ARTICLE:

Electronic evidence and electronic discovery in the Hong Kong Special Administrative Region, People's Republic of China

By **Ronald Yu**

Law of evidence in general

Sources of law

In the Hong Kong Special Administrative Region (the 'HKSAR') all evidence, whether electronic or not, must be relevant and must not fall into one of the exception categories. In other words electronic evidence, as with other forms of evidence, needs to comply with standards of admissibility governing all forms of evidence according to the laws of the HKSAR and must comply with rules relating to the production of such evidence. This means that parties adducing evidence must be cognizant of the differences between criminal and civil proceedings.

Although constitutionally integrated into the People's Republic of China, the HKSAR retains the common law system that had been in place before Hong Kong's handover from the United Kingdom to China on 1 July 1997. In accordance with the constitution of Hong Kong, the Basic Law of the HKSAR (the 'Basic Law'), that laws applied before the handover and the common law became part of the laws of Hong Kong in accordance with art 8 of the Basic Law , which reads:

> 'The laws in force in the Hong Kong Special Administrative Region shall be this Law, the laws previously in force in Hong Kong as provided for in Article 8 of this Law, and the laws enacted by the legislature of the Region…'[1]

In addition, art 84 of the Basic Law states the following:

> 'The courts of the Hong Kong Special Administrative Region shall adjudicate cases in accordance with the laws applicable in the Region as prescribed in Article 18 of this Law and may refer to precedents of other common law jurisdictions.'

Relevant statutory authorities with respect to electronic evidence, include the Hong Kong Evidence Ordinance, Cap 8; the Criminal Procedures Ordinance, Cap 221 and, with respect to electronic records and signatures, the Electronic Transactions Ordinance, Cap 553.

Types of evidence

Primary and secondary evidence

As Hong Kong's rule of evidence derives from the common law, rules governing the primary and secondary concepts of evidence are generally the same as in England and Wales.

Electronic records

In recognition of the increasing use of electronic signatures and the increase in global e-commerce, the Electronic Transactions Ordinance, Cap 553 ('ETO'), which came into operation on 7 January 2000 and was updated in June 2004, was enacted to provide statutory recognition to transactions done electronically. The ETO gives statutory recognition for

[1] It should be noted that the rest of art 8, Basic Law reads:
'…National laws shall not be applied in the Hong Kong Special Administrative Region except for those listed in Annex III to this Law. The laws listed therein shall be applied locally by way of promulgation or legislation by the Region.
The Standing Committee of the National People's Congress may add to or delete from the list of laws in Annex III after consulting its Committee for the Basic Law of the Hong Kong Special Administrative Region and the government of the Region. Laws listed in Annex III to this Law shall be confined to those relating to defence and foreign affairs as well as other matters outside the limits of the autonomy of the Region as specified by this Law.
In the event that the Standing Committee of the National People's Congress decides to declare a state of war or, by reason of turmoil within the Hong Kong Special Administrative Region which endangers national unity or security and is beyond the control of the government of the Region, decides that the Region is in a state of emergency, the Central People's Government may issue an order applying the relevant national laws in the Region.'

contracts entered into by offer and acceptance by way of electronic means, without disturbing the common law right of the offeror specifying the method of communication of acceptance.[2] However, it is not applicable to the following classes of documents: wills, trusts, power of attorney, stampable instruments (for example, contracts for sale of shares and conveyancing instruments), oaths and affidavits, statutory declarations, judgments or orders of the court, negotiable instruments and warrants issued by a magistrate or a judge.[3]

The ETO also has provisions pertaining to the satisfaction of rules of law that require the information to be given in writing; that information be presented or retained in its original form; and for the retention of certain information in writing or otherwise. In this manner, the ETO treats electronic transactions in the same way as physical transactions.

Where information must be given in writing
Under s 5, ETO, if an electronic record is accessible for future reference, then the information contained therein satisfies a rule of law that requires or permits the information to be given in writing.

Where information must be presented or retained in its original form
A document in the form of an electronic record satisfies a rule of law that requires that certain information be presented or retained in its original form, provided there is a reliable assurance as to the integrity of the information from the time it was first generated in its final form to the time it is required. The information must be capable of being displayed in a legible form.[4] The criterion for assessing the integrity of the information is whether the information has remained complete and unaltered, except for changes that arise in the normal course of communication, storage (for example, the time which the file was saved during a back-up may change), display or by the addition of any endorsements.[5] The standard of the reliability of the assurance is determined by the purpose for which the information was generated and all the other relevant circumstances.[6]

Where information must be retained in writing
Where a rule of law requires that certain information be retained in writing or otherwise, the retention of electronic records satisfies this requirement if: (i) the information contained in the electronic record remains accessible for subsequent reference; (ii) the relevant electronic record is retained in the format in which it was originally generated, sent or received, or in a format that can be demonstrated to accurately represent the information originally generated, sent or received; and (iii) the information identifying the origin and destination of the electronic record and the date and time when it was sent or received is retained.[7]

Admissibility of an electronic record
An electronic record cannot be denied admissibility as evidence in any legal proceedings on the sole ground that it is an electronic record[8] without prejudice to any rules of evidence,[9] although for almost all court proceedings in Hong Kong,[10] the retention, signing and sending by electronic means does not apply.[11] In other words, pleadings, affirmations, service and filing of these documents must still be done physically.

Service of documents
Except for the limited purposes of the proceedings specified in Schedule 3 to the ETO – that is, landlord and tenant-related, government rent and rates – the service of documents by electronic means is treated as satisfying the requirement of personal service or service by post.[12] In 2007, Schedule 3 was amended to extend electronic service to water and electricity bills and tax returns. Electronic service was further extended to delivery and completion of a schedule served under the Census and Statistical Ordinance, Cap 306 in 2009 and the Business Registration Ordinance, Cap 310 in 2010.

Electronic and digital signatures

The ETO differentiates between digital and electronic signatures. Under s 2, ETO, an 'electronic signature' means 'any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record', while a 'digital signature' is defined as follows:

[2] Electronic Transactions Ordinance, s 17.
[3] Electronic Transactions Ordinance, Sch 1.
[4] Electronic Transactions Ordinance, s 7.
[5] Electronic Transactions Ordinance, s 7(2)(a).
[6] Electronic Transactions Ordinance, s 7(2)(b).
[7] Electronic Transactions Ordinance, s 8(1).
[8] Electronic Transactions Ordinance, s 9.
[9] For example, relevance of the evidence or requirements under ss 22A or 54 of the Evidence Ordinance.
[10] Electronic Transactions Ordinance, Sch 2.
[11] Electronic Transactions Ordinance, s 13 excluding the applications of ss 5, 5A, 6, 7 and 8.
[12] Electronic Transactions Ordinance, s 5A.

> 'in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine-
>
> (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and
>
> (b) whether the initial electronic record has been altered since the transformation was generated.'

The major technical difference lies in the use of an asymmetric cryptosystem and a hash function in the case of a digital signature.

Among private citizens, if one party signs a document with an electronic signature and the other party consents to such a mode of signing, then the electronic signature satisfies a rule of law requiring the signature of a party on a document.[13] However, if one of the parties is signing on behalf of the government, then a digital signature is required.[14]

Admissibility

Authentic

To be admissible evidence must be authentic, and in the case of digital records, the reliability (and thus probative value) of digital records will depend on how the information is stored, preserved and retrieved; how the information is supplied in the course of normal activities; and how well the device is protected from undue interference or whether it was working properly. As the evidential weight of digital evidence is dependent on the procedures used to create the record and the safeguards used to preserve the data or the operational integrity of the device, it is imperative that investigators take care to preserve evidence, maintain chains of custody and extract file data such as the time of creation or whether data had been deliberately tampered with. Guidelines on the proper collection and preservation of electronic evidence are available from the website of the Information Security and Forensics Society of Hong Kong.[15]

Relevance

All evidence, whether electronic or not, must be relevant to a material issue in order to be admissible; material issue referring to a fact in issue in the case.[16] Therefore relevance must be viewed in the context of the individual facts, in particular the issues involved.

