International Conference on Electronic Litigation

International Conference on ELECTRONIC LITIGATION

Editor-in-Chief

Justice Lee Seiu Kin

General Editor

Yeong Zee Kin

Academy Publishing

Academy Publishing is a division of the Singapore Academy of Law ("the Academy"). The Academy is the umbrella membership body of the legal community in Singapore. The Academy's activities are driven by three strategic priorities – enhancing legal knowledge, improving efficiency of legal practice through the use of technology and supporting the legal industry. The work in each of these areas is directed towards raising the standards and quality of legal practice and building a strong legal community. For more information, visit www.sal.org.sg.

The General Editor
c/o Singapore Academy of Law
1 Supreme Court Lane
Level 6
Singapore 178879
Tel No: +65 6332 4388
Fax No: +65 6334 4940
E-mail: publications@sal.org.sg

ISBN 978-981-07-2788-8

Editors

Germaine Boey

Jurena Chan

Monica Chong

Jerald Foo

Joshua Lim

Rajaram Vikram Raja

Colin Seow

Eugene Sng

Jonathan Yap

Justin Yeo

PREFACE

1 The Singapore Academy of Law's inaugural International Conference on Electronic Litigation 2011 was held on 11 and 12 August 2011. We were privileged to host over 350 participants and speakers, comprising a fair mix of practitioners and in-house counsel, judges and arbitrators, litigation technology managers and specialist service providers. Almost a quarter of the delegates came from more than 30 foreign jurisdictions, embracing all major legal systems of the world. Participants hailed from the region – Malaysia, Brunei, Hong Kong and China, Japan, Korea, Australia and New Zealand – as well as jurisdictions further afield – Namibia, Mauritius, Russia and Azerbaijan.

2 As noted by the Chief Justice of Singapore in his Opening Address, "electronic litigation is, essentially, the application of technology in the litigation process". With the pervasiveness of information technology in our modern society, the conference had much ground to cover. On the first day, Lord Justice Rupert Jackson addressed the issues and options for managing civil litigation at proportionate costs in his keynote speech. The rest of the day was followed by a mix of plenary and panel discussions on the increasingly pertinent issue of electronic discovery and the closely related issues pertaining to the preservation of electronic evidence.

3 The second day opened with Judge of Appeal Justice VK Rajah providing the conference with perspectives on the incorporation of technology in court advocacy gleaned from both his time at the Bar, where he was an eminent Senior Counsel, and his present experience on the Bench. The focus on the second day was on the legal and practical issues concerning the presentation of electronic and computer forensic evidence in court. The discussions had, of course, to include a consideration of the impact – both procedural and evidential – of the pervasive use of social media today on civil litigation.

4 Since the conclusion of the conference, the speakers and panellists were put to task to convert inchoate thoughts, sharpened during the panel discussions, into concrete ideas and articulating them in the papers for this conference publication. Our task was made all the more challenging both by the swift changes in the technological landscape, as well as a burst of legislation in the last quarter of 2011 and the first quarter of 2012. While we dare not claim that the discussions at the conference fomented the legislative awakening, the coincidence and close timing do suggest this possibility.

5 The Chief Justice had, in his Opening Address, spoke of his direction for a review of the law applicable to discovery. The Rules of Court Working Party completed its review and issued a public consultation, which took place over October and November 2011. Thereafter, the electronic discovery practice directions in Part IVA of the Supreme Court Practice Directions were amended in February 2012, taking effect from 1 March 2012. The amendments to the electronic discovery practice directions brought us one step further along the path towards a mandatory model. Certain categories of cases were identified where the application of Part IVA is to be considered more seriously than others. Clarifications were also introduced, particularly with respect to the court's powers to order the adoption of an electronic discovery plan either on application by a party or on its own motion. Similar clarifications were introduced to draw a distinction between the differences in treatment of inspection of databases and *forensic* inspection of recording devices and storage media.

6 New concepts were introduced: certain electronically stored documents are "not reasonably accessible" and these will only be discovered if they are sufficiently relevant and *material* such that the costs and burden of retrieving them are justified. The emphasis on balancing costs and relevance is perhaps the single thread that runs through the 2012 amendments to Part IVA. Another new introduction was the articulation of the hitherto tacit principle that underlies the list of factors that the court is required to consider: *viz*, that Part IVA was intended to provide "a framework for proportionate and economical discovery". One of the manifestation of this emphasis on costs is the introduction of a new optional framework for conducting discovery through the exchange of softcopies of discoverable documents (preferably in native format). This dispenses with the time-consuming and tedious effort of compiling a detailed list of documents in favour of an abridged list with meaningful

descriptions for each category or sub-category of documents in the optical disc or other mode of exchange. Under this optional framework, inspection is deferred and ordered only when necessary.

7 Concomitantly, the Ministry of Law issued a public consultation on proposed amendments to the Evidence Act over the months of September and October 2011. The amendments covered several areas: modernising hearsay exceptions and the clarification of legal privilege of in-house counsel's advice. But the most pertinent for our purposes was the abolition of our erstwhile section 35 in favour of presumptions that assist with the proof of authentication. The panellists that agitated for the removal of section 35 from our statute books during our conference panel on "Electronic Evidence in Singapore – Out with the Old, In with the New" were of course excited. That chapter had to be almost entirely re-written, but was a task undertaken with pleasure and enthusiasm by the authors. Hence, discussions on the challenges that section 35 posed to practitioners – and efforts to find practical ways around it – are now complemented by a consideration of the new presumptions and approaches taken when the Evidence (Amendment) Act – which was passed by Parliament in February 2012 and which received Presidential assent in March 2012 – takes effect, hopefully later this year. The new provisions are not without their issues and the chapter hopes to stimulate discussion and focus attention on some of the issues that are anticipated.

8 In the area of the impact of social media on civil litigation, there were developments that had to be added to the relevant chapter. On 14 December 2011, the Lord Chief Justice of England and Wales handed down a new practice guidance entitled "The Use of Live Text-Based Forms of Communication (including Twitter) from Court for the Purposes of Fair and Accurate Reporting". This permitted the use of live text-based instantaneous communications by law reporters in courtrooms. A consideration of the issues relating to "tweeting" in court had to be added to round off the discussion on the impact of social media in civil litigation.

9 It was therefore an eventful period following the conclusion of the conference. You now hold in your hands a conference publication that seeks to bridge the discussions at the conference and recent developments. It may be too much to wish that the discussions contained in this tome will tide us until the next conference, planned to be held in 2014. But in this exciting intersection of technology and law, the one thing that we can be assured of

is that when the conference next meets, some of the legal issues herein discussed will be outdated, some resolved and many more new issues will have been introduced by new technologies waiting in the wings.

LEE Seiu Kin
Judge
Supreme Court of Singapore
16 May 2012

CONTENTS

OPENING ADDRESS

CHAN Sek Keong
Chief Justice
Supreme Court of Singapore

I. INTRODUCTION

1 The pervasive use of information technology in developed and developing economies all over the world has generated great efficiencies and improvements in the way business is conducted, the way we work, and the way we live. Information in electronic form is ubiquitous in today's world. If you want to be modern you cannot escape the Net, nor would you want to once you are caught by it. Because of the free and easy manner in which communications are made through emails and word documents, information is being produced and transmitted on a massive scale every day, much more than print was ever able to do. This massive accumulation of information in digitised form creates tremendous obstacles in the way of regulators, litigants and lawyers, particularly when they are searching for relevant information for investigation, litigation and other purposes. This problem is felt most acutely in litigation under the common law system where the parties are required to give full discovery to their opponents before the trial of their disputes.

2 Electronic litigation occupies a field where litigation interfaces with information technology, and e-discovery is only one facet of electronic litigation. Electronic litigation has arrived in developed jurisdictions, and many developing jurisdictions are interested in its potential to improve efficiencies in their legal systems. Electronic litigation is, essentially, the application of technology in the litigation process, but for it to be functionally successful, the right technology must be used – otherwise we will end up with worse than electronic white elephants – better for show than purpose. In this address, I shall give a brief account of our experience in e-litigation over the last decade and highlight some of the key challenges ahead as we strive to strike an optimal balance between the temptation to use cutting edge information technology in the litigation process, and the need to ensure that access to justice is not hindered by excessive costs in litigation. Ultimately, the application of information technology to the processing of legal information and the litigation process is all about

efficiency and effectiveness of purpose, at the most economical cost. I will close by setting some directions which the Courts will take as we strive to attain this balance.

II. SINGAPORE'S EXPERIENCE WITH ELECTRONIC LITIGATION

3 Our courts, both the Supreme Court and the Subordinate Courts, have always adopted a practical approach towards integrating technology into the litigation process. Technology is never implemented for its own sake, or simply because it creates the impression of modernity, because to do so would be costly. Every piece of technology which we integrate into our court administration or the litigation process must achieve the desired purpose of achieving savings in the time or effort required to produce the outcomes that we want, in line with the key performance indicators based on the best practices of other developed jurisdictions. Our goal is simply to provide our legal profession and the courts with an efficient technological framework for legal research, managing cases, and conducting court trials and hearings. Among other things, these developments will reduce somewhat the inequality of arms between advocates in the large firms and those in the small firms. Also, they enhance access to justice for public institutions, private organisations and individuals through convenient and easy access to the court processes.

4 We began our e-litigation journey with the introduction of electronic filing in the late-1990s. Today, electronic filing is commonplace in many developed jurisdictions, and every judiciary in a developed or developing country can have it, if it so desires. Electronic filing is good to have, but it may not justify the costs for small jurisdictions which do not have a substantial volume of litigation. For us, the cost of implementing it was high, but it was necessary because we were already then a regional financial centre and we were aspiring to be an international business hub as well. Contrary to a common misconception, our initiative to introduce e-filing had nothing to do with clearing the backlog of cases, as by then the backlog had been successfully contained and our court processes to track the disposal of court cases had been fully computerised. E-filing was then a journey into unchartered territory for us, and we had to constantly remind ourselves not to develop a system that gave the edge to speed and efficiency over justice.

5 At the beginning, because the initiative came from the Courts, one of the biggest challenges was to change the mindset of the lawyers and their innate resistance to change. The legal profession had to be prodded into embracing change, even if it had to pay for it. In spite of frequent consultations with the Law Society, there were many teething problems. But, as the Borg in Star Trek are wont to say: "Resistance is futile". And change the Bar eventually did. Today, they are in the forefront of wanting more changes and more electronic services, as the profession adapts and legal practice evolves. So now we have a customised, effective and efficient end-to-end electronic filing system ("EFS") which is an essential component of our machinery of justice. EFS is a nationwide system (made easier because we are a small nation) and is mandatory. Parties must use EFS to file their claims, either through their lawyers or the service bureaux appointed by the Courts. EFS has effectively extended the Courts' working hours to 24 hours a day for every day of the year. Up to the end of May 2011, about 7.27 million documents have been filed and processed through the EFS in both the Supreme Court and the Subordinate Courts.

6 The introduction of technology did not stop at the threshold of the court house. We also, through the Singapore Academy of Law, ushered legal research into the Internet age by setting up LawNet – a one-stop practice portal providing a complete suite of information and transactional solutions for the Singapore and global legal community. LawNet comprises several modules for supporting legal practice. The cornerstone is its legal research module (called the Legal Workbench), other modules include due diligence searches for corporate information, litigation cases and property transfers. It is the authoritative source of legal information, with primary and secondary sources of law in Singapore and around the Commonwealth. LawNet is not free, not yet any way (because LawNet was developed by an outside agency which, although owned by the Government, has to recover its share of the cost of developing the system) but it is more than a legal database and is also much cheaper than the search services provided by commercial providers of legal databases.

7 Video conferencing for court hearings is another technology we have been using for some time in our five Technology Courts. Not surprisingly, because of Singapore's status as a business hub, video conferencing is used frequently, usually to take evidence of expert witnesses abroad, or where for some reason or other the witnesses did not wish to travel to Singapore. It is used daily in the criminal mentions courts in the Subordinate Courts. In

the Supreme Court, we use video conferencing for criminal pre-trial conferences, for bankruptcy hearings and in the Duty Registrar's chambers. Video conferencing is, of course, used to enable vulnerable witnesses, usually young victims of sexual offences, to give evidence from another room in the Supreme Court, away from the presence of the accused person.

III. FUTURE CHALLENGES

8 As I have said earlier, electronic filing is becoming common place nowadays. Our EFS is efficient by the current standard of information technology. But it is a paper-based system. It should be a paperless system. I attended a conference in Seoul, Korea in June 2011, and the Korean Judiciary very proudly showcased its electronic court system to over 30 Chief Justices from the Asia Pacific countries. Theirs is also a nationwide system, but given the geographical and demographic size of Korea, it is a much bigger and expensive system than ours.[1] Although we were not aware of what the Korean Judiciary has been doing, we have been working in the last few years on a replacement system called "eLitigation", or Integrated Electronic Litigation System. It promises greater efficiency by eliminating redundant steps in electronic filing. We will also be making use of modern e-form technology to automatically generate drafts of court orders and other documents.

9 Beyond electronic filing, we have embarked on our first steps to make better use of technology in our courtrooms so that hearings may be conducted more effectively. We have begun paperless hearings in the Court of Appeal so as to reduce the volume of paper generated for each appeal, and also to reduce the costs associated with making multiple sets of documents for use by the judges. It will take time to make the hearings more efficient as the retrieval and display of digitised information on the screens today is not done by counsel, but by a trained court clerk. When the parties or their counsel are able to do this, then the judges can simply sit

1 According to Chief Justice Lee Yong-hoon, it cost the government about US$98 million each year for 16 years from 1994 to develop their electronic court filing system. It was an astronomical sum compared with the size of the Korean Judiciary's past budgets, but he also said that the electronic registry system generated an estimated budget savings of approximately 6.4262 trillion Korean Won, equivalent to US$5.934 billion since its implementation ("The Judiciary in the Information Age: The Present State and the Future Direction", 13 June 2011 at the 14th Conference of Chief Justices of Asia and the Pacific).

back, listen, look at the screen, ponder and decide. No hearing can be more efficient than that.

10 But for court trials, we still need a working voice-recognition technology which can print out immediately (if needed) a transcript of what was said earlier in court to make our trials more efficient. We already have digital recording, but it is second best.

11 I now come to electronic discovery. Our lawyers and our courts have not had much experience in this area, but we have studied the literature on this area of work. We have issued a Practice Direction and our courts have issued four judgments on electronic discovery. Our procedural rules for discovery are fast becoming obsolete in the internet era. Lawyers familiar with the *Peruvian Guano* test (which requires the disclosure of any document which may fairly lead a person to a train of inquiry to advance his own case or to damage that of his adversary) will not operate efficiently in today's digital environment. We have not had a case of the magnitude of some of the cases in other jurisdictions, such as the UK, Australia or the USA. The current practice of listing documents for disclosure, the physical inspection of such documents and the making of copious paper copies is completely obsolete and out of place in today's digital environment.

