investigator went under cover to rent a room from the apartment and made a request for a free UBC service. The owner agreed to provide the

⁴ *Central IP and IT Court case number Deang. Sor. 2/2542 (1999). The Central IP and IT Court considered all the evidence and granted a provisional order ex parte on the same day that the application was filed (20 December 1999).*

⁵ *Central IP and IT Court case number Deang. Sor. Por. 2/2544 (2001). The Central IP and IT Court examined all the evidence and issued an ex parte provisional order on the same day that the application was filed (4 July 2001).*

⁶ *Central IP and IT Court case number Deang. Sor. Por. 1/2549 (2006). The Central IP and IT Court considered all the evidence and granted a provisional order ex parte on the same day that the application was filed (2 March 2006).*

connection for the service at no cost. The investigator then recorded every process, including the television as it was broadcast in his rented room. UBC requested a provisional order under Rule 20-22 from the Central IP and IT Court to inspect the apartment and to seize all broadcasting equipment and related documents.

The Central IP and IT Court finally granted such civil searches under Rule 20-22 in favour of UBC. The order specified that the search had to be conducted by an officer from the Department of Execution and UBC. However, the court only allowed UBC to videotape or photograph the infringing equipment to use as evidence in court, because there was no need to seize all of the broadcasting equipment at once. The court order also limited the duration of the order by allowing UBC fifteen days to execute the search order, and conversely ordered UBC to present a guarantee in damages in the sum of 10,000 Baht (approximately US\$ 320).

Civil search and seizure of digital evidence

Although the Central IP and IT Court has the tendency to grant civil searches and seizures in intellectual property litigation, the shift from physical evidence to digital evidence makes the issues surrounding the collection and seizure of digital evidence even more complicated. In intellectual property cases, demonstrating the necessity for the taking of evidence between physical and digital evidence has some similarities. However, the scope and limit of searches and seizures of intangible property is much more doubtful, compare to those of physical evidence.

Computers and other digital devices are now used for almost every activity; for example, business records, personal data, private records, documents, images and the storage of music. Moreover, it is certain that the amount of digital property used will continue to rise. In addition to the question of endless scope of digital evidence, the most important problem is how to separate the relevant digital evidence. Evidence in the physical form is distinct and is relatively easily separable from a physical location. Parties and officials can see and divide the relevant physical evidence with their bare eyes. In comparison, digital data must be interpreted through machines.⁷ The questionable issue is whether the party or any officials responsible for executing a civil search order has the right to ‘open’ every file on a digital storage device in order to see what data is really relevant to the court order or not.

In the AutoCAD case,⁸ Autodesk—AutoCAD’s right holder—filed a copyright case seeking civil damages from an ink cartridge company, claiming the cartridge company infringed its AutoCAD program. Autodesk also requested the Central IP and IT Court’s provisional measure order under Rule 20-22 for entering the cartridge company, inspecting, and seizing all digital evidence, computers, and hard disks of that cartridge company. Prior to the filing, Autodesk hired a group of people to search the job seeker section from the internet and newspapers. The people hired by Autodesk searched for job positions that required the ability to use the AutoCAD program. Then, they selected a list of companies and telephoned to check if the company had AutoCAD programs in their workplaces, and if so, how many they had. In this case, the staff found that it was highly possible that a particular cartridge company had an illegal AutoCAD program in its office. Autodesk therefore filed the civil case without any prior notice and requested an *ex parte* order from the court to seize all digital evidence, computers, and hard disks.

The petition was filed on 31 October 2007, and the Central IP and IT Court examined the petition *ex parte*. It declined the petition on the same day, reasoning that

‘...[Application for taking of evidence under] Rule 20 shall establish the facts showing the necessity for the taking of evidence which means such evidence on which the applicant may have to rely in the future will be lost or become difficult to adduce at a later stage. In this case, the petitioner states that the cartridge company has used piracy computer software. Although such a fact is correct and the cartridge company infringed the petitioner’s copyright, the petition has not stated or established that such copyright infringement contains any particular feature, compared to an ordinary copyright infringement. Without particular features or special consequences, the petitioner cannot establish a distinctive necessity for the taking of evidence in advance.’

Autodesk later file a further three petitions to request the same provisional measures under the same rule on 26, 27, and 30 November, 2007, claiming the same reason that its AutoCAD software could be easily deleted or destroyed, however, the Central IP and IT Court confirmed the orders would be denied.

⁷ Stephen Mason, *Electronic Evidence: Disclosure, Discovery & Admissibility*, (LexisNexis Butterworths, 2007) Chapters 1 and 2; Ray Ming Chang, *Why the Plain View Doctrine Should Not*

Apply to Digital Evidence, 12 *Suffolk J. Trial & App. Advoc.* 31, 35-37 (2007); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 *Colum. L. Rev.* 279, 292-293 (2005).

⁸ *Central IP and IT Court case number Deang. Tor. Por. 158/2550 (2007)*. The Central IP and IT Court declined the search and seizure petition to search and seize computer software.

Concluding comments

Powers of search and seizure in civil proceedings have been widely used by intellectual property rights holders to enjoy faster and more efficient results of civil search. Nevertheless, the shift from physical evidence to digital evidence leads to questionable issues of the reasonableness of a digital search, and the scope and limit of the search. The AutoCAD case is an excellent example to illustrate the rationale of a digital evidence search in the Thai courts. Whereas the petitioner tried to claim the special character of computer software which could be easily deleted or destroyed, the Central IP and IT Court reasoned that merely claiming the universal feature of computer software was not enough to establish a distinctive necessity for the taking of evidence in advance. In addition, the use or reproduction of piracy software by a very small scale infringer alone, such as an end-user, might not justify the granting of a provisional measures or search order.

Besides the wide scope and inseparable character of digital evidence as mentioned, the search and seizure of digital evidence in civil proceedings is facing other numerous arguable issues. Some challenging questions include the justification of general digital search or

unrestricted scope search, the proper limit of digital search in a court order (for example, allowing only certain file types, excluding deleted files), the on-site search, or time limits.⁹ It may be too soon to claim any conclusion, since the existing legal rules will naturally change in response to the changes of technology. Digital evidence extends beyond borders, since we all share the same networks and same digital world. In a broad comparison with different approaches, we may expand to embrace new and creative procedures for regulating the collection of digital evidence.

© Jumpol Pinyosinwat, 2008

Jumpol Pinyosinwat is also Director of the Intellectual Property Research Center, ECAP II, the Honorable Advisor to the Committees on Independent Body Affairs of the Thai Parliament, an Adjunct Professor at the Law School of Golden Gate University, US, and Adjunct Professor at the Law School of Bangkok University, Thailand.

⁹ Orin S. Kerr, *Search Warrants in An Era of Digital Evidence*, 75 *Miss. L. J.* 85, 95-98 (2005).