Exceptions

There are several exceptions to excluding relevant evidence to be tendered at trial including opinion, expert witnesses, a general exclusion in criminal cases, and hearsay.

The role of expert witnesses

The common law rules governing the use of experts and their ability to give their opinion on the 'ultimate issue' in Hong Kong are the same as in England and Wales. Expert evidence is admissible provided it is relevant to a fact in issue, necessary, that the science or scientific method being applied is sufficiently reliable and that the witness is properly qualified to give evidence. Section 65DA of the Criminal Procedures Ordinance, Cap 221 (the 'CPO') governs the exchange of expert reports prior to trial in criminal cases. An accused should disclose their expert report as soon as practical after the committal to the Court of First Instance or transfer to the District Court. Section 65DA CPO does not apply to cases in the magistrates' courts, therefore there is no statutory time limit for an accused to do so in such instances. It is the duty of the prosecution to make disclosure in advance of the trial, and s 65DA CPO governs the time for the defence to disclose their expert report in practice.

Hearsay

Hearsay evidence is inadmissible under common law. Generally speaking, digital data may be records that have been produced as a result of the computer being used as a calculator;[17] information the device has been programmed to record, so there is no effective human input;[18] or have directly or indirectly been entered by a person, then recorded and processed by

[13] Electronic Transactions Ordinance, s 6(1).

[14] Electronic Transactions Ordinance, s 6(1A).

[15] Computer Forensics, 'Part 1: Introduction to Computer Forensics, Computer Forensics', Part 2: Best Practices, Computer Forensics: Glossary', available at http://www.isfs.org.hk/manual.html .

[16] Simon N. M. Young, *Hong Kong Evidence Casebook*, (2004), Sweet & Maxwell, p 32.

[17] *R v Wood* 76 Cr App R 23, CA; *R v Spiby* (1990) 91 Cr App R 186, (CA).

[18] *R v Spiby* (1990) 91 Cr App R 186, (CA).

the device. Digital data may be stored either on an individual basis (such as an owner taking a photograph of his new car with his digital camera and storing the image on his computer) or as part of a process (such as a store using a computer as part of its sales procedures).

While individual digital evidence may be admissible: for example, 'a picture of a car was found on the man's computer', to prove the event depicted in the picture actually occurred would require testimony – for example, if the picture showed the car at a park on a particular day and time, the owner might need to testify that his vehicle was indeed at that location on that day and at that time.

The considerations are different for data generated as part of a process. For example, if a person borrows a book from a library, the librarian may scan in the information from the barcode attached to the book into a computer, which would then make a digital record of the transaction (for example, that person A borrowed a particular book on a particular date). At some future date, the information can be retrieved for other purposes: for example to check whether person A has any overdue books. However, as the record is kept as part of a regular process it would be difficult, though not impossible, for the librarian to recall that he or she rented out a particular book to a particular person on a particular date. Indeed, if the librarian retained a paper ticket identifying the book in a cardboard pouch with A's name, they would still not be able to recall that they rented out a particular book to a particular person on a particular date.

In such a case, the library's computer is presumed to be working properly and the record would be admissible as evidence – for example, to show that person A rented book B on a particular date by the production of the relevant computer record unless it can be shown that the computer had been tampered with, was not working properly, or was not sufficiently protected from undue interference or, for example, the librarian provides specific testimony about the accuracy or validity of a particular record and can successfully challenge the integrity of the library's process.

In *R v Spiby*[19] the court recognised an important boundary to the hearsay rule – that rule does not apply to data recorded by a machine without human intervention.[20] Computer-generated documents therefore may or may not be hearsay in nature depending on whether the document was created or had some form of human input. In *Luitel Shom Prasad v HKSAR*,[21] the admissibility of a report generated from the information recorded on the card holder's stored value smart card that showed the times and dates that the card (and by inference the card holder) was used to enter and exit the Mass Transit Railway (MTR) station – and this evidence was not challenged.[22] However, if a computer was used to transmit information observed and recorded by a person, the hearsay rule applies if the facts recorded need to be proven, as in the case of *The Queen v For Kau*,[23] where an operator entered and sent a caller's telephone number to a recipient's pager.

In civil proceedings, experts may be called by either party or by the court pursuant to Order 40 of the Rules of the High Court ('RHC').[24]

Hearsay in criminal proceedings

The common law prohibition on hearsay is retained for criminal cases. Hearsay evidence is generally inadmissible unless there are other rules admitting the hearsay evidence, for instance an oral admission of an accused under caution. There is some movement to change this. On 30 November 2005, the Hearsay in Criminal Proceedings Sub-committee of the Law Reform Commission of Hong Kong[25] released a consultation paper followed four years later by a report on *Hearsay in Criminal Proceedings*.[26] In the report, the Commission proposed that relevant and

[19] (1990) 91 Cr App R 186, (CA).

[20] Simon N. M. Young, *Hong Kong Evidence Casebook* (2004), Sweet & Maxwell, p 289.

[21] *[2002] HKEC 157, CFI, [2002] HKCFA 3, FAMC10/2002 (7 June 2002).*

[22] Riders on Hong Kong's MTR may use a stored value smart card known as an Octopus card to enter and exit MTR stations. The entry and exit times are automatically recorded. During the trial, counsel for Prasad raised an objection that as the report relating to the Octopus card had not been disclosed, the prosecution breached its duty to disclose this evidence. On first appeal, *HKSAR v Luitel Shom Prasad* [2002] HKCFI 289, HCMA766/2001 (31 January 2002), Beeson J accepted that non-disclosure constituted a material irregularity but concluded that the irregularity did not cause any unfairness and did not affect the result. This was upheld by the Court of Final Appeal in *Luitel Shom Prasad v HKSAR* [2002] HKCFA 3, FAMC10/2002 (7 June 2002).

[23] [1994] 1 HKCLR 122.

[24] The Rules are made under s 54 of the High Court Ordinance, Cap 4.

[25] Hearsay in Criminal Proceedings Sub-committee, The Law Reform Commission of Hong Kong, *Consultation Paper: Hearsay in Criminal Proceedings*, (November 2005), available at http://www.hkreform.gov.hk/en/publications/crimhearsay.htm.

[26] The Law Reform Commission of Hong Kong, *Report on Hearsay in Criminal Proceedings*, (November 2009), available at http://www.hkreform.gov.hk/en/publications/rcrimhearsay.htm.

reliable hearsay evidence should be admitted under a comprehensible and principled approach where there is a need for such evidence, while unreliable and irrelevant hearsay evidence should be excluded.

Hearsay in civil proceedings

In civil cases, hearsay evidence is governed by Part IV of the Evidence Ordinance ('EO'), and hearsay evidence is generally admissible unless the court is satisfied, having regard to the circumstances of the case, that the exclusion of evidence is not prejudicial to the interests of justice.[27]

Rules of production of electronic evidence

Form of production

In general, if a document in question is not in dispute and is tendered by consent, then the form of production is not important; the court will accept either the original document or a copy of it.

Banker's records

Banker's records' are records that are kept by a licensed bank[28] and are defined in s 2, EO as:

> '(a) any document or record used in the ordinary business of a bank; and
>
> (b) any record so used which is kept otherwise than in a legible form and is capable of being reproduced in a legible form.'

Banker's records' are admissible in both civil and criminal cases by the production of either the original or a physical copy irrespective of whether the (banker's) records have been stored physically or electronically.