12 Just to give everyone an idea of the sheer quantity of electronic documents being exchanged in litigation, as well as the costs involved, I need do no more than highlight 3 cases from the USA. The first was highlighted in a 4 March 2011 New York Times article entitled "Armies of Expensive Lawyers, Replaced by Cheaper Software".[2] It mentioned a case in 1978 involving a US Justice Department anti-trust lawsuit against CBS where the discovery proceedings produced 6 million documents which had to be examined by an army of lawyers and paralegals at a cost of more than US$2.2 million. The second case was also reported in the same New York Times article, and this case provides a marked contrast from the first case. In 2011, Blackstone Discovery of Palo Alto, California, was able to use e-discovery software to analyse 1.5 million documents for less than $100,000. The third is a case in 2005, where Ronald Perelman sued Morgan Stanley for fraud in connection with the sale of his company, Coleman Co. The court sanctioned Morgan Stanley for mishandling the emails: the jury drew an adverse inference against Morgan Stanley for destroying emails, and awarded Perelman US$1.57 billion in actual and

2 See <http://www.nytimes.com/2011/03/05/science/05legal.html>.

punitive damages, inclusive of interest. The damages award was set aside by the appellate court which found that Perelman had suffered no loss. Later, Morgan Stanley paid SEC $15 million to settle a claim that it had compromised investigations into IPOs and analysts' reports by destroying emails. Morgan Stanley was alleged to have destroyed at least 200,000 emails and falsely claimed that it had archived millions of others.

13 So, to sustain Singapore as a business hub we have no choice but to improve our electronic processes to meet this challenge of profusion of digital information, and also the easy destruction of such information. In this area, we can certainly learn a lot from the larger jurisdictions, such as the UK, Australia and USA, to ensure that e-discovery is effective in getting the material documents into court at an affordable price. This requires us to put in place a set of procedural rules that will balance the need to find the hidden truth – "the smoking gun" if you will – but not to discover everything that is discoverable, at an inordinate cost in time and expense. The formula which is currently applicable is to allow discovery necessary for "the *fair disposal of the matter* or for the saving of costs", but as everyone knows, the devil is in the details. We may also need to fashion evidential rules that give the courts more leeway in not drawing adverse inferences in cases where a party is unable to explain missing emails in a broken thread of emails. Destruction of evidence is an offence under the Penal Code, but this offence has seldom been prosecuted in our courts.

14 So, the challenges posed by modern technology have to be tackled at multiple levels with a multi-pronged strategy that straddles substantive and procedural law reform and upgrading of technological skills. The law on discovery requires review. I have tasked the Chairman of the Rules of Court Working Party to conduct a root and branch review of the law and practice of discovery and to consider recent reform initiatives in this area from various jurisdictions.[3]

15 While our Practice Directions for electronic discovery in 2009 have ensured that there are firm guidelines in place to help lawyers and litigants navigate through the complexities of preserving and producing electronically stored information for litigation, more can be done by outside

3 The review was completed and a public consultation conducted in October and November 2011. Thereafter, the electronic discovery practice directions in Part IVA of the Supreme Court Practice Directions were amended in February 2012. See discussion in "Electronic Discovery: An Evolution of Law and Practice", below at p 96.

experts to enable the profession to acquire more expertise in this area. If left to market forces, the legal profession may take too long to adopt the right technology and acquire the requisite skills.

16 Apart from this, we must also take bold steps to promote greater use of technology by the legal profession to practise law in today's technological environment. In recent years, a new industry of specialist electronic litigation service providers has developed to provide professional services like computer forensics and electronic discovery support. But for Singapore to maintain its status as a regional dispute resolution centre – whether for litigation or arbitration – we need more. Our lawyers and paralegals must also have the technical tools and skills to handle cross-border disputes involving large volumes of documents and in a cost-efficient manner. That is the lofty goal which I set for the Bar.

17 To buttress our legal industry's ability to handle disputes involving large volumes of electronic documents, the following areas have to be addressed. First, the legal profession needs access to an online electronic document review and exchange platform, ideally through LawNet. This will ensure that the legal profession has the requisite computing muscle on tap, and also to reduce the cost of using the platform. We see this to be yet another levelling of the playing field.

18 Second, training – not only of lawyers but also the paralegals and other litigation support professionals in law firms. As practitioners grapple with large-volume litigation, they are invariably backed up by a cadre of silent but steady paralegals. These stalwarts cannot be ignored as the Bar re-tools for litigation in the modern age. Equal attention will have to be paid to updating lawyers on the law and technology, and providing paralegals with upgraded skills to operate the new tools to manage large volumes of electronic documents that they are often called upon to harness.

19 Finally, we cannot ignore lawyers' working processes when they interact with their clients. In our early steps in the area of electronic discovery, we have too often come across the situation where electronic documents from clients are printed for lawyers as they prefer to work with printed documents. I find it amusing that businesses are quite content to conduct the majority of their dealings over the e-mail and yet, when lawyers enter the picture, all the e-mails are printed out. Hence, law firms need to put in place an electronic workflow with their clients. This will ensure that electronic documents are efficiently handled between lawyers and clients

with the appropriate level of care, even before a suit is filed or notice of arbitration issued. By ensuring an electronic workflow upstream, we will face greater success in ensuring that electronic documents remain in digital form to facilitate efficient management during discovery and the remainder of the litigation process, leading up to presentation in a court room at trial.

MANAGING CIVIL LITIGATION AT PROPORTIONATE COST

Rupert **JACKSON**
Lord Justice of Appeal
Court of Appeal of England and Wales

I. INTRODUCTION: CHANGING OBSTACLES IN THE PATH OF DELIVERING JUSTICE

1 Plato taught that justice is an abstract ideal which can only be studied through philosophy and imitated in the mortal world.[1] Plato's pupil, Aristotle, took a rather more practical approach. He divided justice into two parts: distributive justice and corrective justice.[2] Those two concepts have resonated across 2,000 years, and they still form the starting point for any serious discussion of political philosophy or jurisprudence. The concept of corrective justice has had a massive impact on civil law and common law, both systems being represented at this conference. Corrective justice, as a concept, forms the basis of delict in civil law and tort in common law. It also plays a significant part in the foundations of contract and criminal law.

2 Of course, litigation in the time of Aristotle was relatively straightforward. The parties to litigation in those times were always individuals and the quantity of evidence adduced was for the most part manageable. On the other hand, issues of fairness, justice, or what is proper compensation for accidental or deliberate injury, which were grappled with 2,000 years ago were similar then and now. But the practical problems of delivering justice, the obstacles which now lie in the path of delivering justice have changed beyond recognition.

II. INSTANT ELECTRONIC COMMUNICATION: BANE OR BOON?

3 Instant electronic communication is a boon in many respects, but not in all aspects of modern society. It is not a boon in all aspects because of the

1 Plato, The Republic (Translated by Robin Waterfield, Oxford University Press, 1993).
2 Aristotle, Nicomachean Ethics (Translated by Roger Crisp, Cambridge University Press, 2000).

role, for example, which instant communication has played in the recent London riots.[3] Instant communication is of great benefit to lawyers doing transactional work, and delivering financial and other services to their clients. But instant electronic communication poses several difficulties in dispute resolution. In any major project, all the participants are regularly talking to each other and communicating by instant electronic means: text messages, emails, social network sites, and so forth. And all of these instant electronic communications remain in permanent form to be studied in detail by those who have time and resources. This means, as the Chief Justice Chan Sek Keong ("Chief Justice") has pointed out in his opening address,[4] that the full and painstaking analysis by lawyers of every communication can generate prodigious and sometimes terrifying costs. Of course, as stated by other speakers in the course of this conference these costs can be mitigated by electronic devices and the volume of electronic documents which lawyers must consider can be reduced.

4 The fact remains, however, that sometimes, close scrutiny by lawyers of a large number of documents or electronic material does yield dividends. For example, I recently dealt with an appeal in an intellectual property case where huge sums were incurred in electronic disclosure and analysis of metadata and those huge costs did bear dividends as the claimants were able to demonstrate that certain crucial documents relied upon by the defence were forged. That had a substantial impact on the outcome of the case because it was established that those documents had been prepared at a later date than was alleged. However, as the Chief Justice explained earlier this morning, there are also many cases where huge sums of money are spent on disclosure to little benefit.[5] Sometimes, emails are discovered on both sides where parties or their employees have made incautious comments. While these emails are good material for cross-examination, they usually do not affect the outcome of the litigation.

---

3 See <http://www.telegraph.co.uk/news/uknews/crime/8689076/London-riots-Twitter-users-face-arrest-for-inciting-looters.html>; and <http://abcnews.go.com/Blotter/london-riots-blame-twitter-blackberry-messenger/story?id=14255618>, for newspaper reports which state that instant communication means such as BlackBerry Messenger and social media (eg Facebook and Twitter) were used to coordinate looting and rioting in London in July to August 2011.

4 Chief Justice Chan Sek Keong's Opening Address, above p 1, at [12].

5 *Ibid*.

5 One of the challenges which lawyers in dispute resolution now face is how to manage discovery at proportionate costs and to tailor discovery to the needs of each individual case so that parties are not put to wasted expenditure. In England, the Senior Master Steven Whitaker ("the Senior Master") has developed a new Practice Direction 31B on Disclosure of Electronic Documents ("Practice Direction").[6] This has made a major contribution to dealing with electronic material which needs to be disclosed in litigation in England.[7] I am now seeking to build on this Practice Direction by developing a rule known as the menu option.

6 The principle which underlies this new rule is that we must move away from obsession over standard disclosure as the default option or the starting point in every case. Instead, there must be a more thorough analysis of the issues at the outset of the litigation in every substantial case, so that the courts will make a discovery order which is tailored to the justice of the individual case. The menu from which the courts will choose will be the following:[8]

(a) an order that the court will dispense with discovery altogether;

(b) an order that each party disclose the documents on which it relies and at the same time specify any specific disclosure it requires of another party (this is a rule which is commonly used in international arbitration);

(c) where practical, an order that disclosure be given on an issue-by-issue basis by a party on the material issues in the case;

(d) an order for standard disclosure (that is currently the normal order in England in the majority of cases);

6 Practice Direction 31B – Disclosure of Electronic Documents, which supplements r 31 of the Civil Procedure Rules (SI 1198 No 3132) (UK).

7 See the Senior Master's paper, "International Developments in E-Discovery" below, at p 77, at [16]–[19].

8 The Right Honourable Lord Justice Jackson, *Review of Civil Litigation Costs: Final Report* (Norwich: The Stationery Office, 2010) ("*Jackson Report*") at pp 275–277; 368–372.

(e) an order for *Peruvian Guano* disclosure,[9] which may still be necessary in some cases where fraud or dishonest conduct is alleged; and

(f) any other order in relation to disclosure, that having regard to the overriding objective, the court considers appropriate.

7 This is the outline of the rule on which my colleagues and I are working at the moment. We will be working with the Senior Master to mesh in the final version of this rule with the Practice Direction which he has developed. It is intended that this rule for the menu option will come into force in October 2012.

III. JACKSON REPORT: EXPLORING CAUSES OF EXCESSIVE CIVIL LITIGATION COSTS AND RECOMMENDATIONS TO TACKLE THE PROBLEM

8 Mention of the menu option leads me on to the general reform programme of civil litigation which is now in progress in England, in order to control costs which have escalated far too high. As was mentioned earlier, I was given the task in January 2009 of reviewing the rules and principles governing civil litigation and making proposals to promote access to justice at proportionate costs. The terms of reference are as follows:

(a) establish how present costs rules operate and how they impact the behaviour of both parties and lawyers;

(b) establish the effect case management procedures have on costs and consider whether changes in process and/or procedure could bring about more proportionate costs;

(c) have regard to previous and current research into costs and funding issues; for example any further Government research into conditional fee agreements – *ie*, "no win, no fee" – following the scoping study;

(d) seek the views of judges, practitioners, the Government, court users and other interested parties through both informal consultation and a series of public seminars; and

9 See *The Compagnie Financiere et Commerciale du Pacifique v Peruvian Guano Company* (1882) 11 QBD 55 ("*Peruvian Guano*").

(e) compare the costs regime for England and Wales with those operating in other jurisdictions.

9 I was required to look at the academic research, to consult with all interested groups, to review overseas jurisdictions, to compare those with our own, to look at our own processes and procedures, to recommend procedural reforms and to produce a report within 12 months setting out my recommendations. I divided 2009 into 3 parts: (i) fact-finding, (ii) consultation and (iii) writing the final report. During the fact-finding stage, I asked all judges to record details over a four-week period on every case where summary or final assessment of costs was made. I gathered data from insurers and other sources and set that out in a preliminary report. We then had a consultation period with public seminars, with no punches pulled, where the warring factions and groups with various vested interests laid into one another and forcibly expressed their views. Several thousands of pages of written submissions were provided which I read in August 2009. I prepared my final report ("the Jackson Report") in the autumn of 2009 and it was published in January last year.

IV. CAUSES OF HIGH COSTS OF CIVIL LITIGATION IN ENGLAND AND WALES

10 In the *Jackson Report*, I concluded that there are 16 causes of the high costs of civil litigation in England and I made recommendations as to how those high costs might be tackled. I mention these with some diffidence, because each jurisdiction has different problems, and some but not all of ours will overlap with yours. The 16 causes which I have identified are as follows:[10]

(a) the rules of court requires parties to carrying out time-consuming procedures involving professional skill;

(b) the complexity of substantive law;

(c) the costs rules as they now stand in England;

(d) too few solicitors, barristers and judges have a sufficient understanding of the law on costs or how costs may be controlled;

10 *Jackson Report*, *supra* note 8, at pp 40–51.

(e) lawyers are generally paid by reference to time spent rather than work product;

(f) the recoverable hourly rates of lawyers are not satisfactorily controlled;

(g) the preparation of witness statements and expert reports can generate excessive costs;

(h) the present cost shifting rule creates perverse incentives;

(i) the conditional fee arrangement regime in England and Wales;

(j) the advent of email and electronic databases means that in substantial cases, the process of standard disclosure may be prohibitively expensive;

(k) there is no effective control over pre-action costs, and certain pre-action protocols lead to magnification of these costs;

(l) in some instances, there is ineffective case management both by the parties and by the court;

(m) some cases which ought to settle early, settle too late or not at all;

(n) the procedures for detailed assessment are unduly cumbersome, with the result that they are too expensive to operate and they frequently discourage litigants from securing a proper assessment;

(o) the current level of court fees is too high; and

(p) despite the growth of court fees in recent years, the civil courts still remain under-resourced in terms of staff and information technology ("IT").

11 After a year of pondering and receiving a vast mass of evidence, that was my analysis of the causes of high costs, or rather excessive costs in civil litigation in my own jurisdiction. In my final report, I set out a large number of recommendations as to how those causes of high costs should be tackled.

V. KEY RECOMMENDATIONS MADE TO TACKLE HIGH CIVIL LITIGATION COSTS IN ENGLAND AND WALES

12 Due to time constraints, I will only touch on a few of my recommendations. In relation to the complexity of the rules of procedure,[11] I have recommended that we need to make a determined effort to simplify the rules of procedure and not attempt to legislate for every eventuality, that being a hopeless quest.