If the records are kept on a computer, a print-out from a computer will suffice[29] although, in accordance with s 20(3), EO, it must be proved that a document produced by the computer that is tendered in evidence as a copy: ' … was so produced under the direction of a person having practical knowledge of and experience in the use of computers as a means of storing, processing or retrieving information' and that during the period when the computer was used for the purpose of keeping such record:

> '…appropriate measures were in force for preventing unauthorized interference with the computer; and… that during that period, and at the time that the document was produced by the computer, the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents…'[30]

Under s 20A, EO, the same principles apply to banks that have ceased business[31].

Electronic discovery in Hong Kong

General principles

Electronic discovery in Hong Kong is governed under Order 24 of the RHC, although because of the nature of the documents, the volume involved and their accessibility the treatment of electronic discovery differs from that of hard-copy documents discovery. An application for e-discovery is made under Order 24 Rule 7 of the RHC and requires support of an affidavit.[32] The Court will determine whether discovery is necessary under Order 24 Rule 8 of the RHC.

Relevant legal principles under Order 24 RHC

A party seeking specific discovery of documents must make a *prima facie* case that:

1. there is in existence a specified document or class of documents; class documents are classified by nature, not by issues;[33]
2. the party against whom the order is sought has or had the document in his possession, custody or power;
3. the document or class of document relates to a matter in question in the action; and
4. discovery thereof is necessary either for disposing fairly of the cause or matter or for saving costs.[34]

Discovery is only granted if it was necessary for fairly disposing of the cause or matter – even if existence,

[27] Evidence Ordinance, s 47(1)(b).
[28] Meaning a bank with a valid banking licence granted by the Monetary Authority: see ss 2 and 16 of the Banking Ordinance, Cap 155.
[29] Evidence Ordinance, s 20.
[30] Evidence Ordinance, s 20(3)(b) and (c).
[31] Evidence Ordinance, s 20A.
[32] Order 24 Rule 7(3) RHC.
[33] *Deak and Co (Far East) Ltd v NM Rothschild and Sons Ltd*, [1981] HKC 78 Para 17.
[34] *Full Range Electronics Co. Ltd. v General-Tech Industrial Ltd & Another* [1997] HKCFI 396 at Para4, *The Incorporated Owners of Kodak House II and No. 321 Java Road v Kai Shing Management* [2012] HKCFI 1559 at [9].

possession etc. and relevancy were established[35] and the task of the court will often be to determine when the discovery exercise passes from the necessary and permissible to the unnecessary and impermissible.[36]

While the pleadings in an action define the issues to be tried, that an issue is raised in the pleadings is not determinative as to whether it relates to a matter. Discovery is not required of documents that relate to irrelevant allegations in pleadings which, even if substantiated, could not affect the result of the action.[37]

A party that fails to both comply with a court order and cooperate with the other party for discovery will be required to pay the extra costs the other party incurred to gain access to the electronic documents. Additionally, de-duplication of electronic documents must be ensured and a party failing to carry out this process may be ordered to pay the costs to the other party. Finally, a 'staged' approach can be adopted for appropriate cases so that one may start the search of the electronically stored information with the most important people.[38]

Practice Direction SL 1.2 (PD SL 1.2)

On 1 September 2014, PD SL 1.2 came into effect implementing a pilot scheme for the discovery and inspection of electronically stored documents in the Commercial List. The pilot scheme has continued to operate since. The Practice Direction applies to all actions started in or transferred to the Commercial List where the claim or counterclaim exceeds HK$8 million, and there are at least 10,000 documents to be searched for the purposes of discovery; or where the parties agree to be bound by the Practice Direction or where the court directs the parties to follow PD SL1.2 though existing rules related to the discovery and inspection of documents between parties under Order 24 of the RHC still apply.

Aims and schedule of PD SL 1.2

The purposes PD SL 1.2 are to provide a framework for reasonable, proportionate and economical discovery and supply of Electronic Documents under Order 24 RHC and to encourage and assist the parties to reach agreement in relation to the discovery of such documents in a proportionate and cost-effective manner.

The wording of PD SL 1.2 emphasizes the efficient management of electronic documents, the use of technology to ensure document management activities are undertaken effectively and efficiently, and that the cost of discovery of electronic documents must be proportionate to the amounts claimed in the proceedings.[39]

This is reflected both in the Practice Direction's mention that it is limited to electronic documents 'directly relevant to an issue arising in the proceedings … which are likely to be relied on by any party to the proceedings …. or which support or adversely affect any party's case'[40] and that 'background' or other electronic documents that might lead to a 'train of enquiry' need not be discovered.[41] This is also reflected in its provisions that the court will not accede to applications for photocopies or paper copies of electronic documents[42] unless there is good reason to do so, as well as in provisions defining what constitutes 'reasonable search'[43] where the Practice Direction lists relevant factors such as the circumstances of the case, the numbers of electronic documents involved, the nature and complexity of the proceedings, the ease and expense of retrieving documents,[44] the availability and significance of electronic documents that are likely discovered during the search.[45]

In addition to the main text, PD SL 1.2 includes four schedules:

I. Guidance Notes on Discovery of Electronic Documents

II. Electronic Documents Discovery Questionnaire ('EDDQ')

III. Guidance Notes on the EDDQ

[35] *Deak and Co (Far East) Ltd v NM Rothschild and Sons Ltd*, [1981] HKC 78 at [16].
[36] *Mariner International Hotels Ltd v Atlas Ltd & another,* [2002] HKCFI 1300 at [9].
[37] *Paul's Model Art Gmbh & Co KG v U.T. Limited & Ors* [2005] HKCA 481 at [25].
[38] *Chinacast Education Corporation and Others v. Chan Tze Ngon and Others*, [2014] HKCFI 1489; [2014] 5 HKC 277; HCA 1062/2012 (15 August 2014) at Para 28
[39] Paras 4(1)-(3) PD SL1.2.
[40] Para 5(1) PD SL1.2.
[41] Para 5(2) PD SL1.2.
[42] Pursuant to Order 24, rules 9, 11 and 11A of the RHC. Footnote 1 PD SL1.2.
[43] Paras 17-21, see in particular paras 17-19 PD SL1.2.
[44] This in turn may depend on how easy documents can be viewed, their location, the devices involved, their likelihood of location, the cost of recovery if they are not easily available as well as other associated costs, their likelihood of being materially altered in the course of recovery, discovery or supply. Para 18(3) PD SL1.2.
[45] Paras 17, 18 PD SL1.2.

IV. Sample Protocol for Discovery of Electronic Documents.

Case management conference
Prior to the first Case Management Conference (CMC), the parties need to discuss how they will use technology, both in the management of electronic documents and the conduct of proceedings, to:

1. Create lists of electronic documents to be disclosed,

2. Conduct the actual process of discovery by the provision of documents and information about electronic documents, and

3. Present documents and other materials at trial.

The parties can choose to adduce evidence at trial in the format of electronic documents, but may need to bring along their own devices equipped with any necessary software or specialised technology for presentation to the court.[46]

The Electronic Documents Discovery Questionnaire (EDDQ)
The EDDQ provides a means for the parties to obtain and exchange the requisite information in a structured manner and is designed to help the parties reach agreement on a proportionate and cost-effective manner of effecting discovery and the supply of electronic documents with regard to the underlying objectives under Order 1A of the RHC.[47] The EDDQ allows parties to propose limiting the search to specific date ranges in addition to other proposals regarding the extent of the search.

There are questions for information about the various issues that are relevant to the parties':

Electronic documents, communications, document management and database systems

Data formats for electronic documents

Document retention policies

Past instructions, if any, to preserve electronic documents

Use of encrypted files

Data custodians

The parties can also identify problematic geographical locations of files (such as locations that might hamper the collection of data) and legacy application systems that may contain potentially relevant data.