13 In relation to understanding of costs,[12] I have recommended that there needs to be much better training, both of judges and of the profession in relation to costs. By training about costs, I do not just mean learning how to assess costs after the event. I mean how one budgets for costs before the event. Solicitors are supposed to give to their clients a proper estimate of the costs of any legal task, contentious or non-contentious, at the outset. Some solicitors in England and Wales are very good at this, either because of their experience, or because they have developed a cost-budgeting software. Other solicitors who may be extremely good at totting up the bill right at the end are not quite so good at budgeting. The Bar has by tradition taken a lordly disinterest in costs, saying that these are matters for the solicitors and their clients. It seems to me to be essential that barristers have a full understanding of costs and budgeting, not least because when they are recommending that work be put in hand, they should understand the costs to which they are committing their clients. And then one comes to judges. It must be said that my profession is not hugely interested in costs. I have some sympathy with that. I wasn't hugely interested in costs until I was asked to prepare a report on the subject. But in truth, if judges are going to manage litigation and give directions controlling for example, the scope of evidence and the scope of discovery, they really must have a proper understanding of costs budgeting and costs assessment.

14 In my view, it is no longer acceptable for the judiciary to disengage itself from the costs aspect of litigation. One should not forget that in very many cases, at least in England and Wales, costs are more than the sum in issue. Judges are very good at working out what damages should be awarded; they understand the principles that regulate damages. In my respectful submission, they need to develop, possess and use precisely the same skills in relation to costs.

11 *Supra* para 10(a).

12 *Supra* para 10(c).

15 I now turn to the seventh cause of high civil litigation costs identified in the *Jackson Report*, *viz*, preparation of witness statements and expert reports.[13] In England, witness statements and expert reports can run to prodigious lengths and cover many matters which ultimately do not prove to be important in the litigation. I have recommended that we need more thorough case management to focus both factual and expert evidence at an earlier stage. I have presented to the Rule Committee and the Rule Committee has approved some amendments to the rules which will lead to greater focusing of expert evidence. Again, these proposed new rules are being held in escrow in order to come into effect on October next year.

16 Moving on through the list of causes of high civil litigation costs, there is the advent of email and electronic databases.[14] I recommended that the Senior Master's Practice Direction[15] should be brought into force, and that has happened. Following that, we need to develop the rule on the menu option, and that is now work in progress.

17 I now move to case management.[16] In relation to case management, I have made a large number of recommendations. One recommendation is that there should be greater continuity of judge. By that, I mean that we do not want cases moving from one judge to another during the case management process more often than is essential. Often, practitioners on both sides of a case are unanimous in urging the need for docketing of cases. Of course, this isn't always welcome to court administrators, because they want to keep flexibility of judicial time. Also judges might find it dull if they become over-specialised. But it does seem to me that cases should be docketed as far as possible. Every jurisdiction has been moving towards a docketing system. I understand that in Singapore, there have been great moves towards docketing, as in Australia and elsewhere. I have made some proposals to ensure greater continuity of judges in managing cases and these are currently being piloted at the court centre in Leeds. Again, if these proposals work out, I hope that they will be applied nationally as of October 2012.

18 Another recommendation which I have made, is that there needs to be much more robust enforcement of time limits and court orders than has

13 *Supra* para 10(g).
14 *Supra* para 10(j).
15 *Supra* para 5.
16 *Supra* para 10(l).

hitherto been the case. It seems to me that parties who are in default are too often let off the hook. Professor Adrian Zuckerman of Oxford University has written forceful articles to the effect that rule 3.9 in our Civil Procedure Rules[17] is in large measure the cause of this.[18] Rule 3.9 sets out a list of matters which the court must consider when a party is in default and is seeking relief from sanctions. The Queen's Bench Masters are very concerned about this rule, and so are many practitioners and the judges. I have recommended that rule 3.9 should be radically rewritten so that courts enforce much more rigorously reasonable time limits imposed by the practice directions and orders of court. Our Rule Committee has approved my recommended redraft of rule 3.9, and that too is being held in escrow until October of next year. I am particularly interested in developments in this regard in Singapore because Singapore built up a great backlog of cases in the past. There was a change of philosophy in the courts, and there was much tougher enforcement by the courts with the result that the backlog was dealt with and cases now move more speedily and less expensively through the system. Every act of non-compliance, every relief from sanction and every extension of time which is granted adds to the costs of civil litigation, so I hope that as of October of next year, there will be a tougher approach in England in relation to the enforcement of orders and reasonable timelines which have been set by the courts.

19 Moving on to another cause, which is the need for better court IT,[19] I set out in Annex 1[20] the various IT systems which now exist in our courts, and I have also included a summary of the e-working system, which is being developed for the Commercial Court, the Technology and Construction Court, and the Chancery Division. I have attached to my conference paper a note prepared by Mr Justice Ramsey, my successor as the Judge in Charge of the Technology Court, and he has developed our e-working system.[21] Of course, in Singapore, you have developed an excellent court IT system, and I have seen a demonstration of the new integrated Electronic Litigation System which is planned for introduction later this year. A court IT system

17 Civil Procedure Rules (SI 1198 No 3132) (UK).

18 Adrian Zuckerman, "How seriously should unless orders be taken?" (2008) 27(1) CJQ 1.

19 See para 10(p) above.

20 See below at pp 23–25.

21 Mr Justice Ramsey's note is not attached to this transcript of Jackson LJ's speech. In essence, it outlines the features of e-working and explains the benefits. For example, it is possible for a litigant anywhere in the world to log in and issue proceedings in the Technology and Construction Court in London.

like this makes a huge contribution towards to controlling of costs incurred in civil litigation, and reduces the time which lawyers are required to spend on administrative steps, all of that time being highly expensive. I congratulate Singapore both in the successful development of its Electronic Filing System,[22] now 11 years old, and the new IT systems being developed, and I am urging the courts in our country to build upon the e-working system.

20 So, Mr Chairman, I have run through a small number of the recommendations made in my report to tackle the causes of high costs. Some of the causes of high costs do not affect other jurisdictions. For example, Singapore does not have the problem which we have of rather strange rules about conditional fee agreements and after the event insurance. So that is not an aspect on which I will comment at this conference.

VI. IMPLEMENTATION OF RECOMMENDATIONS MADE IN THE JACKSON REPORT

21 My report was presented in January of last year, and the government of the day were kind enough to commend it and to say that they would probably implement it. The senior judiciary also expressed support for the recommendations as a package. Despite the favourable response of the government of the day, there was a general election shortly afterwards, where the government of the day was summarily voted out of office and a new coalition government took its place. The new coalition government faced more immediate and pressing problems, such as a massive deficit and the other economic difficulties of which you are aware. I therefore feared that my labours may be wasted, and my report may simply gather dust, like so many other well-intentioned reform reports. It was a great pleasure, for me at least, to see that someone took it out and read it in the course of last year. In November last year, the government published a consultation paper proposing to implement the principal recommendations. Consultations followed, and at the end of March of this year, the government indicated an intention to implement most of the recommendations. A Bill is now going through Parliament in order to give effect to the principal recommendations. It has had two readings in the House of Commons, and

22 See generally Lionel Leo, "Case Management – drawing from the Singapore Experience" (2011) 30 CJQ 142, for a discussion on the Electronic Filing System.

it will now go to the Committee stage. It will subsequently go before the House of Lords. Of course, I do not know what will be the outcome of the Parliamentary process. If however, the Bill is approved by Parliament, it looks likely to come into effect toward the end of next year possibly in October, or possibly at some later date.

22 In the meantime, a small number of recommendations in the report have been implemented, but others are being developed and then held in escrow. It is my hope that a substantial package of the reforms recommended in my report will be introduced in the latter part of next year, perhaps in October, and I have mentioned one or two examples. If these amendments are introduced as a package, they will have more of an impact than introducing individual recommendations at different times.

23 In Singapore, the judiciary has succeeded in achieving a change in culture. An interesting book which I was given yesterday describes it as "Judiciary-led series of reforms".[23] I very much hope that when the reforms in the *Jackson Report* are implemented, if they are implemented, as seems likely but not certain, that we shall achieve a similar change in culture in England. There is still over a year between now and October 2012. In addition to developing draft rules and holding them in escrow, I am also piloting a number of the proposals in my report in individual court centres. The timelag gives a golden opportunity to try out some of the ideas.

24 I have mentioned to you the pilot in Leeds in relation to docketing. We have a pilot running in Manchester in relation to concurrent evidence, otherwise known as "hot-tubbing". This is the Australian procedure whereby opposing expert witnesses give their evidence simultaneously in an enlarged witness box, in the form of a discussion chaired by the judge. The Australian experience is that it is highly beneficial; it puts the experts at ease, and gets the best out of them. Also, it speeds up the process of taking expert evidence and leads to satisfactory results. When I was visiting Australia in the course of the Costs Review, I talked to judges to see what their experience was. I also talked to practitioners to see if they were of the same view. It is not always the case that judges and practitioners are of the same view about the benefits of new procedures. But the practitioners gave me exactly the same answer as the judges. So also did one or two of the court users. Encouraged by this, I recommended that we should pilot concurrent

23 Waleed Haider Malik, *Judicary-Led Reforms in Singapore: Framework, Strategies and Lessons* (World Bank Publications, 2007).

evidence or "hot-tubbing" in England, and if it works, we should add it to our rules. Well, it has been piloted in Manchester, early results are hopeful, and therefore it may well be that this will be another reform for introduction towards the end of next year.

25 Another reform which is being piloted is the provisional assessment of costs. The idea here is that one side lodges its bill of costs, and the other side lodges its objections in writing. The court doesn't have any formal hearing at all but the court issues a provisional decision. The parties can then either accept it, or challenge it. If they challenge the decision, and the party who challenges it does not get a substantially better result, then he will bear the full costs of the taxation or assessment process. We got the idea from Hong Kong, and it is being piloted in Leeds. Again, the early indications are favourable.

26 Another of the reforms being piloted is costs management. I mentioned in the list of causes of high costs, that lawyers are paid by reference to the number of hours worked rather than work product. Now, in the lower value cases, this can be dealt with by a scheme of fixed costs. But a scheme of fixed costs for higher value cases, although it may be feasible in a civil law jurisdiction, is not feasible in a common law jurisdiction. I have therefore after extensive consultation come up with a process of costs budgeting or costs management by the court. The essence of this process is that at an early stage, the solicitors who must prepare a budget for their own clients, should share that budget with the court and the other side, and that it should be put into a special format. The court will then hear arguments about the budget, and then approve or modify the budgets of each party. Thereafter, the court will seek to manage the litigation in line with the approved budgets, of course, making modifications to the budgets if that becomes necessary.

27 It seems to me unreasonable that litigation is the only business project which is conducted without reference to a budget. Much litigation is a business venture for commercial parties on each side. If a commercial organization embarks on a project, whether it is a construction project or anything else, it will do so with reference to a budget. If that organization embarks upon bringing or defending a claim, for business reasons, it would like a budget for that as well. When I floated this idea during the costs review, some lawyers threw up their hands in horror. "Disgraceful", they said; "litigation costs what it costs, justice has no price tag". However, when

I attended some seminars with court users, their view was different. Their attitude was "we don't think that the absence of a price tag is a good idea. Our finance directors want to know what litigation will cost. We think that costs budgeting is rather a good idea."

28 In June 2009 I started to pilot cost budgeting in Birmingham, in the Mercantile Court and the Technology and Construction Court. I ran this on a voluntary basis, so costs budgeting was done only when both parties agreed. The feedback was extremely interesting. The parties on both sides stated that not always, but very often, they found it extremely helpful to know at an early stage of litigation what costs were likely to be awarded to the winning party. It was helpful to see what the other side's costs were. Sometimes, this led to an early settlement, because each party saw what it would have to pay out in costs if it lost, and to what extent its own costs would be irrecoverable if it won. On other occasions, parties with a much better understanding of the financial position went on to trial, but thereafter the costs of the receiving party were readily settled in line with the approved budget because they knew the likely outcome of any judicial assessment of costs.

29 I have subsequently been piloting costs management with the support of the Senior Master in relation to defamation cases in London. The defamation costs management pilot is being revised in the light of experience, and that revised pilot will start in October of this year, and will complete by October of next year. Also, drawing on the experience of Birmingham, I am proposing to pilot costs management in all Mercantile Courts and Technology and Construction Courts across England and Wales. In the new pilot, at the outset of litigation, each side is going to be required to put in a budget for a case in the form of precedent HB.[24] The precedent divides up the costs into pre-action costs, pleading costs, the case management conference, disclosure, witness statements, expert reports and so on. Each stage of the action is set out. There is a breakdown of costs, the various grades of fee earners, the costs of counsel, the likely disbursements, and so on. This form will have a self-calculating mechanism. So if the solicitors feed in the hourly rates, the anticipated times and so forth, the calculations will be done automatically, and the figures will be automatically carried across to the front page. Then the judge will see at the start of each

24 See below at pp 26–29. This will probably be revised before it is finally introduced.

case what the parties' budgets are planned to be. At Annex 3[25] is the current draft of the costs management pilot practice direction. This sets out the procedure to be followed by the court, in approving the budget, managing the case within the budget, and the effect of the approved budget on the assessment of costs at the end of the case. If this costs pilot is successful, we hope that by the end of next year, we will be able to introduce costs management as a feature of our procedural rules.

VII. CONCLUSION

30 In closing, may I say that these conferences are extremely valuable for we face common problems. We can in this forum share our ideas and share our solutions. Singapore is an excellent venue for such a conference, because of the dramatic and successful reforms initiated here in this jurisdiction. If we can overcome the practical problems thrown up by modern society and modern communication, then we can join with Plato and Aristotle in the quest for effective justice.

Editor's Note. Following the delivery of Jackson LJ's address at the International Conference on Electronic Litigation 2011, the Ministry of Justice (United Kingdom) has announced that the implementation date of Jackson LJ's proposals will be deferred from October 2012 to April 2013.[26]

25 See below at pp 30–33.

26 See <http://www.lawgazette.co.uk/news/jackson-civil-cost-reforms-deferred-until-april-2013>.

ANNEX 1

Information technology in the English courts: a patchwork quilt.

At present, there is a plethora of different IT systems operating or being developed in the civil courts of England and Wales. These systems have been installed individually over a long period of time and they are not all compatible with one another. There had been plans to introduce a holistic electronic system across England and Wales, known as the Electronic Filing and Document Management ("EFDM") project, and while EFDM was in development other projects were postponed or cancelled. However, the EFDM project was halted for lack of funding in late 2008.

The main IT systems currently in place in the civil courts are described in chapter 43 of the Costs Review Final Report as follows:

(i) LINK: This was a project to install IT equipment and connections into the courts. That network is now in place in all courts and HMCTS's offices. It is gradually being migrated onto the DOM 1 system under the DISC Infrastructure Renewal (DIR) project so that the same IT system is used throughout the court and tribunal system.

(ii) COINs: A case management system launched in 1997 for what is now the Administrative Court and it allows electronic records of cases to be kept. The application runs on an x.gsi network (accredited to government confidential criteria). COINs has inbuilt functionality that includes the creation and storage of documents against the case record, barcode scanning, a suite of management information reports and a listing diary. The application can be adapted to allow for changes in jurisdiction including, recently, the regionalisation of the Administrative Court.

(iii) Possession Claims Online ("PCOL") and Money Claims Online ("MCOL"): Electronic systems which allow litigants to issue simple, straightforward claims for possession or monetary claims online. The scope of PCOL and MCOL ends once a claim is defended, at which point the cases are printed and transferred to the traditional court system.

(iv) Claims Production Centre: Also known as the County Courts Bulk Centre ("CCBC"). This is a facility attached to Northampton County Court for the filing of vast numbers of straightforward claims. It has been in place since 1991 and it is mainly used by credit card providers to issue debt proceedings.

(v) CaseMan: An electronic case management system which was designed to replace manual record cards in the county courts. Every event in a case can be recorded onto CaseMan and this allows court staff and judges to quickly review the status and history of any given case. There is no centralised database and each county court has its own system with only a partial link between them.

(vi) eDiary: An electronic diary and scheduling system which has been deployed across the county courts. It is limited to each county court, although the courts are able to view one another's diaries.

(vii) New Supreme Court software: Developed by external consultants.

(viii) SUPs: The Service Upgrade Project started in 2003 with a plan for it to be installed in all civil courts. SUPs is a replacement for CaseMan and FamilyMan. It began national roll out on 21 September 2009. It is intended to provide a national database of court records, together with a range of case management, word processing, enforcement and other functions. It is aimed at improving the underlying IT infrastructure across the courts and providing a foundation for an electronic filing and document management system.

(ix) InterCOMM: Also known as the Commercial Court IT project ("CCIT"). The first phase of this project, an electronic case management and listing system for internal use by court staff, was launched in 2005. The second phase of the project was to extend the system to court users but this was cancelled in favour of the EFDM project.

(x) Electronic working: Could be considered the spiritual successor to EFDM. Electronic working (generally known as "e-working") provides an electronic filing system to court users and an

electronic case file for judges and court staff plus the listing component from CCIT. It can be described as being fully end-to-end covering all transactions between parties, court staff and judges.

ANNEX 2

[Claimant / Defendant]'s costs budget dated [ ]

In the: [to be completed]
Parties: [to be completed]
Claim number: [to be completed]

PRECEDENT HB

Work done / to be done	Assumptions [to be completed as appropriate]	Disbursements	Profit Costs	Total
Pre-action costs		£0.00	£0.00	£0.00
Issue / pleadings		£0.00	£0.00	£0.00
CMC		£0.00	£0.00	£0.00
Disclosure		£0.00	£0.00	£0.00
Witness statements		£0.00	£0.00	£0.00
Expert reports		£0.00	£0.00	£0.00
PTR		£0.00	£0.00	£0.00
Trial preparation		£0.00	£0.00	£0.00
Trial		£0.00	£0.00	£0.00
Settlement discussions		£0.00	£0.00	£0.00
Contingent cost A: [explanation]		£0.00	£0.00	£0.00
Contingent cost B: [explanation]		£0.00	£0.00	£0.00
Contingent cost C: [explanation]		£0.00	£0.00	£0.00
GRAND TOTAL (including both incurred costs and estimated costs)				£0.00

comprising incurred costs of: £0.00
and estimated costs of: £0.00

Assumed into the costs of each stage should be the time costs for (a) attendance on own client (b) correspondence with the other party and (c) the general project and strategy management of completing that stage

This estimate excludes:

VAT [if applicable]
Success fees and ATE insurance premiums [if applicable]
Costs of detailed assessment
Other [to be completed as appropriate]

A breakdown of the above figures is found on the following pages.

[Claimant / Defendant]'s costs budget dated [ ]

In the: [to be completed]
Parties: [to be completed]
Claim number: [to be completed]

	Delete as applicable:		Incurred / estimated		Incurred / estimated		Incurred / estimated		Incurred / estimated		Incurred / estimated	
			Pre-action costs		Issue / pleadings		CMC		Disclosure		Witness statements	
		RATE (per hour)	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total
	Fee earners' time costs											
1	Grade A			£0.00		£0.00		£0.00		£0.00		£0.00
2	Grade B			£0.00		£0.00		£0.00		£0.00		£0.00
3	Grade C			£0.00		£0.00		£0.00		£0.00		£0.00
4	Grade D			£0.00		£0.00		£0.00		£0.00		£0.00
5	**Total Profit Costs (1 to 4)**		0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**
	Expert's costs											
6	Fees			£0.00		£0.00		£0.00		£0.00		£0.00
7	Disbursements											
	Counsel's fees [indicate seniority]											
8	Leading counsel			£0.00		£0.00		£0.00		£0.00		£0.00
9	Junior counsel			£0.00		£0.00		£0.00		£0.00		£0.00
10	**Court fees**											
11	**Other Disbursements**											
12	Explanation of disbursements [details to be completed]											
13	**Total Disbursements (6 to 11)**			£0.00		£0.00		£0.00		£0.00		£0.00
14	**Total (5 + 13)**		0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**

[Claimant / Defendant]'s costs budget dated [ ]

In the: [to be completed]
Parties: [to be completed]
Claim number: [to be completed]

	Delete as applicable:		Incurred / estimated		Incurred / estimated		Incurred / estimated		Incurred / estimated		Incurred / estimated		Incurred / estimated	
		RATE (per hour)	Expert reports		PTR		Trial preparation		Trial		Settlement (negotiation / mediation)		Contingent cost A: [explanation e.g. application for a freezing injunction]	
			Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total	Hours (if applicable)	Total
	Fee earners' time costs													
1	Grade A	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
2	Grade B	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
3	Grade C	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
4	Grade D	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
5	**Total Profit Costs (1 to 4)**		0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**
	Expert's costs													
6	Fees	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
7	Disbursements													
	Counsel's fees [indicate seniority]													
8	Leading counsel	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
9	Junior counsel	£0.00		£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
10	**Court fees**													
11	**Other Disbursements**													
12	Explanation of disbursements [details to be completed]													
13	**Total Disbursements (6 to 11)**			£0.00		£0.00		£0.00		£0.00		£0.00		£0.00
14	**Total (5 + 13)**		0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**	0	**£0.00**

[Claimant / Defendant]'s costs budget dated [ ]

In the: [to be completed]
Parties: [to be completed]
Claim number: [to be completed]

	Delete as applicable:		Incurred / estimated		Incurred / estimated	
		RATE (per hour)	Contingent cost B: [explanation e.g. amending pleadings]		Contingent cost C: [explanation e.g. specific disclosure application inc. hearing]	
			Hours (if applicable)	Total	Hours (if applicable)	Total
	Fee earners' time costs					
1	Grade A	£0.00		£0.00		£0.00
2	Grade B	£0.00		£0.00		£0.00
3	Grade C	£0.00		£0.00		£0.00
4	Grade D	£0.00		£0.00		£0.00
5	**Total Profit Costs (1 to 4)**		0	**£0.00**	0	**£0.00**
	Expert's costs					
6	Fees	£0.00		£0.00		£0.00
7	Disbursements					
	Counsel's fees [indicate seniority]					
8	Leading counsel	£0.00		£0.00		£0.00
9	Junior counsel	£0.00		£0.00		£0.00
10	**Court fees**					
11	**Other Disbursements**					
12	Explanation of disbursements [details to be completed]					
13	**Total Disbursements (6 to 11)**			£0.00		£0.00
14	**Total (5 + 13)**		0	**£0.00**	0	**£0.00**

ANNEX 3

Practice Direction 5lF
Costs Management in Mercantile Courts and TCC – Pilot Scheme

This Practice Direction supplements CPR Parts 29, 43, 44, 59 and 60

General

1.1 This Practice Direction is made under Rule 51.2. It provides for a pilot scheme (Costs Management in Mercantile Courts and TCC Scheme) to:

(1) operate from 1 October 2011 to 30 September 2012;

(2) operate in all Mercantile Courts and Technology and Construction Courts; and

(3) apply to proceedings in which the first case management conference is heard on or after 1 October 2011.

1.2 In this Practice Direction "costs management order" means: an order approving the costs budget of any party to the proceedings, after the court has made any appropriate revisions. For the avoidance of doubt, the court cannot approve costs incurred before the date of the first costs management order, but the court (a) may record its comments on those costs and (b) should take those costs into account when considering the reasonableness and proportionality of all subsequent costs.

1.3 Without prejudice to the court's general powers of management under Rule 3.1, in any case proceeding before a Mercantile Court or a Technology and Construction Court in which the Judge considers it appropriate to do so, or on the application of any party in accordance with Part 23, the Judge may make a costs management order.

Modifications of Relevant Practice Directions

2. During the operation of the Costs Management in Mercantile Courts and TCC Scheme:

Use of Costs Budgets in Case and Costs Management

(1) Practice Direction 29 is modified by inserting after paragraph 3B:

> **Case management and costs in Mercantile and TCC cases.**
>
> 3C. In cases within the scope of the Costs Management in Mercantile Courts and TCC Scheme provided for in Practice Direction 51F, the court will manage the costs of the litigation as well as the case itself, making use of case management conferences and cost management conferences in accordance with that Practice Direction.

Estimates of Costs to be set out in detailed costs budgets

(2) Paragraph 6.4(1)(a) of the Costs Practice Direction does not apply to proceedings within the scope of the Costs Management in Mercantile Courts and TCC Scheme.

(3) Section 6 of the Costs Practice Direction is modified by substituting for paragraph 6.5 the following:

> **Costs Budgets in Mercantile Courts and TCC**
>
> 6.5 In proceedings within the scope of the Costs Management in Mercantile Courts and TCC Scheme provided for in Practice Direction 51F, the estimate of costs must be presented as a detailed budget setting out the estimated costs for the entire proceedings in a standard template form, which substantially follows the precedent described as Precedent HB and annexed to that Practice Direction.

Filing of Costs Budgets

3.1 Save where the court otherwise orders, as part of its preparation for the first case management conference, at the same time as filing its Case Management Information Sheet, each party shall file and exchange its costs budget substantially in the form set out in Precedent HB annexed to this Practice Direction.

(In Mercantile cases see paragraph 7.7 of the Practice Direction under Part 59).

(In TCC cases see paragraph 8.3 of the Practice Direction under Part 60).

3.2 Each party should include separately in its costs budget reasonable allowances for:

(1) intended activities: e.g., disclosure (if appropriate, showing comparative electronic and paper methodology), preparation of witness statements, obtaining experts' reports, mediation or any other steps which are deemed appropriate to the particular case;

(2) identifiable contingencies, e.g., specific disclosure application or resisting applications made or threatened by an opponent; and

(3) disbursements, in particular court fees, counsel's fees and any mediator or expert fees.

Purpose of Costs Management

4.1 The court will seek to manage the costs of the litigation, as well as the case itself.

4.2 The objective of costs management is to control the costs of litigation in accordance with the overriding objective. (See rule 1.1).

4.3 At any case management conference or pre-trial review, the court will have regard to any costs budgets filed pursuant to this Practice Direction and will decide whether or not it is appropriate to make a costs management order.

4.4 If the court decides to make a costs management order it will, after making any appropriate revisions, record its approval of a party's budget and may order attendance at a subsequent costs management hearing (by telephone if appropriate) in order to monitor expenditure.

4.5 Any party may thereafter apply to the court if that party considers another party is behaving oppressively in seeking to cause that party to spend money disproportionately on costs.

Discussions between Parties and Exchange of Budgets

5. A party submitting a costs budget to the court under this Practice Direction is not required to disclose it to any other party save by way of exchange. The parties should however discuss their costs budgets during the costs budget building process and before each case management conference, costs management hearing, pre-trial review or trial.

Revision of Approved Budget

6. In a case where a costs management order has been made, at least seven days before any subsequent costs management hearing, case management conference or pre-trial review, and before trial, a party whose costs budget is no longer accurate must file and serve a budget revision showing what, if any, departures have occurred from that party's last approved budget, and the reasons for any increased budget. The court may approve or disapprove such departures from the previous budget.

Keeping the Parties Informed

7. No later than seven days after the conclusion of any hearing, each party's legal representative must:

(1) notify its client in writing of any costs management orders made at such hearing; and

(2) provide its client with copies of any new or revised budgets which the court has approved.

Effect on Subsequent Assessment of Costs

8. When assessing costs on the standard basis, the court:

(1) will have regard to the Receiving Party's last approved budget; and

(2) will not depart from such approved budget unless satisfied that there is good reason to do so.

THE INCORPORATION OF TECHNOLOGY IN COURT ADVOCACY

V K RAJAH*
Judge of Appeal
Supreme Court of Singapore

I. INTRODUCTION

1 We live in a bewilderingly dynamic world that is being ceaselessly reshaped by developments in information and communications technology. It would be no exaggeration to say that the information technology revolution now pervades the entire realm of human activity, even in less developed countries. [1] Additionally, developments in information technology also provide the key reference points for animated debates about the nature and desirability of contemporary social change. It has entirely altered the modes, speed and extent of our communication. The effects of time and space can now be compressed effortlessly. We can now communicate almost instantly with others anywhere anytime through very affordable audio and/or visual messaging devices. The extent of separation with strangers is no longer six degrees but – more often than not – merely a single click. Like King Canute, we cannot stop this unceasing tide of technological waves that often overwhelm us. All of us have to now tread water faster just to stay in the same place. Perhaps Thomas Friedman best captured the impact of the staggering changes that are being unceasingly nourished by connective technology when he famously declared in 2005, "The World is Flat".[2] Inevitably, the courts have not been spared from this

---

* Judge of Appeal, Supreme Court, Singapore. I am greatly indebted to Justin Yeo, Justices' Law Clerk, for his assistance in the preparation of this paper. The views expressed here are personal.

1 Fredric Lederer, "The Road to the Virtual Courtroom? A Consideration of Today's – and Tomorrow's – High-Technology Courtrooms"(1998–1999) 50 South Carolina Law Review 799 ("*The Road to the Virtual Courtroom*") at p 800; Richard Magnus, "The Confluence of Law and Policy in Leveraging Technology: Singapore Judiciary's Experience" (2004) William & Mary Bill of Rights Journal 661 ("*The Confluence of Law and Policy in Leveraging Technology*") at p 661, citing in footnote 2 Manuel Castells, *Information Age: Economy, Society and Culture*.