Service obligations
The parties must serve a draft EDDQ when they serve their respective pleadings with a view to reaching agreement on the scope and extent of the discovery exercise and tools to be used. A signed, completed EDDQ verified by a statement of truth[48] must be filed with the court, together with the Information Sheet for the first CMC,[49] no later than seven days before the first CMC.[50]

Documents under PD SL 1.2
The definition of 'documents' under PD SL 1.2 is consistent with that under Order 24 RHC, which includes tape recordings, computer databases and word processing files.[51] Under PD SL 1.2, 'document' is broadly defined as 'anything upon which data, information or evidence is recorded in a manner intelligible to the senses or capable of being made intelligible by the use of equipment and includes 'electronic documents',[52] which are defined as any data or information held in electronic form that are stored on any device, including portable devices, memory sticks, mobile telephones, computer systems, electronic devices and media, servers and back-up systems.

In addition, a 'document' can be an e-mail[53] and other electronic communication such as a text message or voicemail, a word-processed document or a files, image, sound recording, video, web page, databases, metadata,[54] embedded data not typically visible on

[46] Para 32 PD SL1.2.
[47] Schedule 1, Para 4 PD SL1.2.

[48] The person signing the statement of truth must be available to attend the hearing of the first CMC and any interlocutory applications relating to discovery. That person may be a party, its employee or an electronic discovery specialist or digital evidence specialist. Para 14 PD SL1.2.
[49] The Information Sheet submitted to court should include a summary of the matters on which the parties agree and on which they disagree in relation to the discovery of electronic documents (including agreements on orders and protocols for the discovery and supply of electronic documents). Para 16 PD SL1.2.
[50] Schedule 1, Para 10 PD SL1.2.
[51] Hong Kong Civil Procedure 2016, Vol. 1, Part A, Hong Kong Sweet & Maxwell, (c) 2015, p. 572
[52] Para 3(3) PD SL1.2.
[53] PD SL1.2 notes that there are various types of e-mail system (for example, Outlook, Lotus Notes, web-based accounts), whether stored on personal computers, portable devices or in web-based accounts (for example, Yahoo, Hotmail, Gmail). See Footnote 17, PD SL1.2.
[54] PD SL1.2 defines 'metadata' as '…data about data. In the case of an Electronic Document, Metadata is typically embedded information about the document, in addition to the user generated content, some of which is not readily accessible once the Native Electronic Document has been converted into an electronic image or a paper

screen or in a print out and includes data or information held in electronic form that has been deleted but not yet overwritten.[55]

Electronic document lists

Parties may agree to provide document lists in an electronic file in .csv (comma-separated values) or other agreed format. Should a party already possesses data relating to the documents making this possible, for instance date of creation and type of document, this may be acceptable, provided each electronic document is given a unique reference number so far as is possible.

Documents should be listed individually and, where a different order would be more convenient, parties may list documents in an order other than date order,[56] but must be consistent in the way they list electronic documents with consistent column headings repeated on each page of the list. Discovery list numbers used in any supplemental lists of electronic documents should be unique and should run sequentially from the last number used in a previous list.[57]

Privileged documents and the process of discovery

In their discussions prior to the first Case Management Conference (CMC), the parties need to identify privileged or other non-disclosable documents (for instance, those involving trade secrets), identify areas of agreement and disagreement and discuss discovery-related procedures, methodologies and scope.

PD SL 1.2 suggests such discussions cover:

> 1. The categories of electronic documents within the parties' control, the computers, storage systems, devices and media on which any relevant electronic documents may be found. The Practice Direction envisages that the primary source of discovery is normally 'reasonably accessible data' and though a party may request specific discovery of electronic documents that are not reasonably accessible, it must demonstrate that the relevance and materiality of these documents and justify the cost and burden of retrieving and producing them.[58]
>
> 2. Document retention policies.
>
> 3. The scope of the reasonable search (as required by Rule 15A, Order 24, RHC).
>
> 4. The use of tools and techniques to reduce the burden and cost of electronic discovery, including:
>
> > a. The use of agreed keyword searches,[59] concept searching,[60] data sampling,[61] technology assisted review or other technologies or software tools. PD SL1.2 encourages parties to use keyword searches and other automated search techniques where a full review of each and every electronic document would be unreasonable. Such search techniques can be supplemented with other technologies where such automated methods of searching are insufficient. Parties are warned to consider the limitations of such tools with certain types of files – for example document images from scanners or electronic facsimile transmissions, photographs, videos and audio recordings are not readily text searchable – and that the injudicious use of automated search techniques may result in failure to find important electronic documents which ought to be discovered and/or may result in the retrieval of excessive numbers of irrelevant electronic documents, which if discovered would place an excessive burden in time and cost on the party to whom discovery is given.[62]

document. It may include, for example, the purported date and time of creation or modification of a word-processing file, or the purported author and the purported date and time of sending an e-mail. Metadata may be created automatically by an operating system, or manually by a user…'.

[55] Para 3(4) PD SL1.2.

[56] But attachments should immediately follow their parent document even where the date of the attachment differs from that of the parent document.

[57] Para 26 PD SL1.2.

[58] Under Order 24, rules 7 or 15A RHC See Para 21 PD SL1.2.

[59] Defined in PD SL1.2 as 'a software-aided search for words across the text of an Electronic Document'. Para 3(6) PD SL1.2.

[60] Defined in PD SL1.2 as 'a technological tool or method that uses sophisticated statistical and linguistic models to understand the meaning behind search terms by identifying word patterns and occurrences in Electronic Documents which are then translated into concepts to be used to search information stored electronically which matches the translated concepts'. Para 3(1) PD SL1.2.

[61] Defined in PD SL1.2 as 'the process of checking data by identifying and checking representative individual Electronic Documents.' Para 3(2) PD SL1.2.

[62] Footnote to Para 9(3), paras 22, 23, 24 PD SL1.2.

b. Confining the discovery of electronic documents or certain categories of electronic documents to specific date ranges, custodians, locations, categories or types.[63]

c. Methods of identifying duplicate electronic documents.

d. Dividing the discovery process (what PD SL1.2 calls a 'staged approach') with discovery first being limited to specific categories of documents with the categories subsequently broadened or limited depending on the results initially obtained. Where electronic documents are best viewed using technology not readily available to the party entitled to discovery, and that party reasonably requires additional access facilities, PD SL1.2 specifies that the party making discovery shall co-operate in making available to the other party such reasonable additional facilities to obtain access to those electronic documents.[64]

5. Methods used to:

a. Identify privileged and other non-discoverable electronic documents,

b. Redact electronic documents where appropriate,[65] and

c. Deal with privileged or other documents, which have been inadvertently disclosed.[66]

6. The preservation of electronic documents particularly to prevent their loss prior to trial.

7. The formats in which electronic documents are to be provided and the methods to be employed. The parties may agree, or be required by the court, to convert the electronic documents into file formats recognised by the computer or audio visual facilities available in court.[67]

8. The basis of charging for or sharing costs regarding the provision of electronic files and whether such arrangements are final or are subject to re-allocation in accordance with any subsequent order for costs.

9. Whether paper documents should be scanned for discovery and the format in which these scanned documents should be exchanged (e.g. as a text-searchable .pdf document) and

10. Agreement on the exchange of data in an electronic format using agreed fields.[68]

Court interventions

Parties failing to reach an agreement regarding the discovery of electronic documents should seek directions from the court at the earliest practical date.[69] Should a party give discovery of electronic documents without prior discussion with the other parties as to how to plan and manage such discovery, the court may require that that party conduct further searches, repeat any steps it has carried out and may further consider making a wasted costs order.[70]

The court can also provide direction in relation to discovery on its own, or on application by a party if it considers that the parties' agreement in relation to the discovery of electronic documents to be inappropriate or insufficient. A court can further order that the parties complete and exchange a revised and updated EDDQ, including providing answers to any additional questions that arise, within 14 days or such other period as the court may direct.[71]

Preservation and other obligations

Parties' legal representatives must notify their respective clients of their preservation obligations (for

[63] Para 19 PD SL1.2 states: Depending on the circumstances, it may be reasonable to search all of the parties' electronic storage systems, or to search only part of those systems. For example, it may be reasonable to decide not to search for electronic documents which came into existence before a particular date, or to limit the search to electronic documents in a particular place or places, or to electronic documents falling into particular categories.