2 Thomas Friedman, *The World is Flat: A Brief History of the Twenty-First Century* (Farrar Strauss and Giroux, 2005).

technology revolution.[3] That this is so is not surprising: law and its processes are after all structured around specific forms of knowledge, flows of information, and networks of communication.[4]

2 Professor Fredric Lederer, an astute thought leader on the ongoing fascinating interplay between technology and legal processes, has insightfully noted that:[5]

> High-technology courtrooms and technology-augmented litigation are reflections of the understood, but rarely voiced, nature of legal practice. Legal practice, especially litigation and adjudication, is a highly sophisticated form of information management.
>
> > *The courtroom is a place of adjudication, but it is also an information hub.* Outside information is assembled, sorted and brought into the courtroom for presentation. Once presented, various theories of interpretation are argued to the fact finder who then analyzes the data according to prescribed rules (determined by the judge through research, analysis and interpretation) and determines a verdict and result. That result, often with collateral consequences, is then transmitted throughout the legal system as necessary. *The courtroom is thus the centre of a complex system of information exchange and management.*
>
> [footnotes omitted, emphasis added]

3 Determined efforts must be made to adapt and harness technology for the purposes of facilitating both adjudication and advocacy. Failure to do so may result in a progressive decrease in public confidence in the legal system, because wired communities have greater expectations that legal processes will deal with disputes efficiently, transparently and promptly. Courts that do not respond to the need to adapt may find their legitimacy eroded. While some latitude will be given for legal processes to catch up with community practices, the leeway given is unlikely to be generous. However, it must never be forgotten that the dispensation of *even-handed justice* is the *court's lifeblood*.[6] Efficiency is never an *end* in itself, but rather, is the *means* to the more effective dispensation of substantive justice. Improvements

---

3 See generally Richard Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford University Press, 2010) ("The End of Lawyers").

4 Andrew Clark, "Information Technology in Legal Services" (1992) 19(1) Journal of Law and Society 13 ("*Information Technology in Legal Services*") at p 14.

5 *The Road to the Virtual Courtroom*, *supra* note 1, at p 803.

6 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 661, citing Beverley Mclachlin, "Judicial Power and Democracy" (2000) 12 Singapore Academy of Law Journal 311.

generated by technology should *complement* tested and proven methods of administering *justice*.[7] As will become apparent in this paper, the constant tension between *efficiency gains in the justice system* and the *attainment of substantive justice* features at the forefront of decision-making regarding the use of technology in legal processes in general and the courts in particular.

4 Two terms in the title of this paper, "technology" and "advocacy", will be briefly defined. The reference to "technology" is a reference to *information and communications technology* – in a manner of speaking, a reference to *electronic* rather than *electrical* technology.[8] The reference to "advocacy" includes, of course, a reference to the place of adjudication, the courts; however, more than just the courtroom, this paper further examines the *process* of litigation which extends far beyond the courtroom. Admittedly, the title of this paper, "The Incorporation of Technology in Court Advocacy", is so broad-ranging that it ought to encompass a range of issues that could not be contained in a monograph, let alone a single conference paper. As such, it is necessary to limit, at the outset, the ambitions of this paper. First, whilst attempting to look into the future, the present paper does not attempt the impossible task of *predicting* in any detail what a future court will look like. Besides the great amount of conjecture such a predictive exercise will take, it often leaves the futurologist embarrassed when technology far surpasses the limits of his imagination in the blink of an eye. Second, the present paper does not purport to discuss in any great detail the issues that will be addressed in the other papers published in this conference publication.

5 In terms of structure, this paper will briefly *describe* some of the existing technology available in high-technology courts today, focusing in particular on the courts in the United States of America and Singapore. It will also attempt to present *projected* trajectories of such technology within a

---

7 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 661. The learned author goes on to point out that in the view of former Chief Justice of Singapore Yong Pung How, justice should not be on the cutting edge of technology as dignity and due process are too important to be jeopardised through potential system failures or malfunction (citing Chief Justice Yong Pung How, Address at the Technology Renaissance Courts Conference, Singapore (1996)).

8 The distinction between "electronic" and "electrical" may not be reflected in dictionary definitions, but it is evident in common understandings of the terms. For instance, it has been said that "… electrical engineers are usually concerned with *using electricity to transmit energy*, while electronic engineers are concerned with *using electricity to process information*…" (emphasis added).

modest 20–25 year timeframe.[9] However, beyond description and projection, this paper will touch on the important issues of *evaluation* and *justification* of technologically-advanced court advocacy. The key issue in this regard is the *impact* of *technology* on *court advocacy* and *justice* (both procedural as well as substantive) – the extent to which the use of technology enhances or impedes access to and dispensation of justice. This paper's thesis is that technology – when properly utilised – is an enormous boon rather than a bane to *both* court efficiency and the dispensation of justice. Time for adaptation is of course required when new technologies are introduced. However, as society evolves and adapts, problems related to technology resistance should diminish.

6 This paper is arranged as follows. In Part II, the tasks of *description* and *projection* will be undertaken: technology currently available in courtrooms (including futuristic technology courtrooms) will be discussed, and some of the issues related to the respective technologies will be highlighted. Part III focuses on *evaluation* and *justification*. It considers five issues relating to the impact of technology on advocacy, the courts, and justice as a whole. Part IV attempts to pull together the key ideas discussed in this paper and provides some concluding remarks.

II. TECHNOLOGY IN ADVOCACY AND THE COURTS

7 This section provides a *descriptive* survey of the leading technology currently available in courtrooms (including specialised technology courtrooms). It will also proffer a *projection* of possible trajectories of such technology, based on academic commentary, postulation and imagination. For ease of discussion, analysis will be carried out under five sub-sections, with each distinct (but related) stage of litigation being addressed in a separate sub-section. The five sub-sections are:

(a) Pre-trial processes;

(b) Trial processes and adjudication;

(c) Appellate processes and practice;

9 Andrew Clark notes that despite the dominant uses of information technology, the trajectories of technological development in legal services are neither fixed nor immutable: *Information Technology in Legal Services*, *supra* note 4, at p 26.

(d) Law reporting and legal resources; and

(e) Virtual hearings.

8 In each sub-section, the issues related to the respective technologies will be briefly discussed, with the major discussions regarding the impact of technology reserved to Part III of this paper.

1. Pre-trial processes

9 At the pre-trial stage, technology may feature in many different ways, including electronic discovery, electronic pre-trial conferences, electronic case management systems and legal research technology. The first two issues will not be dealt with in this paper. Issues related to electronic discovery have been addressed in depth by the papers on "International Developments in Electronic Discovery" (Senior Master Steven Whitaker, High Court of England and Wales) and "Preservation of Electronic Evidence" (Cavinder Bull, Senior Counsel). Issues related to electronic pre-trial conferences will be considered in the context of virtual hearings (see Part II.E *infra*). Therefore, this sub-section focuses on *electronic case management systems* and *legal research technology*.

(a) Electronic case management systems

10 The trial process begins long before trials are heard in court. Pre-trial, lawyers and courts are faced with the processes of, *inter alia*, filing of pleadings, summonses and supporting documents, *etc*.[10] Modern case management requires systems that help court personnel and lawyers to manage and resolve the steady flow of cases.[11] Case information must be kept current and simultaneously routed to a variety of persons, including clients, opposing counsel, critical court administrative personnel and judicial officers.[12] Managing a case effectively requires managing the *information* that gives rise to the case.[13]

11 Electronic mail ("e-mail") permits instant (or near-instant) communication of information without the need for the physical

10 *The Road to the Virtual Courtroom*, *supra* note 1, at p 803.

11 *Ibid*.

12 *Ibid*, at p 804.

13 *Ibid*.

transference of hardcopy documents. However, e-mail is inadequate as a case management device, at least from a systemic point of view. From the court's perspective, efficiency requires that the case name, parties, lawyers and other data be supplied to the court in an identifiable manner that permits the court to capture that specific information for case management purposes.[14] Many courts worldwide have therefore employed dedicated *electronic filing systems* to enhance case management, although the respective electronic filing systems and their capabilities differ across jurisdictions and courts. In the most basic form, electronic filing either permits or requires lawyers to send pleadings electronically to court,[15] whereas a more advanced system will, *inter alia*, provide for the dispatch of copies to all other necessary parties.[16]

12 I pause to make a few observations on Singapore's foray into electronic case management systems. Singapore has developed the world's first *nation-wide* paperless court system, affectionately known as "EFS" (short for "Electronic Filing System").[17] The EFS is comprehensive in its approach and has revolutionised the conduct of civil litigation through its facilities for electronic filing, electronic extracts, electronic service of documents and the provision of electronic information services.[18] Indeed, the EFS has greatly altered the civil litigation landscape in Singapore. Since its introduction in the late 1990s, more than 7 million documents have been filed and processed through the EFS as at the end of May 2011. The EFS has also effectively allowed documents to be filed after the traditional operating hours of the court registry, and more than 40% of documents have been filed after the registry's traditional closing times. The EFS, however, will soon be replaced by a more-advanced Integrated Electronic Litigation System ("IELS"), which promises greater efficiency and the reduction of redundant steps in electronic filing. Modern electronic form ("e-form") technology will also be used to dynamically generate drafts of court orders and other documents.

13 An equivalent of the IELS for criminal proceedings, the Integrated Criminal Case Filing and Management System ("ICMS"), is also being developed. The ICMS is a comprehensive end-to-end electronic case

14 *Ibid.*
15 *Ibid.*
16 *Ibid.*
17 The Electronic Filing System website is available at <http://info.efs.com.sg/default.htm>.
18 *Ibid.*

workflow designed for the initiation, processing, scheduling, hearing and tracking of all criminal, traffic, juvenile and coronial proceedings from inception to conclusion, from the moment a case is filed to the time a final verdict is pronounced.[19]

14 In the context of family law and matrimonial proceedings, the Subordinate Courts of Singapore has, since 2003, been utilising the electronic Family Application Management System ("FAMS") for, *inter*

19 The main features of the ICMS are:

(a) *E-Lodgement*. Enforcement agencies will be able to electronically register a case and file charges from the convenience of their office 24/7. This will help reduce courthouse visits and time spent in court by investigation officers and counsel in straightforward applications like summonses to witnesses and summonses to accused which the system will enable to be lodged electronically.

(b) *E-Service*. ICMS will enable parties to effect service of documents on each other and the system will incorporate auto-generated alert features to enable the court to keep track of breaches of stipulated timelines for service.

(c) *E-Case File*. Parties will only need to file documents electronically, with no paper copies required. Automatic acknowledgments will be sent to parties on successful filing. The documents filed in connection with a case will be indexed into an electronic file. This will result in readier access to the file for the trial judge. The availability of the case file in the front-end module will also result in immediate availability to parties of their case documents.

(d) *E-Hearings*. Hearings will be conducted electronically with the judge and parties being provided computers to view the documents filed and to present video-recorded evidence, etc. and with display screens for the witness, accused and interpreter. The judge will also have word processing facilities for notes of proceedings to be recorded. The judges' assistant's work station will have the capability to audio-record the proceedings and the DVD file of the proceedings will be uploaded to the electronic case file for use by the court.

(e) *E-Courtroom*. This feature will enable the review of inactive cases, *ie* cases which are pending the execution of the warrant of arrest, through an electronic platform avoiding the necessity for a court attendance by a prosecutor. It will also allow for selected hearings to be conducted virtually in the form of an e-courtroom.

(f) *Tracking function*. This feature will assist in the tracking of case processing and management timelines to flag cases that have exceeded timelines or if performance indicators are not met in a particular case. It will automatically notify court administrators and judges of the occurrence of uncompleted tasks and will assist in the monitoring of the compliance of orders by sending alerts to the courts to provide updates on pending cases.

(g) *Select a court date*. For applications of summons to accused and notice to attend court, there will be a calendar display providing the investigation officer with the opportunity to choose from the available dates when the matter is to be first heard in court.

alia, matrimonial maintenance related matters, personal protection orders, the generation of affidavits, and so forth.[20]

15 The benefits of electronic filing systems are apparent: the use of electronic filing almost entirely eliminates physical storage costs and nullifies the time required for communication purposes.[21] An additional advantage is that electronic filing may also make public access to court documents truly meaningful, for instance, in advanced electronic filing systems where pleadings and associated legal documents are accessible by the public through the Internet.[22] Such public access will be especially invaluable for cases of enormous public interest.[23]

16 Another critical aspect of case management involves the electronic scheduling of hearings. Scheduling hearings is often a tedious process which involves consideration of the schedules of many parties, including the judge, the lawyers and the witnesses. *Electronic scheduling systems* will help to ameliorate problems by helping the parties involved to find a common time at which a hearing can be held. This would require a centralised system which is capable of accessing several calendars. Although the judge's calendar is critical, efficient scheduling should involve access to all other hearings involving the same counsel.[24] A full-featured electronic scheduling system does not currently exist in Singapore. Nonetheless, two developments should here be highlighted. First, the Electronic Queue Management System ("EQMS") provides a system of ensuring an equitable and orderly queue for hearings in the Supreme Court.[25] Second, an

20 The main features of the FAMS are (a) Case Management; (b) Party Management; (c) the Finance Module; and (d) the Counselling Module.

21 *The Road to the Virtual Courtroom*, *supra* note 1, at p 805.

22 *Ibid*.

23 *Ibid*.

24 *Ibid*.

25 According to a brochure provided by the Supreme Court of Singapore (titled "Technology in the Supreme Court"), the EQMS provides an equitable and orderly queue system in the Supreme Court, especially for chamber hearings before the Registrars. The EQMS, which works on a first-come-first-served basis, notifies lawyers of when their case is going to be heard through display screens at various locations in the building. Lawyers and litigants can also opt to be notified via a Short Message Service ("SMS") text message on their mobile phones when their case is due to be heard. With these services, lawyers and litigants are now able to make more effective use of their time while waiting for hearings. The EQMS also allows the Registrars flexibility in managing queues by enabling them to arrange for short matters, such as adjournment or consent applications, to be heard first.

e-Calendar application is currently in the pipeline in the Subordinate Courts. The e-Calendar is a paperless and comprehensive electronic resource management system which, when fully functional, will manage the hearing diaries of the courts and the allocation of courtrooms and chambers across the Criminal, Civil and Family and Juvenile Justice Divisions of the Subordinate Courts to optimise court resources and to more efficiently schedule cases for trials and hearings. Real-time updates of the courts' fixings will also be available to court users and members of the public on the Internet.

17 Several problematic concerns arise from the use of the technology outlined above, although it is suggested that none of these problems are insurmountable. *First*, there is a concern that using electronic systems generally and electronic filing systems in particular will alienate those who have little or no access to technology. Not all lawyers and members of the public are familiar with (or even use) computers; they may therefore be disadvantaged where the legal system requires knowledge of operating such technology. This problem, however, is unavoidable. An adaptation period is almost always required where revolutionary new technologies are introduced. However, as society evolves and adapts, problems related to technology-illiteracy should diminish. In the interim, problems can be ameliorated by assisting lawyers and litigants in accessing and operating the relevant technology. *Second*, and related to the point above, technology adoption and training expenses are significant especially if the court, bar and public is less computer literate.[26] Once again, however, this problem is inescapable, and should diminish with time. *Third*, courts adopting electronic systems may find themselves faced with (potentially problematic) periodic upgrading of software and hardware, which may involve grappling with issues related to compatibility, proprietary software, and so on.[27] *Fourth*, there is a risk that security of certain private documents may be compromised in electronic filing systems; such problems must be carefully addressed to ensure the privacy and confidentiality of those documents.[28]

26 *The Road to the Virtual Courtroom*, *supra* note 1, at p 806.

27 *Ibid*.

28 *Ibid*.

(b) Legal research technology

18 Technology-augmented legal research has become the norm since the ready availability of Internet-based legal resources. The Internet is the best library ever conceived, with vast amounts of information at the user's fingertips. Although information on the Internet is usually unorganised, unwieldy and – not infrequently – unreliable, the development of various software tools helps to filter, curate and facilitate online research.[29] The top tier of research tools is that consisting of *paid specialised knowledge bases* such as LexisNexis,[30] Westlaw,[31] HeinOnline,[32] JStor,[33] and – in the Singapore context – the Singapore Academy of Law's ("SAL") LawNet system.[34] These databases provide a readily accessible wealth of information for lawyers to make their arguments and for judges to refer to. They are also coupled with powerful and intuitive search tools that are able to separate the wheat from the chaff, presenting relevant cases and materials for the busy practitioner and judge alike. Apart from the paid resources, there are also *free online resources*, as provided through Google Scholar,[35] the various Legal Information Institute websites,[36] the Social Science Research Network,[37] and – in the Singapore context – the SAL's Singapore Law website,[38] Singapore Law Watch website,[39] the Attorney-General's Chambers' Statutes Online website,[40] and so on. These databases (both paid and free) have facilitated the locating and citation of relevant authorities in legal submissions and judicial decisions.

19 There is vast potential for the development of legal research technology over the next few years. *First*, knowledge bases have already provided some form of technology to allow the parties concerned to tell – at

29 On this point, see footnote 45 *et seq*.

30 The LexisNexis website is available at <http://www.lexisnexis.com>.

31 The Westlaw website is available at <http://www.westlaw.com>.

32 The HeinOnline website is available at <http://www.heinonline.org>.

33 The JStor website is available at <http://www.jstor.org>.

34 The LawNet website is available at <http://www.lawnet.com.sg>.

35 The Google Scholar website is available at <http://scholar.google.com>.

36 The World Legal Information Institute website, which provides links to the other country-specific Legal Information Institute websites, is available at <http://www.worldlii.org>.

37 The Social Science Research Network website is available at <http://www.ssrn.com>.

38 The Singapore Law website is available at <http://www.singaporelaw.sg>.

39 The Singapore Law Watch website is available at <http://www.singaporelawwatch.sg>.

40 The Attorney-General's Chambers' Statutes Online website is available at <http://statutes.agc.gov.sg>.

a glance – if a case has been overturned, reaffirmed, questioned or cited by later cases (see, *eg*, LexisNexis' "Shepardizing", Westlaw's "Key Cite", *etc*). It would not be a stretch to imagine that such functions could be integrated into legal submissions (especially if such submissions are *electronic*[41]) to allow all parties involved to know whether particular case authorities still remain good law, or have been distinguished or overruled. This would also be of great assistance to the judges, who will be assured (and, if necessary, empowered to do the necessary delving to ascertain) that the legal authorities cited before the court indeed represent the contemporaneous state of the law.

20 *Second*, several online databases provide digital library services (see, *eg*, HeinOnline, JStor, *etc*), and sometimes even for free (see, *eg*, Google Books,[42] Amazon,[43] *etc* which permit free (but limited) browsing of book contents). Based on these currently-available services, it is suggested that a true online law library is not far away. If the relevant stakeholders (*eg*, law firms, law libraries, courts, *etc*) contribute an annual subscription fee to fund payment of royalties to copyright owners of the works provided through an online library, there appears to be no reason in principle why a true online law library cannot be developed based on existing technology. It should be added that having such an online law library can save significant time and resources expended in photocopying hardcopy case authorities and materials for submissions to court. Another bonus for law firms and courts alike will be that online libraries will also help bring down the space requirements and other overheads associated with physical libraries.

21 *Third*, with advances in mobile technology (*eg*, smart phones, tablet computers, *etc*), mobile research becomes increasingly easier. It is already possible under current technology to load entire statutes, subsidiary legislation, regulations and case law authorities *etc* into a smart phone or a tablet computer. In this regard, the Supreme Court of Singapore has already released an "e-Rules of Court" application for computers running the Macintosh or Microsoft operating systems.[44] The SAL has also launched, at this conference, its first mobile computing application – a LawNet application for Apple Inc's "iPad" device. It would clearly not be a stretch to

41 On the point of electronic submissions, see Part II.B(1)(i) *infra*.

42 The Google Books website is available at <http://books.google.com>.

43 The Amazon website is available at <http://www.amazon.com>.

44 The e-Rules of Court website is available at <http://app.supremecourt.gov.sg/default.aspx?pgID=97>.

conceive of the development of applications which allow users to perform legal research on the go, and indeed even when addressing the court itself (for instance on a point that was not contained in the lawyer's submissions).

22 The benefits of legal research technology are manifold, but this paper focuses on a *key* benefit of technology-augmented legal research, namely, the facilitation of knowledge processing.[45] The central paradox of the "information age" is encapsulated in Baudrillard's perceptive observation that "*we are in a universe where there is more and more information, and less and less meaning*".[46] In situations where the problem stems from an *excess* rather than a *lack* of information, it is the capacity to encode and decode information that remains scarce.[47] This problem brings to mind the term "technology lag", coined by Professor Richard Susskind in his provocative book *The End of Lawyers?* to represent the lag between two forms of technology, that is to say, *data processing* and *knowledge processing*.[48] Susskind recognises that we have become very adept at data processing, which involves the use of technology to capture, distribute, reproduce and disseminate information. However, a result of this is that we now suffer from information overload. Knowledge processing technology, on the other hand, is the type of technology that helps us to analyse, sift through, and sort out the mountains of data created and to help make them more manageable. Technology-augmented legal research reduces the "technology lag", and helps all parties involved to more effectively manage the mountains of data that are now generated in legal systems all over the world. In less abstract terms, with the increase in the amount of legal data generated both locally and worldwide (and especially in a legal climate where comparative research is becoming increasingly important), technology-augmented legal research enables a concurrent increase in knowledge processing of legal data by enabling parties to find the relevant materials and to present them before the judicial decision-maker. This is a key, and crucially important, benefit of legal research technology.

---

45 This term is a term of art, and is explained in the text accompanying note 48 *et seq*.

46 *Information Technology in Legal Services*, *supra* note 4, at p 18, citing Jean Baudrillard, *In the Shadow of the Silent Majorities: Or, the End of the Social and Other Essays* (Semiotext, 1983) at p 95.

47 *Information Technology in Legal Services*, *supra* note 4, at p 18.

48 *The End of Lawyers*, *supra* note 3, at p 17.

2. Trial processes and adjudication

23 The core element that characterises technology-augmented litigation and high-technology courtrooms is the use of technology to present *evidence* and *counsel-originated information*.[49] Briefly, the former relates to high-technology computer generated evidence, whereas the latter relates to paperless litigation, visual presentations, and other forms of electronic presentation technology.

(a) Paperless litigation and presentation technology

24 The Supreme Court of Singapore has recently begun conducting paperless hearings for appeals to the apex court, the Court of Appeal. This dovetails with the Singapore courts' commitment to maximise the benefits of technology in its state-of-the-art purpose-built complex, and is a significant step *vis-à-vis* the incorporation of presentation technology in the courtroom. With effect from 4 July 2011, all hearings for appeals to the Court of Appeal are conducted on a "paperless" basis. Liquid crystal display ("LCD") screens are set up on the Court of Appeal bench, the bar table and the public gallery. The LCD screens display the documents (*eg*, electronic written submissions, records of evidence and exhibits, *etc*) that counsel refer to in the course of the hearing, helping judges, lawyers and members of the public to follow the case, and obviating the need for voluminous hardcopy bundles of documents.

25 Undoubtedly, there will be further developments with regard to courtroom presentation technology. This paper discusses *three* possible technologies in this area, namely:

(a) Electronic Submissions;

(b) Integrated Evidence Presentation Systems; and

(c) Immersive Virtual Environment Technology.

(i) Electronic submissions

26 As the experience in the United States shows, electronic submissions are *already possible* given the existing state of technology. The first CD-ROM electronic submission (also known as an "electronic brief" in the

49 *The Road to the Virtual Courtroom*, *supra* note 1, at p 812.

United States) known to be filed by a party was filed in 1997 in the American patent case of *Yukiyo v Wantanabe* 111 F 3d 883 (Fd Cir 1997) ("*Yukiyo*").[50] The electronic submission in *Yukiyo* constituted *multi-media* electronic submissions: for instance, it contained video illustrating dental matters and an audio/video excerpt from a deposition.[51] After objection by the respondent, the United States Court of Appeals for the Federal Circuit struck out the electronic submissions because the appellant had failed to seek the leave of court to file the same, and because the court was of the view that the electronic submissions prejudiced the respondent.[52] However, a CD-ROM submission was accepted by the court shortly thereafter in the case of *In re Berg* 43 USPQ 1703 (Fed Cir 1997).[53]

27 The benefits of electronic submissions are many. At the most basic level, electronic submissions can be regarded as more efficient and environmentally sound versions of traditional hardcopy submissions. The resource savings accrue in the form of savings in printing, file cabinet storage space, and other physical structures needed to house filing cabinets.[54]

28 At another level, however, electronic submissions enable counsel to present cases in a more engaging and interactive way, and avoid the need for judges (and opposing counsel) to manually cross-reference written submissions with other pieces of evidence that are littered throughout a potentially voluminous record of proceedings. These submissions may be in multi-media form, and may involve *inter alia* hyper-linking to the authorities or documents cited in the submissions. For instance, a relevant video or audio recording may be brought up through clicking on a hyperlink; or, the relevant part of the cited authority or document may be referred to by clicking on the citation, without the need to call up a separate "bundle of authorities" or "bundle of documents". In short, where submissions are electronic and hyper-link enabled, the potential for enhancing portability, readability and comprehension of the material is very great.

---

50 Fredric Lederer, "The Effect of Courtroom Technologies on and in Appellate Proceedings and Courtrooms" (2000) 2 Journal of Appellate Practice and Process 251 ("*The Effect of Courtroom Technologies*") at p 263.

51 *Ibid.*

52 *Ibid.*

53 *Ibid.*

54 *Ibid.*

29 As already alluded to above, it would not require new breakthroughs in technology before electronic submissions become feasible. Indeed, the state of technology as long ago as 1997 was already sufficient to support relatively technologically-advanced electronic submissions. There is no reason to doubt that – once such submissions are allowed in courts – they will become the preferred choice (and, indeed, the staple) of litigation lawyers in the near future.

(ii) Integrated Evidence Presentation Systems ("IEPS")

30 The most primitive form of electronic evidence presentation is that presented through the lens of a document camera. Moving onward from the document camera, advanced technological courts such as the New York Supreme Court's Courtroom 228 (also known as "Courtroom 2000") are equipped with integrated evidence presentation systems ("IEPS").[55] These IEPS essentially involve one or more computing devices specifically designed to organise and present evidence of all types and forms in order to maximise persuasive impact.[56] The litigator is the strategist, while the IEPS serves as the faithful adjutant that marshals the evidential arsenal to capture the fact-finder's attention.[57]

31 There are many benefits of an IEPS. *First*, an IEPS is a powerful tool that takes advantage of computing power to effectively convey focused information to the fact-finder.[58] *Second*, by allowing the lawyer to store and present all of his or her documents and other evidence in one central location, an IEPS decreases the time needed to retrieve documents and video footage in court.[59] *Third*, an IEPS allows the lawyer not just to present, but to *interact* with trial evidence immediately;[60] for instance, an area of focus in a document can be highlighted or enlarged through

55 See the New York Supreme Court's Courtroom 228 (also known as "Courtroom 2000"), which has its own IEPS known as DEPS™.

56 Elan Weinreb, "'Counselor, proceed with caution': The use of integrated evidence presentation systems and computer-generated evidence in the courtroom" (2001–2002) 23 Cardozo Law Review 393 ("*IEPS and CGE in the Courtroom*") at p 398.

57 *Ibid*.

58 *Ibid*, at p 396.

59 *Ibid*, at pp 400–401.

60 *Ibid*, at p 401

close-up zooming.[61] *Fourth*, once the infrastructure for IEPS has been set in place, it is a relatively cost-effective technology.[62]

32 However, several issues are raised by the use of IEPS as well. *First*, there is the issue of costs. While IEPS can be cost-effective technology, in extremely high profile or complex cases, IEPS costs may be exorbitant and cost-prohibitive.[63] IEPS also require regular maintenance, and machinery failure is always a potential problem.[64] These are recurring costs that have to be borne by the court – costs which may increase the cost of litigation as a whole.

33 *Second*, there is potential prejudicial effect where lawyers present evidentiary images to the court based on their own interpretation of the meaning of these images.[65] For instance, electronic slideshows raise the possibility of intentional insertion of "visual bias", the equivalent of semantically "loading" the spoken or written message with words carefully chosen to induce a specific psychological reaction.[66] However, it should be noted that this potential prejudicial effect *already exists* where traditional evidence is being presented – the same concerns arguably apply to electronic media as to gruesome photographs of murder victims.[67] A possible way to ameliorate this problem would be for fact-finders to be appropriately sensitised to the potential prejudicial effects, and for other procedural safeguards to be put in place.

34 *Third*, there is a concern that electronic images of evidence that began as or exist as non-digital physical evidence are not identical to the original evidence.[68] For instance, current technology is such that even if a totally accurate image of the original is made or captured, the displayed image will differ in colour or resolution.[69] In most cases, however, such colour differences are irrelevant, because the information context of the evidence is

61 *Ibid*.
62 *Ibid*.
63 *Ibid*, at p 407.
64 *Ibid*.
65 *The Road to the Virtual Courtroom*, *supra* note 1, at p 817.
66 *Ibid*.
67 *Ibid*, at p 818.
68 *Ibid*, at p 816.
69 *Ibid*.

what is important.[70] Accordingly, where the accurate reproduction of colour and/or lighting is necessary, courts should be careful not to rely entirely on the electronically-reproduced evidence.

(b) High-technology electronic evidence

35 The topic of electronic evidence has been examined in the paper on "International Developments in Electronic Evidence" (Mr Stephen Mason), and further discussed in the panel discussions on "Electronic Evidence in Singapore – Law & Practice" and "Presentation of Computer Forensic Evidence". The plenary session and panel discussions covered *inter alia* the treatment of electronic evidence, the authentication of electronic evidence, the reliability of computers and the gathering of evidence by computer forensic experts. Readers are referred to the respective conference papers for further details. As this paper does not propose to cover the same ground, the observations here are limited to *technologically-advanced computer generated evidence* ("CGE") and *immersive virtual environment technology* ("IVET").

(i) Computer Generated Evidence ("CGE")

36 CGE refers to computer-generated productions that purport to represent the operation of some scientific principle ("animations") or the recreation of events at issue in a case ("simulations").[71] In the United States, CGE has already been used in a variety of cases: it has aided both prosecution and defence in trials (*eg*, murder cases, medical malpractice, *etc*).[72] In Singapore, a number of the courtrooms of the Supreme and Subordinate Courts are equipped with computer animation and simulation (or forensic multimedia) technology, allowing visual proximation of the vital elements of real world situations.[73]

37 As already alluded to above, CGE comes in two main forms, *simulations* and *animations*. The distinction between animations and simulations should be emphasised. A computer animation is

70 *Ibid*. For example, the precise colour of the paper or ink constituting a written contract is often irrelevant to the case.