[64] As may be appropriate in accordance with Order 24, rule 15A of the RHC. See Para 31 PD SL1.2.

[65] If a party wishes to redact or make alterations to an electronic document or documents, that party must inform the other party that redacted or altered versions are being supplied and must ensure that the original un-redacted and unaltered version is preserved, so that it remains available if required. However, this does not apply where the only alteration made to the document is an alteration to the Metadata as a result of the ordinary process of copying or obtaining access to the document. Para 30 PD SL1.2.

[66] Parties are encouraged to enter into 'claw back' agreements setting out detailed protocols to deal with the inadvertent disclosure of electronic documents and to provide details of any such agreement to the court as part of the Information Sheet for the first CMC. Footnote 3 PD SL1.2.

[67] Para 33 PD SL1.2.

[68] Paras 8, 9, 20 PD SL1.2.

[69] Para 10 PD SL1.2.

[70] Para 12 PD SL1.2.

[71] Para 11 PD SL1.2.

instance, that discoverable documents, including electronic files that might be deleted either in accordance with a document retention policy or in the ordinary course of business, must be preserved[72]) as soon as litigation is contemplated and advise them to issue appropriate instructions to employees or any other custodians. Legal representatives should also advise clients of the need to maintain a well-organized and readily searchable system and filing management of electronic documents for the purposes of discovery.[73]

Electronic documents need to be preserved in their in the original form in which the electronic documents were created by a computer software program (i.e. their native formats),[74] in a manner which preserves the associated metadata such as the date of creation of each electronic document,[75] even if those same documents are later disclosed in another format.[76] But where the court has directed, or the parties have agreed not to provide the electronic documents in their native format, the parties should provide searchable optical character recognition (OCR)[77] versions of the disclosed electronic documents, unless there is a good reason not to do so.[78]

Where a party requests the discovery of metadata or forensic image copies of electronic documents that are disclosed, the party making the request must demonstrate the relevance and materiality of the requested metadata and justify the cost and burden of producing it.[79]

Electronic documents disclosed in another format should be rendered in such a way as to include any pertinent information (for instance, 'track changes', 'comments and mark-up', 'speakers notes', 'hidden rows', 'hidden columns', 'hidden worksheets', etc.) and information should be rendered in colour where colour is present and material to the comprehension of the content.[80] Furthermore, where the court has directed, or the parties have agreed not to provide the electronic documents in their native format, the parties should provide searchable optical character recognition (OCR)[81] versions of the disclosed electronic documents, unless there is a good reason not to do so.[82]

Application of PD SL 1.2 [Heading type C]

The principles of PD SL 1.2 were applied in *Chinacast Education Corporation and Others v. Chan Tze Ngon and Others,*[83] where the court noted that when parties make e-discovery applications courts must bear certain principles in mind to ensure, *among other things*, that discovery is not oppressive, depends on issues at trial and that a party failing to cooperate with the other side and to comply with court orders for discovery or carry out de-duplication of copies may need to bear extra costs.[84]

Civil proceedings

As the rules for production of electronic evidence are much more relaxed in civil proceedings than for criminal proceedings, a court, subject to relevance, will more readily accept an item of electronic evidence submitted by consent in a civil, as opposed to a criminal, case.

Business records

Under s 54, EO, the records of a business or public body are admissible in civil proceedings without further proof, provided there is a computer certificate signed by an officer of that business or public body.[85] For the purpose of this section, 'records' include computer-generated records and an 'officer' includes

[72] Para 7 PD SL1.2.
[73] That is, to ensure that potentially relevant electronic documents, which might otherwise be deleted in the ordinary course of business or under a document retention policy, are preserved until the final determination of the litigation. Sch. 1 Para 7 PD SL1.2.
[74] Para 3(8) PD SL1.2.
[75] Para 27 PD SL1.2.
[76] Para 7 PD SL1.2.
[77] PD SL1.2 defines Optical Character Recognition (OCR) as 'the computer-facilitated recognition of printed or written text characters in an electronic image in which the contents cannot otherwise be searched electronically. See: Para 1(9) PD SL1.2. Except in the case of redacted information, parties should not unnecessarily alter the OCR text, which they maintain within their system at the time of production or discovery. A party should ensure that the OCR of a redacted section of a document is not provided, but that the OCR of the remainder of the document is provided. Footnotes 10,12 PD SL1.2.
[78] Para 29 PD SL1.2.
[79] Para 25 PD SL1.2.
[80] Para 28 PD SL1.2.
[81] PD SL1.2 defines Optical Character Recognition (OCR) as 'the computer-facilitated recognition of printed or written text characters in an electronic image in which the contents cannot otherwise be searched electronically. See: Para 1(9) PD SL1.2. Except in the case of redacted information, parties should not unnecessarily alter the OCR text, which they maintain within their system at the time of production or discovery. A party should ensure that the OCR of a redacted section of a document is not provided, but that the OCR of the remainder of the document is provided. Footnotes 10,12 PD SL1.2.
[82] Para 29 PD SL1.2.
[83] Although PD SL 1.2 was not been in operation as of the date of the trial, the Court chose to make reference to the guidelines as set out in the Practice Direction. [2014] HKCFI 148 at Para 10
[84] [2014] HKCFI 1489; at Paras 10, 28
[85] Evidence Ordinance, s 54(1) and (2).

any person occupying a responsible position in relation to the relevant activities of the business or public body or in relation to its records.[86] For instance, if the record is concerns employees' personal details, then a member of staff of the Human Resources Department can sign the certificate.

Records are admissible under s 54, EO, but under s 54(5), EO, the court may, having regard to the circumstances of the case, direct that all or any of the provisions of this section do not apply in relation to a particular document or record. In *Preamble Properties Finance Limited v Italian Motors (Sales and Service) Limited & another*,[87] the plaintiff, in proving its losses arising from loss of use of a car, put forward a number of documents. Defence counsel argued for the application of s 54(5), because there were numerous discrepancies on the documents about the age of the car and the amount of losses involved. The judge agreed to the defence submissions, treated the documents as hearsay documents (not records), and applied the criteria in s 49 EO in assessing their weight.[88] Although the documents in the *Preamble* were physical ones, there is no reason why the principles should not apply to computer-generated records.

Weight

As previously noted, computer-generated documents may or may not be hearsay in nature. If they are records of business, then s 54, EO applies and the contents will be admitted without further proof. No question of weight arises in respect of the document itself. To challenge the weight of such business records requires the submission of other evidence. However, if the documents are not business records, then s 49 EO applies with regards to the question of their weight.

In assessing the weight given to hearsay evidence, a court will consider '…any circumstances from which any inference can be reasonably drawing as to the reliability or otherwise of the evidence…'[89] including whether: it was reasonable and practical for the party by whom the evidence was adduced to have produced the maker of the original statement as a witness; the original statement had been made contemporaneously with the existence or occurrence of the matters stated; multiple hearsay was involved; any person involved had any motive to conceal or misrepresent matters; the original statement was an edited account or was made in collaboration with another or for a particular purpose; the circumstances in which the evidence is adduced as hearsay are such as to suggest an attempt to prevent proper evaluation of its weight; and the evidence adduced by the party is or is not consistent with any evidence previously adduced by the party.[90]

In estimating the weight of electronic evidence, all these factors can be considered to be 'common sense', yet with many computer-generated documents it is difficult, if not impossible, to identify the maker of the original statement and as such the maker cannot be called. Much therefore will depend on the nature of the document and the number of people that can be identified as being associated with the making of the document.

Criminal proceedings

Pre trial

Search and seizure

The search and seizure of persons in a public place by police officers is governed by s 54 of the Police Force Ordinance, Cap 232 ('PFO'). Under the provisions of art 14 of the Hong Kong Bill of Rights,[91] which is itself identical to the terms of art 17 of the International Covenant of Civil and Political Rights ('ICCPR'),[92] officers of law enforcement agencies are not allowed to search private premises unless armed with a search warrant. Article 14 of the Hong Kong Bill of Rights reads as follows:

> '(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.'

Search warrants

If persons have committed a crime using digital devices in some manner, the acquisition of electronic

[86] Evidence Ordinance, s 54(4).
[87] [2003] HKCFI 255, HCA2135/2000 (25 July 2003).
[88] HCA 2135/2000 at [38].
[89] Evidence Ordinance, s 49(1).
[90] Evidence Ordinance, s 49(2).
[91] Under s 8 of the Hong Kong Bill of Rights Ordinance, Cap 383.
[92] Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976 in accordance with art 49, ICCPR.

evidence will be required to support prosecution. Under ss 103 and 104 of the Criminal Procedure Ordinance, Cap 221, a search warrant can be obtained by law enforcement personnel by laying information on oath to satisfy a magistrate or a judge to seize any instruments, materials or things which there is reason to believe are provided or prepared, or being prepared, with a view to the commission of any indictable offence.[93]

External serious offence

Where there are reasonable grounds to believe that a thing relevant to the criminal matter involving an external serious offence[94] is located in Hong Kong, an appropriate authority of the relevant place may make a request to the Secretary for Justice to arrange for a search warrant in relation to the thing. An officer, nominated by the Secretary for Justice, can apply to a magistrate for a search in relation to that thing by laying information on oath before the magistrate, setting out the grounds for his reasons for believing that the thing in question is or will be in the possession or control of a person or upon any land or upon or in any premises at a specific time.[95]

Surveillance

Police officers have general powers to undertake surveillance by following a person in a public place, to take photographs and videos and intercept electronic communications.

The Interception of Communications and Surveillance Ordinance, Cap 589 (the 'ICSO') came into operation on 9 August 2006. The ICSO governs covert surveillance by four law enforcement agencies: the Customs and Excise Department, the Hong Kong Police, the Immigration Department and the Independent Commission Against Corruption and Ordinance. The interception of any communication in the course of postal or telecommunications systems[96] is illegal unless the interception is authorised[97] by a judge appointed by the Chief Executive of Hong Kong under the ICSO. A code of practice, issued by the Secretary for Security, sets forth relevant guidelines.[98] The Commissioner on Interception of Communication and Surveillance has produced annual reports from 2006 to 2010, setting out the number of applications for authorisations that year, the problems that arose in the surveillance, the extent of compliance by the law enforcement agencies and recommendations for improvement.[99]

The admissibility of evidence under s 61(1) ICSO[100] was challenged in *Ho Man Kong v Superintendent of Lai Chi Kok Reception Centre*,[101] which involved the admissibility of telephone recordings in respect of offences allegedly committed by the applicant that had been gathered by Australian authorities. The court upheld the admissibility of the recorded evidence on the basis that that the telephone recordings did not fall within the definition of 'telecommunications interception product', and therefore were not caught by the provisions of s 61(1).

In *HKSAR v Muhammad Riaz Khan*,[102] the Court of Final Appeal, rejected the appellant's contention that a secret recording of a conversation by law enforcement officials made before the enactment of the ICSO violated the appellant's constitutional right to privacy and that its use at the trial was an error of law for which his conviction ought to be quashed. The court also noted that at the time when the recording was made, there was no sufficient legal framework in place for the interception of communications and surveillance, but since then the ICSO has supplied the necessary framework and that a recording such as the one made could now be authorised under the ICSO.

Records admitted under s 22A, EO

Section 22A, EO provides two avenues for the admissibility[103] of records from a computer in criminal

[93] This is the general power to apply for search warrants. Other provisions that cater for application of a search warrant in particular circumstances, such as in connection with an offence of incitement to disaffection under s 7 of the Crimes Ordinance, Cap 200, or in connection with corruption under s 10B of the Independent Commission Against Corruption Ordinance, will not be discussed here.

[94] An external serious offence means an offence against a law of a place outside Hong Kong, the maximum penalty for which is death, or imprisonment for not less than 24 months: Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525, s 2.

[95] Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525, s 12.

[96] *Interception of Communications and Surveillance Ordinance Code of Practice,* Pursuant to Section 63 of the Interception of Communications and Surveillance Ordinance, available at http://www.sb.gov.hk/eng/special/pdfs/cop_e.pdf.

[97] Interception of Communications and Surveillance Ordinance, s 5.

[98] Interception of Communications and Surveillance Ordinance, s 4.

[99] For which, see http://www.info.gov.hk/info/sciocs/en/index.htm.

[100] The Interception of Communications and Surveillance Ordinance, s 61(1) states:
'(1) Any telecommunications interception product shall not be admissible in evidence in any proceedings before any court other than to prove that a relevant offence has been committed.'

[101] [2011] HKCFI 502, HCAL17/2011 (28 July 2011).

[102] [2012] HKCFA 38, FACCI13/2010 (22 May 2012).

[103] Under the Evidence Ordinance, s 22A(1) or s 22A(3).

proceedings as *prima facie* evidence of a fact stated in the record: evidence may be adduced, either orally or by consent; or records stored in computers may be produced in the form of a computer certificate.[104] Whether a combination of computers are used, or different computers are used in succession or a combination of computers are used in succession, all are treated as a single computer for the purposes of s 22A, EO.[105]

Evidence adduced orally or by consent [Heading Type C]

Where direct oral evidence of a fact is admissible,[106] evidence may be adduced, either orally or by consent, under the provisions of s 22A(1):

> '(a) that the computer in question was used to store, process or retrieve information for the purposes of any activities carried on by any body or individual;
>
> (b) that the information contained in the statement reproduces or is derived from information supplied to the computer in the course of those activities; and
>
> (c) that while the computer was so used in the course of those activities:
>
> (i) appropriate measures were in force for preventing unauthorised interference with the computer; and
>
> (ii) the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.'

To a large extent, this requires the oral evidence of a witness testifying on the above conditions unless the defence agrees to such evidence or evidence is produced in the form of a computer certificate, for which see below.

With respect to section 22A(2)(c)(i), EO, questions may arise as to what constitutes 'appropriate measures' for the prevention of unauthorised interference. This point has not yet been addressed by Hong Kong courts, although it is submitted that login names and passwords or the installation of some form of antivirus software may suffice in this context.

Section 22A(2)(ii), EO provides for the situation where the computer was not functioning properly in some non-material aspect. Providing the data in question had been backed up, it is unlikely that any malfunction will affect the accuracy of the records. Where information supplied to the computer was done without human intervention or in any appropriate form, it is treated as information supplied to the computer within the meaning s 22A, EO.[107]

Four important points emerge from the provision of s 22A(3), EO.

First, s 22A(3)(b), EO covers the situation where the computer was only operated by the accused, where they are a person occupying a responsible position in relation to the operation of the computer. The inclusion of the phrase 'other than a person charged with an offence to which such statement relates', prevents s 22A(3), EO from being rendered otiose for a computer seized from an accused person operating a business as a sole proprietor.

Second, s 22A(3)(c), EO mandates that the document be produced by a person 'having practical knowledge of and experience in the use of computers as a means of storing, processing or retrieving information', but does not require this person to have knowledge and experience in the use of the particular computer in question; knowledge and experience of computers as a means of storing, processing or retrieving information, in general, is deemed to be sufficient. In practice, such a person is usually a police officer of the Hong Kong Police who has attended seminars and training in computer forensics. The capacity of such police officers in producing a document from a computer in question has not yet been challenged in the courts of Hong Kong.