71 Elizabeth Wiggins, "What we know and what we need to know about the effects of courtroom technology" (2003–2004) 12 William & Mary Bill of Rights Journal 731 ("*What we need to know*") at p 739.

72 *IEPS and CGE in the Courtroom*, *supra* note 56, at pp 405–406.

73 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 669.

computer-generated *demonstrative* evidence, such as a computer illustration of (expert) witness testimony or opinion.[74] A computer simulation, on the other hand, involves a computer becoming a witness, and accordingly constitutes *substantive* evidence.[75] In a computer simulation, the computer not only *illustrates* a testimony, it actually *presents* it: sets of variables are fed into the computer, which then processes and synthesizes this information to yield output in the form of a visual presentation that conforms to the laws of physics and science.[76]

38 CGE brings with it many benefits. It may be tremendously persuasive and significantly aid fact-finders in comprehending difficult issues.[77] It can also aid a fact-finder immensely in its retention of information.[78] Indeed, some have observed that the effect of CGE may in fact extend to the negotiating table as well.[79] This is because parties will have a better gauge beforehand – through examining the CGE – as to the likelihood of success at trial. It is thus possible that in this indirect manner, CGE may increase the number of out-of-court settlements.[80]

39 There are, however, several issues raised by CGE. *First*, CGE's greatest power is its ability to impact persuasively. This leads to the concern that CGE may turn a fact-finder into a captive audience. Furthermore, it is unclear whether or not fact-finders attach too much weight to CGE – for instance, in the United States, a trial judge's instructions to the jury were found to be insufficient to offset the tendency of jurors to believe what they see in the CGE, even when physical evidence directly contradicted CGE.[81] *Second*, manipulation and stealth alteration of the evidence which serves as the source for computer animations or simulations is a prominent concern of many commentators.[82] This must carefully be guarded against. *Third*,

74 *IEPS and CGE in the Courtroom*, *supra* note 56, at p 404.
75 *Ibid*.
76 *Ibid*.
77 *Ibid*, at p 396.
78 *Ibid*, at p 420.
79 *Ibid*, at p 407.
80 Bailenson *et al*, "Courtroom Applications of Virtual Environments, Immersive Virtual Environments, and Collaborative Virtual Environments" (2006) 28 Law and Policy 249 ("*Courtroom Applications of Virtual Environments*") at p 262.
81 *Ibid*, at p 420.
82 *Ibid*, at pp 418 and 421.

the use of CGE can be prohibitively expensive, especially if courts require experts to testify upon any and every CGE-related concern at trial.[83]

(ii) Immersive Virtual Environment Technology ("IVET")

40 In the traditional setting, lawyers sometimes employ physical virtual environments in courtrooms, *eg*, using physical objects to indicate a suspect's and witnesses' relative positions.[84] With technology (specifically, IVET), truly virtual environments can be created, to be experienced by the relevant parties involved. The use of IVET would allow judge, jury and witnesses to experience a recreation of a particular scene, the fear or emotional distress, *etc*,[85] through "synthetic sensory information that leads to perceptions of environments and their contents as if they were not synthetic".[86] Such an environment perceptually surrounds the user of the system, the sensory information of the IVET being more psychologically prominent than the sensory information of the physical world.[87] The parties involved may interact with the virtual environment by using any perceptual channel – visual (head-mounted display), auditory (earphones), haptic (gloves that use mechanical feedback or air blasts), olfactory (nosepieces), or gustatory senses.[88]

41 There are many benefits of IVET. Although IVET cannot be used to ascertain an objective truth, these immersive simulations can greatly help to impeach the testimony of unreliable witnesses, test forensic assertions and enhance understanding of a past experience.[89] For instance, IVET is useful where a subjective measurement of perspective is called for and where that perspective needs to be tested and even impeached.[90] IVET has also been used to re-create crime and accident scenes.[91] Furthermore, as observed in the context of CGE earlier, a further collateral benefit of IVET is that it may in fact help to reduce the number of cases that go for trial. Parties will have a better gauge beforehand – through interaction with the IVET – as to

83 *Ibid*, at p 417.
84 *Courtroom Applications of Virtual Environments*, *supra* note 80, at p 251.
85 *What we need to know*, *supra* note 71, at p 742.
86 *Courtroom Applications of Virtual Environments*, *supra* note 80, at p 250.
87 *Ibid*, at p 251.
88 *Ibid*, at pp 250–251.
89 *Ibid*, at p 255.
90 *Ibid*, at p 250.
91 *Ibid*, at p 255.

the likelihood of success at trial. It is thus possible that in this indirect manner, IVET may increase the number of out-of-court settlements.[92]

42 There are, however, several issues raised by the IVET, most of which are similar to those expressed *vis-à-vis* CGE. *First*, IVET could come close to replacing the fact-finder's detached objectiveness with subjective experience.[93] Persons interacting within the IVET may be so persuaded by its lifelike nature that they may become swept up by the IVET content and therefore become unable to objectively consider an opposing viewpoint.[94] That said, although there is the potential of inflammatory information being surreptitiously introduced through IVET, the ability to provide inflammatory information exists in the courtroom today *even without* IVET.[95] Accordingly, it is suggested that with sufficient cautioning and training, fact-finders may be adequately equipped to disregard any inflammatory information that may be surreptitiously brought in via IVET.[96]

43 *Second*, it is questionable as to whose assumptions should underlie the creation of an IVET.[97] This problem, however, is not insurmountable, especially in an adversarial trial process. The characteristics of IVET point toward adopting procedural rules that allow all parties to "play" with the virtual reality simulations – judges and litigants should be able to test the immersive experience, and all parties should be permitted to impeach the credibility of the IVET.[98] This will, however, be a time-consuming and costly process, especially if expert witnesses are required on both sides to address concerns related to IVET.

44 In the end, the issues with both CGE and IVET are more practical than principled. So long as the court maintains an active role as gatekeeper and evaluator of scientific and technical evidence presented,[99] together with the very nature of the adversarial system (which tests all forms of evidence in rigorous ways) will ensure that CGE and IVET can be handled in the way that other forms of expert evidence are handled in courts.

---

92 *Ibid*, at p 262.
93 *What we need to know*, *supra* note 71, at p 742.
94 *Courtroom Applications of Virtual Environments*, *supra* note 80, at p 263.
95 And see text accompanying note 66, *infra*.
96 *Ibid*.
97 *Ibid*, at p 258.
98 *Ibid*, at p 250.
99 *Ibid*, at p 264.

(c) Appellate processes and practice

45 The preceding sections of this paper have covered how technology has entered (or may enter) the trial process in certain jurisdictions. This section deals with *appeals*. In deciding appeals, judges weigh the record, the submissions, and the arguments of counsel, mixed well with an independent view of law and policy. As appellate courts must review the conduct of trials and their results, it is clear that appellate courts must now also consider *the effects of technology* at trial.[100]

46 However, legal technology also changes the *nature of the appeals* themselves. For example, appellate courts will be called upon to consider electronic submissions and receive appellate argument in the form of electronic, perhaps even multi-media, presentations.[101] It is also very possible that the manner of carrying out appellate hearings may change such that judges and counsel appear from remote locations via video.[102] Unlike trials, no live witness evaluation is required when an appeal is heard. Existing assumptions about the need for physical courtrooms to hear *all* manner of appeals may accordingly need to be re-examined.

47 A particular technological innovation that will be discussed here is the potential change in the record of trial from text transcripts to multi-media "transcripts".[103] At the outset, it can be taken that a verbatim record is crucial to the appellate process; this is especially so when the issue on appeal is not just a legal issue, but where the appellate court must also consider whether the trial court's decision was reasonably supported by the evidence.[104] The traditional court record consists of a paper text transcript with the necessary supporting exhibits and ancillary papers. It is prepared either by a stenographic or voice-writer reporter, or by a transcriber from an audio or audio/video recording.[105] However, text transcripts present only a small part of what actually happened at trial – neither voice nor image is

100 *The Effect of Courtroom Technologies*, *supra* note 50, at p 252.

101 *Ibid*.

102 *Ibid*.

103 *Ibid*, at p 252, citing Robert C Owen & Melissa Mather, "Thawing Out the 'Cold Record': Some Thoughts on How Videotaped Records May Affect Traditional Standards of Deference on Direct and Collateral Review" (2000) 2 Journal of Appellate Practice and Process 405.

104 Keith Gorgos, "Lost in Transcription: Why the Video Record is actually Verbatim" (2009) 57 Buffalo Law Review 1057 ("*Lost in Transcription*") at p 1065.

105 *The Effect of Courtroom Technologies*, *supra* note 50, at p 253.

present, and their absence can be extraordinarily misleading.[106] Even when described in the record, witness gestures and demeanour are inadequately set forth in text.[107] Voice intonations are absent, and except for word choice, all witnesses "sound" alike in the text transcript.[108] A judge has made this insightful remark in relation to transcripts:[109]

> A recent film, "My Cousin Vinnie [sic]." Made this point. When accused of a homicide, a character incredulously questioned *"I killed (the victim)?"* The typed transcript of this remark became a confession: *"I killed (the victim)."* Although the transcript was completely accurate in reporting the words said, it was totally inaccurate in conveying the message to the speaker because it did not report the intonation. [emphasis added]

48 Somewhat ironically, a large number of court transcripts begin life as audio or audio/video recordings – this is certainly the case in the Supreme Court of Singapore, and may be the case in courts in other jurisdictions as well. However, as a matter of practice, few courts permit non-transcribed videotaped records on appeal.[110] One possible reason was that text could be browsed quickly and the transcript opened to any necessary point, whereas audio and videotapes must be viewed in real time. However, modern technology now makes available the combined text-central, multi-media court record.[111] Text annotations can be created that are tied to timestamps indicating the tape time and real time to mark particular sections of a recording, such as the start of a particular witness's cross-examination.[112] Indeed, in the year 2000, the United States' Courtroom 21 ("McGlothlin Courtroom") had the capability of producing a contemporaneous multi-media court record, the only problem faced being the lack of storage space (a problem which has largely been resolved today).[113]

49 There are many benefits that can be derived from the usage of video transcripts. *First*, besides human error of the stenographer, studies show that slight variations in verbal and nonverbal language (which include

106 *Ibid*.
107 *Ibid*, at p 254.
108 *Ibid*.
109 *Ibid*, citing *Riley v Murdock* 156 FRD 130 at p 131 note 3 (EDNC, 1994).
110 *The Effect of Courtroom Technologies*, *supra* note 50, at p 256.
111 *Ibid*, at p 257.
112 *Lost in Transcription*, *supra* note 104, at p 1077.
113 *The Effect of Courtroom Technologies*, *supra* note 50, at p 258.

paralanguage[114] and kinesics[115]) can convey additional information, different meanings, and have significant impact on the communicative event that may be crucial to the outcome of a trial.[116] In this regard, a video transcript avoids the pitfalls of written transcripts, by capturing both verbal and nonverbal language. *Second*, implementing video systems are substantially cheaper than employing a court reporter to transcribe every proceeding.[117] *Third*, improvements in technology allow for more cameras and camera angles.[118] Many systems are also voice actuated, so that when someone speaks, either the speaker's picture-in-picture image is enlarged on the screen or the speaker appears full screen.[119] The maintenance of multiple smaller camera views, in addition to a larger, voice-activated image is certainly preferable, so that communicative nonverbal information from non-speakers is maintained while others speak.[120]

50 These advantages suggest that the video transcript is far superior to the text transcript. That said, it must be also noted that the presence of a video transcript would certainly encourage counsel to plead that the appellate court ought to become a second trier-of-fact.[121] The impact of technology on appellate processes practice will be discussed in greater detail in Part III.D *infra*.

(d) Law reporting and legal resources

51 Law reporting in the traditional sense involves the reporting of trial proceedings and/or decisions, either in general news sources (newspapers, Internet news sources, *etc*) or in specialised law reports. As already mentioned above, Singapore's publicly available legal material is presently contained in the Singapore Law website (updated periodically with commentaries on the essential principles of Singapore law), the Singapore

114 Paralanguage includes those nonverbal vocal signs that can be heard, such as intonation, emphasis and even silences.

115 Kinesics refers to the interpretation of visual body movements, or what is commonly referred to as "body language", such as facial expressions, hand gestures, and other body movements.

116 *Lost in Transcription*, *supra* note 104, at p 1059.

117 *Ibid*, at p 1075.

118 *Ibid*.

119 *Ibid*, at p 1079.

120 *Ibid*.

121 *Ibid*, at p 1124.

Law Watch website (a free daily legal news service for the legal community in Singapore and abroad), as well as the Attorney-General's Chambers' Statutes Online website. There is also a micro-site on Singapore law in the Asian Legal Information Institute ("AsianLII") website, although that micro-site does not appear to be frequently updated.[122]

52 The concept of law reporting can be transformed once the possibility of *real-time law reporting* is considered. Experiments have been done in the United States to release real-time text transcripts of court proceedings on the Internet. This is in line with the idea of judicial proceedings as public proceedings, and increases the accountability of the judiciary as well as the transparency of the judicial process. This, it is suggested, might lead to an increase in public confidence in the judiciary, and also ensure that mis-reporting of judicial proceedings by the media is reduced. As Lederer suggests:[123]

> [a]lthough any form of recording or reporting would be satisfactory, appellate courts would do well to consider real-time reporting. Real-time would not only give the court a transcript of the argument but would also permit contemporaneous publication of the argument to the Internet for the edification of the bar and public.

53 Indeed, some commentators have even suggested allowing for real-time *videos* of court proceedings to be placed online. Insofar as the public should have greater access to legal proceedings, so long as adequate security measures are taken, there seems to be no reason in principle why real-time videos of court proceedings cannot in time to come be streamed "live" on the Internet. Indeed, since 1997, the Supreme Court of Canada has broadcast its hearings on cable television. The Supreme Court of New Zealand has also allowed television coverage of court proceedings, with high-definition video feeds and individual cameras covering each of the five sitting judges as well as the counsel addressing the court. In some United

122 The micro-site on Singapore law in the AsianLII website is available at <http://www.asianlii.org/resources/257.html>. At the last check (on 3 August 2011), the Singapore micro-site only contained selected decisions of the Singapore Court of Appeal up to 2009.

123 *The Effect of Courtroom Technologies*, *supra* note 50, at p 262, noting in footnote 31 that some American state courts and organisations are currently recording oral argument and publishing it on the World Wide Web. See, *eg*, Florida Supreme Court, *Gavel to Gavel*; Wisconsin Supreme Court, *Search for Oral Arguments*; Nortwestern University, *The Oyex Project*.