Third, to avoid an accused making use of this subsection to render admissible an otherwise inadmissible piece of self-serving evidence, s 22A(3)(d), EO prohibits an accused from making use of s 22A(3), EO to produce a document from a computer to prove a statement in the document as part of the defence case.

Finally, the conditions precedent are that direct oral evidence of that fact is admissible in the proceedings,[108] and that the computer had been operating properly at the material time or, if not, any respect in which the computer was not operating

[104] Evidence Ordinance, ss 22A(5).
[105] Evidence Ordinance, ss 22A(4).
[106] Evidence Ordinance, s 22A(1)(a).
[107] Evidence Ordinance, s 22A(9)(a).
[108] Evidence Ordinance, s 22A(3)(a).

properly or not at all neither affected the production of the document nor the accuracy of its contents.[109]

Production of records in the form of a certificate
Records stored on computers may also be produced in the form of a computer certificate.[110] This only requires a document to be produced from a computer, together with a signed certificate, for which see below, and does not require a witness. Section 22A(5), EO dispenses with the need for the 'person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities' to testify in court provided that he signs a certificate, generally known as a 'computer certificate', that:

> (a) identifies the document containing the statement and describing the manner in which it was produced, and explaining the nature and contents of the document. This document is usually annexed to the computer certificate;
>
> (b) gives the particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer. Basically, this involves identifying a cloned hard disk, a computer and a printer;
>
> (c) deals with matters about appropriate measures that were in force to prevent unauthorised access to the computer and that the computer was at the material times operating properly (matters in subsection (2));
>
> (d) purports to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities In practical terms, it is typically signed by the police officer who handled the hard disk, computer and printer[111].

Prerequisites
Such a document *is prima facie* evidence of any fact stated within the document if it is shown, in accordance with the provisions of s 22A(3), EO, that:

> '(a) direct oral evidence of that fact would be admissible in those proceedings;
>
> (b) it is shown that no person (other than a person charged with an offence to which the statement relates) who occupied a responsible position during that period in relation to the operation of the computer or the management of the relevant activities-
>
> (i) can be found; or
>
> (ii) if such a person is found, is willing and able to give evidence relating to the operation of the computer during that period;
>
> (c) the document was so produced under the direction of a person having practical knowledge of and experience in the use of computers as a means of storing, processing or retrieving information; and
>
> (d) at the time that the document was so produced the computer was operating properly or, if not, any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents,
>
> but a statement contained in any such document which is tendered in evidence in criminal proceedings by or on behalf of any person charged with an offence to which such statement relates shall not be admissible under this subsection if that person occupied a responsible position during that period in relation to the operation of the computer or the management of the relevant activities.'

The conditions precedent are that direct oral evidence of that fact is admissible in the proceedings, and the computer had been operating properly at the material time or, if not, any respect in which the computer was not operating properly or not at all it neither affected the production of the document nor the accuracy of its contents.

Certificates
The person signing the certificate only need state the matter to the best of his knowledge and belief in the computer certificate. The computer certificate will then be prima facie evidence of the statement. Unless the person cannot be found or if found is not willing and able to testify (as in subsection (3)), the court may require the person who made the computer

[109] Evidence Ordinance, s 22A(3)(d).
[110] Evidence Ordinance, s 22A(3).
[111] Evidence Ordinance, s 22A(5).

certificate to attend court and give oral evidence on any of the matters referred to in s 22A(5), EO.[112]

Unless the opposite party does not take issue on time, the computer certificate must be served on the opposite party 14 days before the commencement of the trial.[113] The production of a copy, if the original is not available, is permissible.[114] Note that the definition of 'certificate' for purposes of s 22A(5), EO differs from and should not be confused with the definition of 'certificate' given in s 2, ETO:

> '(a) is issued by a certification authority for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;
>
> (b) identifies the certification authority issuing it;
>
> (c) names or identifies the person to whom it is issued;
>
> (d) contains the public key of the person to whom it is issued; and
>
> (e) is signed by the certification authority issuing it…'

Also note that for computer print-outs, the term 'original' can misleading, because the computer could, for instance, instruct a laser or ink jet printer to print out multiple copies of a screen image, all of which could be considered 'originals' in the sense that the printer has printed a new (ie 'original') reproduction of the display in a physical format.

Records tendered for purposes other than to prove the truth of a statement

The purpose of s 22A, EO is to prove a statement contained in a document produced by a computer. Where a computer record is tendered for a purpose other than to prove the truth of the statement contained in the document, there is no need to strictly follow the requirements of s 22A, EO. In *Secretary for Justice v Lui Kin Hong, Jerry*,[115] the Hong Kong Court of Final Appeal stressed that the failure to comply with the provisions of s 22A, EO will only affect the admissibility of the computer-generated records if the purpose of tendering the document is to prove the truth of the contents in the document. If the computer-generated document is tendered for a purpose other than proving the truth of its contents, then the requirements under s 22A, EO need not be complied with.

One such instance where a computer record is not tendered to prove the truth of the statement contained in the document is a situation in which a computer record is produced to prove that something did not occur.[116] This can be achieved by proving that a system had been followed under which a person, acting under a duty, compiled a record of the occurrence of all events of that description. Evidence that there is no record of the occurrence of the event in question would be admitted as prima facie evidence to prove that the event did not happen.[117] For example, in proving that an accused did not pay for goods, a member of staff may give evidence about the payment system; for instance that cashiers scan the barcodes on individual items during checkout and that the payment details are recorded on a computer. This, taken together with absence of a payment record in the computer records for the items found in the accused's possession at the material time, will be *prima facie* evidence that the accused did not pay for the goods.

Weight

In considering the weight to be attached to a computer record admitted under s 22A, EO in a criminal trial, the court shall have regard to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement.[118] In particular, consideration is to be given as to whether or not the information contained in the statement was recorded or supplied to the computer contemporaneously with the occurrence or existence of the facts dealt with in that information; and whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.[119]

[112] Evidence Ordinance, s 22A(7).
[113] Evidence Ordinance, s 22A(6).
[114] Evidence Ordinance, s 22B(1).
[115] FACC 3/1999, (1999) 2 HKCFAR 510, [2000] 1 HKLRD 512, [2000] 1 HKC 95.
[116] See Evidence Ordinance, s 17A.
[117] Evidence Ordinance, s 17A(1).
[118] This point is discussed in *Secretary for Justice v Lui Kin Hong* FACC 3/1999, (1999) 2 HKCFAR 510, [2000] 1 HKLRD 512, [2000] 1 HKC 95.
[119] Evidence Ordinance, s 22B(3)(b).

Evidence by way of live television link or video recording

Part IIIA of the Criminal Procedures Ordinance, Cap 221 (the 'CPO') provides procedures to call evidence by way of a live television link, under s 79B, CPO, where the witness is a child,[120] mentally handicapped,[121] a vulnerable witness, or in fear.[122] It also covers procedures to call evidence by way of a video recording, under s 79C CPO, for witnesses who are either children or mentally handicapped. In 2002, the government produced a consultation paper[123] seeking comments on a proposal to provide for the giving of evidence by witnesses in criminal proceedings via a live television link between Hong Kong and overseas jurisdictions. This was followed by the Evidence (Miscellaneous Amendments) Ordinance, which had provisions for the use of live television links in criminal proceedings and the taking of evidence from witnesses outside Hong Kong via a live television link.[124] However, as of the time of writing, these provisions have not come into effect.

Discovery

Obligations of defence to disclose

Except for the defence of alibi for trial on indictment[125] or reliance on defence expert reports, there is generally no obligation on the defence to disclose its defence prior to trial. Section 65DA, CPO reads:

> '(1) Following the committal of any person or the transfer of any charge or proceedings or action or matter for trial in the court, or the making of an order for the retrial of any person in the court, if any party to the proceedings proposes to adduce expert evidence (whether of fact or opinion) in the proceedings (otherwise than in relation to sentence) he shall as soon as practicable, unless in relation to the evidence in question he has already done so-
>
> (a) furnish the other party or parties with a statement in writing of any finding or opinion which he proposes to adduce by way of such evidence; and
>
> (b) where a request in writing is made to him in that behalf by any other party, provide that party also with a copy of (or if it appears to the party proposing to adduce the evidence to be more practicable, a reasonable opportunity to examine) the record of any observation, test, calculation or other procedure on which such finding or opinion is based and any document or other thing or substance in respect of which any such procedure had been carried out.
>
> (2) A party may by notice in writing waive his right to be furnished with any of the matters mentioned in subsection (1) and, in particular, may agree that the statement mentioned in subsection (1)(a) may be furnished to him orally and not in writing.
>
> (3) If a party has reasonable grounds for believing that the disclosure of any evidence in compliance with the requirements imposed by subsection (1) might lead to the intimidation, or attempted intimidation, of any person on whose evidence he intends to rely in the proceedings, or otherwise to the course of

[120] Defined in s 79A, CPO as a person under 17 years of age in the case of an offence of sexual abuse or under 14 in other cases.
[121] A person who is mentally disordered or mentally handicapped, as the case may be, within the meaning of the Mental Health Ordinance, Cap 136).
[122] Section 79B CPO defines a 'witness in fear' as a 'witness whom the court hearing the evidence is satisfied, on reasonable grounds, is apprehensive as to the safety of himself or any member of his family if he gives evidence.'
[123] Consultation Paper: Evidence (Miscellaneous Provisions) Bill, Examination of overseas witnesses via live TV link (March 2002).
[124] These were contained in Part II, Evidence (Miscellaneous Amendments) Ordinance which, when it comes into effect, will amend or add new provisions to the EO and CPO.
[125] Criminal Procedure Ordinance, s 65D; District Court Ordinance, s 75A.

justice being interfered with, he shall not be obliged to comply with those requirements in relation to that evidence.

(4) Where, in accordance with subsection (3), a party considers that he is not obliged to comply with the requirements imposed by subsection (1) with regard to any evidence in relation to any other party, he shall give notice in writing to that party to the effect that the evidence is being withheld and the grounds therefor.

(5) A party who seeks to adduce expert evidence in any proceedings and who fails to comply with subsection (1) shall not adduce that evidence in those proceedings without the leave of the court.

(6) This section shall not have effect in relation to any proceedings in which a person has been committed for trial or ordered to be retried, or in which any charge or proceedings or action or matter has been transferred, before the date on which this section comes into force.

(7) In subsection (1), "document" includes, in addition to a document in writing-

> (a) any map, plan, graph or drawing;
>
> (b) any photograph;
>
> (c) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and
>
> (d) any film (including microfilm), negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom.'

There are two important points to note. First, there is no fixed prescribed period for disclosure of expert reports; the requirement is that the party intending to adduce the report has to serve the expert report on the other side 'as soon as practicable'. This is in contrast to the defence of alibi, where the alibi must be given at least ten days prior to the commencement of the trial. Where a party has failed to serve the report on the other side in time, an application may be made under s 65DA(5) CPO for leave of the court to adduce the expert evidence.[126] Second, this section only applies to trials in the District Court and the Court of First Instance; thus a party is under no obligation to make advance disclosure of expert reports for proceedings in the magistrates' courts.

Obligations of the prosecution to make disclosure

The prosecution is under a duty to disclose to the defence all materials in its possession or in the possession of the law enforcement agencies or materials of which it becomes aware that are or may be relevant to the guilt or innocence of the accused. This obligation recognises the right of an accused to have a fair trial – a right guaranteed by art 10 of the Hong Kong Bill of Rights, which itself is equivalent to art 14, ICCPR. The prosecution's obligation to disclose extends to material which is (a) relevant or possibly relevant to an issue in the case; (b) raises or possibly raises an issue, the existence of which is not apparent from the evidence which the prosecution intends to rely on at trial, and has a real, as opposed to fanciful, prospect of leading on evidence which goes to (a) or (b). The prosecution's duty to disclose relevant matters is a continuous one and the disclosure must be made in a timely manner. Failure to comply with this duty may lead to a conviction being quashed.[127]

Discovery of digital evidence

The prosecution provides to the defence hardcopies, for example, copies of documents printed from the computer of the defendant, and a cloned copy of the

[126] *HKSAR v Lee Chi Fai & others* CACC 99/2002 (21 July 2003).
[127] *Brian Alfred Hall v HKSAR* [2009] HKCFA 65, (2009) 12 HKCFAR 562, FACC 12/2008 (8 July 2009); see also *HKSAR v Lee Ming Tee* [2003] HKCFA 34, (2003) 6 HKCFAR 336, [2004] 1 HKLRD 513, FACC1/2003 (22 August 2003).

hard disk of the defendant's computer to the defendant. In practice, when police seize a computer from an accused, they will make at least two cloned copies of the hard disk. One cloned copy will be used as a working copy. The other will be disclosed to the defendant, thereby enabling the defendant to engage his own expert to carry out tests for the purposes of, for example, searching for malicious software to support a defence's case theory that the defendant's computer might have been hacked into as it contained malicious software.

Authentication

The normal rules of authentication apply; that is, the prosecution is required to prove that the hardcopy of the document or image that was printed out came from the cloned working copy of the defendant's computer. This is typically proven by direct oral evidence of the officer in question. Evidence that the cloned working copy has exactly the same contents will also have to be adduced. In practice, the evidence in this area is seldom challenged in Hong Kong.

Evidence from other jurisdictions

If an overseas witness is unwilling or, for other reasons, unable to travel to Hong Kong to testify, then an application under s 77E EO can be made to the Court of First Instance for a letter of request to a court or tribunal exercising jurisdiction in a place outside Hong Kong to assist in obtaining evidence for the purposes of the criminal proceedings instituted in Hong Kong. The depositions and documents exhibited or annexed to any application received by the Registrar of the High Court pursuant to the Letter of Request shall, on its production without further proof, be prima facie evidence of the fact stated in the deposition as well as in the documents exhibited to the application[128] if both the prosecution and the defence agree to the production of the deposition; or the document attached to the deposition satisfies the usual conditions for business records or computer records.[129]

The provisions for the use of live television links in criminal proceedings and the taking of evidence from witnesses outside Hong Kong via a live television link in the Evidence (Miscellaneous Amendments) Ordinance have yet to come into effect.

Dealing with documents at the end of proceedings

At the conclusion of proceedings, the prosecution are required to apply to have exhibits (including documents produced at trial) disposed of in accordance with s 102, CPO. Under s 102, CPO, the property will be returned to its owner or the defendant; where the owner cannot be found or is unknown, a court may make an order that the property be sold, retained in the possession of the court, the police or the Customs and Excise Service, or destroyed if the property has no value. Documents produced at trial will usually be ordered to be retained in the court's file. However, the prosecution may, with the leave of court, replace an original document with a copy in the court's file where an original document was produced and has to be returned to its owner.

Mr Ronald Yu is a member of the Board of directors of IIPCC.org, a WIPO Permanent Observer. He is a U.S. Patent Agent and a digital forensics examiner. He has taught classes on or published articles, books, and blog posts on electronic evidence, digital forensics, artificial intelligence, information technology, copyright, patent and constitutional law.

http://www.iipcc.org

[128] Evidence Ordinance, s 77F.
[129] Evidence Ordinance, s 77F(2).