States' courts, oral arguments of parties are broadcast live via satellite.[124] These same arguments can be viewed online, along with the parties' submissions.[125] More recently, the Supreme Court of Arkansas (since 16 September 2010) and the Supreme Court of the United Kingdom (since 16 May 2011) have introduced live-streaming of court proceedings on the Internet. The impact of such technology on the legitimacy of, and access to, court proceedings is discussed further at Part III.E *infra*.

(e) Virtual hearings

54 Virtual hearings are technologically possible now in pre-trial processes (*eg*, virtual pre-trial conferences), trial processes (*eg*, virtual trials), and appellate processes (*eg*, virtual appeals). As a simple working definition, a "virtual hearing" is one in which not all the parties are in the same physical location at the same time. Virtual hearings may be classified into two groups, the difference being one of *degree* rather than of *kind*. The first group involves "video-link technology", where there is a component of video conferencing linking a particular party to the courtroom.[126] The second group involves a true "virtual courtroom", where the courtroom exists only in the data exchange network.[127] Both groups are hereinafter discussed separately.

(i) Video-link technology

55 Video-link technology has been widely used in courts since the 1990s. For instance, in March 1996, the Courtroom 21 Project hosted a video conferencing argument before the United States Court of Appeals for the Armed Forces. The court heard *United States v Salazar* 44 MJ 464 (Armed Forces Appeal 1996) in the McGlothlin Courtroom, with two of its five judges appearing by separate video conferencing systems, life-sized with head and shoulders showing.[128] There is reason to believe that the number

124 *The Road to the Virtual Courtroom*, *supra* note 1, at p 826.
125 *Ibid*.
126 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 663.
127 *The Road to the Virtual Courtroom*, *supra* note 1, at p 837.
128 *The Effect of Courtroom Technologies*, *supra* note 50, at p 269.

of virtual hearings will increase, especially in countries where the need to travel vast physical distances may justify the need to have virtual hearings.[129]

56 In Singapore, for *pre-trial* proceedings, video-link technology is used to conduct bankruptcy hearings and in applications for bail or further remand in criminal mentions,[130] pre-trial conferences for criminal cases,[131] *ex parte* applications for maintenance or personal protection orders, mediation of small claims, and co-mediation with foreign judges in cross-border disputes where parties subscribe to Singapore's jurisdiction.[132] A video conferencing facility has also been set up within the Subordinate Courts to enable lawyers to communicate with their clients who are in prison.[133]

---

129 *Ibid.*

130 The Video Conferencing system with Police and Prisons is used for case mentions in Court 26. These are typically very brief appearances and are largely administrative in nature. The video conferencing with Prisons has been in operation since 1999. It was extended to Police in June 2011. Previously, Changi Prisons would have to arrange for all persons in custody who are scheduled to have their case mentioned to be transported to the Subordinate Courts. They are then physically brought up to the trial court for their case to be mentioned. This involved a great deal of effort in logistics to get the persons in custody to the court on time while ensuring that security was not compromised. When the video link with Changi Prisons is connected, the Mentions Court will receive a live feed of the person in custody. By this video connection to Changi Prisons, persons in custody no longer need to be physically transported to the Subordinate Courts. This results in savings on a great deal of time and effort on the part of Prisons. Instead, persons in custody will now remain within Changi Prisons and are taken to video cubicles where they can see and hear everything that happens in Court 26.

131 The purpose of a pre-trial conference is to ascertain if the case is ready for trial. In general, the defense counsel will attend this conference together with the prosecution who will be represented either by a police prosecutor or a deputy public prosecutor. At this conference, the judge will be informed of the nature of the evidence that will be tendered by the prosecution and by defense counsel. The witnesses will also be made known. The judge will thereafter give a date for the trial. To ensure that the pre-trial conference processes are dealt with expeditiously, conferences via video-link were introduced to eliminate the need for person-in-custody to be brought before the judge. This also serves to avoid the need for public prosecutors to physically attend pre-trial conference sessions at Subordinate Courts.

132 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at pp 663–664.

133 On 1 February 2011, the Subordinate Courts instituted a VidLink Centre within the Subordinate Courts compounds to enable lawyers to interview their clients (who are currently prison inmates). This facility provides three video-link cubicles installed with video conferencing equipment for lawyers to conduct video-interviews with their

57 For *trial* proceedings, video conferencing is used in the giving of evidence by (1) vulnerable witnesses in criminal trials of specified offences,[134] or in *inter partes* applications for personal protection orders, (2) accused persons in proceedings under the *Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act*, and (3) witnesses in civil trials.[135] In the case of vulnerable witnesses, these arrangements help to ensure the reliability of the witness's testimony, while affording the witness an environment conducive to testifying freely and fearlessly against the alleged assailant.[136] Another recent technological innovation directed at trial proceedings is the use of video conferencing technology to optimise the use of court interpreters in the Subordinate Courts. With this innovative system, a single court interpreter is empowered to service several courtrooms or chambers via video conferencing on Samsung's "Galaxy" tablet computers, without having to make physical trips to the different courtrooms.[137] This is especially useful in the Singapore context where – owing to our multiracial population – there is keen demand for the services of court interpreters.

58 There are, however, several issues raised by such virtual hearings facilitated by video-link technology. *First*, the United States' Tenth Circuit Court of Appeals' experiences provide lessons that foreshadow at least one recurring problem with video conferencing – the court provides the following instructions regarding oral arguments over video conference:

---

clients. At Changi Prisons Cluster B2, there are three video-link cubicles retrofitted to facilitate the video-interview sessions where inmates will be able to communicate with their lawyers. Similarly, one video-link room will be set up at Changi Women's Prison to facilitate such video-interviews for women prisoners. In order to protect the lawyer-client confidentiality, all recording capability of the video-interview equipment is disabled. At the VidLink Centre within the Subordinate Courts, a police officer will visually monitor (without audio) all interview sessions real time during the sessions from his console. Lawyers will also be required to undergo the necessary security processes before the commencement of the session.

134 In Singapore, for *trial* proceedings, the physical confrontation with opposing witnesses is replaced with virtual confrontation through the use of live video link for vulnerable witnesses (such as young children and victims of sexual offences) to give evidence in a criminal trial: *ibid*, at p 666.

135 *Ibid*, at p 664.

136 *Ibid*, at p 666.

137 The introduction of the Galaxy Tab is to optimise interpreter resources by enabling one interpreter to service several courtrooms or chambers via video conferencing. The project was first piloted in Family Court from May to June 2011. Two scenarios were tested and both were successful and implemented on 1 July 2011.

"During your argument, you may detect a fractional second delay between the time words are spoken and the time they are heard at the remote conference site".[138] If video conferencing impedes the "give and take" of communication and hinders the ability of the court and parties to air key issues, the use of the technology may need to be adjusted to accommodate these problems.[139]

59 *Second*, there are concerns on whether video conferencing interferes with the right to due process, adequate representation by counsel, and a fair trial.[140] Some criminal defence lawyers are additionally concerned with the possible "de-humanising" effect of having defendants appear by videoconference from the prison facility.[141] On the issue of an accused person's right to counsel, one solution may be borne out by Singapore's experience, where a Practice Direction has been issued to ensure that the accused person's right to counsel, and other rights as an accused, are not affected during pre-trial hearings.[142] The Practice Direction deals with the taking of last-minute instructions by counsel, pre-mention interviews by counsel, scenarios where counsel is absent when the case is mentioned, instances where the court may order that a remanded accused be physically produced, the provision of a dedicated telephone in the courtroom, the muting of video-link to facilitate any necessary private communication between the accused and his counsel, and so on. All these safeguards endeavour to ensure that the accused's unimpeded communication with counsel is accorded the fullest protection. With regard to the possible "de-humanising" effect of video conferencing, further empirical research is desirable.

(ii) Virtual courtrooms

60 The true "virtual courtroom" is possible with today's technology. In a basic form, the virtual courtroom is one in which administrative offences may be resolved without the physical appearance of parties before the judge. An example of such a virtual courtroom in the Singapore context is the

138 *What we need to know*, *supra* note 71, at p 738.
139 *Ibid*, at p 739.
140 *Ibid*, at p 737.
141 *Ibid*.
142 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 664.

Automated Traffic Offence Management System ("ATOMS").[143] Through ATOMS, offenders of minor traffic and parking offences are now offered the flexibility of settling their cases at automated kiosks without having to attend court. At present, ATOMS runs on some 350 private-sector owned kiosks located island wide at high traffic areas like shopping malls. Furthermore, to leverage on the pervasiveness of mobile phone ownership in Singapore, there is also an ongoing effort to develop systems for parties to plead guilty to regulatory offences by a combination of mobile phones and credit cards.[144]

61 In a more advanced form, a "virtual courtroom" would involve an interchange of high-quality audio, video, text and graphical information among trial participants without concern for the physical location of those participants. Such technology is also already possible today. For example, Singapore launched in 2002 a system called JusticeOnline ("JOL"), which is a multiparty communication platform that connects the courts, law firms, and other government agencies involved in the administration of justice, allowing for holistic delivery of court services through the Internet.[145] It is an innovative and unique communication platform for the court and legal industry, facilitating new ways of working, collaboration and service delivery through the provision of cutting-edge synchronous digital and mobile communications tools such as video conferencing, 3G and online

143 ATOMS is the brainchild of a multi-party effort to enhance the efficiency of and public access to the Subordinate Courts. Through the use of technology, offenders of minor traffic and parking offences are now offered the flexibility of settling their cases at automated kiosks without having to attend court. ATOMS is the actualisation of the Subordinate Courts' vision of a virtual courthouse. Working in close cooperation with the other original progenitors of this initiative, namely, the Traffic Police and the Land Transport Authority, the ATOMS system has, since its launch, reaped a bountiful harvest of benefits, both tangible and intangible. On 10 January 2000, ATOMS was further extended to cover offences under the Parking Places Act (Cap 213) and the rules made thereunder, which are prosecuted by the Housing and Development Board (HDB) and the Urban Redevelopment Authority (URA).

144 The mobile phone penetration rate in Singapore has been on an upward trend. Based on 2010 figures, the penetration rate is 143.6%. Through this initiative of allowing guilty pleas through mobile phone, offenders of minor traffic and parking offences will be offered the flexibility of settling their cases on the go, without having to attend court. This will bring the Subordinate Courts closer to the vision of a virtual courthouse. This is also an opportunity to introduce new payment modes for court fines, for instance by credit card.

145 *Ibid*, at p 675.

document collaboration.[146] The web conferencing platform is currently used by the courts, the Attorney-General's Chambers, the Legal Aid Bureau and more than 100 law firms, to conduct virtual court hearings or online meetings. It should be noted that the JOL currently covers mainly cases that are usually dealt with in the privacy of the judges' chambers, *eg*, non-contentious civil interlocutory applications as well as pre-trial conferences for criminal cases and family proceedings in the Supreme, Subordinate and Syariah courts.[147]

62 I do not suggest that *all* cases should be handled in virtual courtrooms. Indeed, it is unlikely that, for the foreseeable future, even a *majority* of cases will be dealt with in virtual courtrooms. This is not for lack of technology, but because – socially – it is unlikely that the wider community will be ready to accept such a courtroom, especially for cases where matters of life and liberty are concerned.[148] *One reason for this is that courthouses have long been considered important, if not key, pieces of public architecture, providing a sense of solidity and often conveying the role of law in civic life.*[149] *Courtrooms, the centre of courthouses, embody the administration of justice; virtual courtrooms and virtual trials, it has been said, threaten that sense of place and solemnity.*[150] *There is merit in that concern, at least for now.*

63 While it is unlikely that the virtual courtroom will *replace* the physical courtroom in *all* cases, there will be an increasing amount of virtual litigation and adjudication.[151] For example, given that chamber hearings involve only submissions by lawyers, they do not raise difficult issues about witnesses testifying from remote locations and being assessed differently from witnesses who are physically present. There appears to be no reason in principle why, absent exceptional circumstances, *chamber hearings* cannot be replaced *entirely* by virtual hearings.

146 See the JusticeOnline website at <http://www.justiceonline.com.sg/main/content/view/13/34>.

147 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 676.

148 *The Road to the Virtual Courtroom*, *supra* note 1, at p 842.

149 *Ibid*, at p 841.

150 *Ibid*.

151 *Ibid*, at p 828.

III. THE IMPACT OF TECHNOLOGY ON ADVOCACY, THE COURTS, AND THE ADMINISTRATION OF JUSTICE AS A WHOLE

64 Technology can foster greater access to justice.[152] It can do so in many ways, as mentioned above. To sum up these benefits generally, it is clear that the efficient diffusion of information and effective communication systems compress the effects of time and space.[153] This enables lawyers to link to the global electronic networks of legal (and commercial) information which enable them to deliver fast and flexible services to their clients.[154] Furthermore, although careful scientific studies are necessary, it certainly appears from the Singapore experience that technology use can, and often does, improve administrative efficiency, shorten trials and improve fact-finder comprehension of evidence.[155]

65 However, beyond the benefits and promises of technology, it is crucial to return to the key question posed at the outset of this paper: the real *impact* of technologically-advanced courts and court advocacy on *justice* (both procedural as well as substantive), and the extent to which the use of technology enhances or impedes the access to and the dispensation of justice. In this regard, five issues surface:

(a) first, the impact of technology on the efficient conduct of a trial;

(b) second, the impact of technology on witness testimony and its evaluation;

(c) third, the impact of technology on litigants and law firms of differing financial and technological capacities;

(d) fourth, the impact of technology on appellate processes and practices; and

(e) fifth, the impact of technology on the legitimacy of, and access to, court proceedings and the consequent enhancement of the rule of law.

---

152 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 679.

153 *Information Technology in Legal Services*, *supra* note 4, at p 15.

154 Indeed, information technology underpins the globalisation of corporate legal practice and plays a strategic role for firms seeking to position themselves in increasingly competitive national and international markets for legal services: *Information Technology in Legal Services*, *supra* note 4, at p 15.

155 See also *The Road to the Virtual Courtroom*, *supra* note 1, at p 828.

1. The impact of technology on the efficient conduct of a trial

66 The technology discussed in Part II above covered a range of pre-trial to post-trial matters. Some of the technologies, especially those relating to case management systems, legal research, paperless litigation and presentation technology, present very little detriment. Indeed, if anything, these plainly *facilitate* the smooth *conduct* of a trial, by ensuring that parties' schedules are de-conflicted, legal research is up to date, judges (or fact-finders) are quickly brought up to speed with the facts and difficult scientific concepts, and so forth.

67 However, certain vexing issues have arisen which suggest that technology may not infrequently create some difficulties with regard to the fair and efficient conduct of a trial.

68 At the pre-trial stage, the enormous problems associated with *electronic discovery* have been the subject of much heated debate. Although the discussion of discovery-related technology has been left to other sessions in this conference, some remarks will be offered here with regard to electronic discovery's impact on the efficient conduct of a trial. With the broadening range of storage media and the adoption of disaster recovery practices in many organisations, a request for discovery can quickly become too broad and inclusive, thereby hugely inflating the cost of compliance with such requests (which have traditionally been borne by the disclosing party).[156] This could impede the proper conduct of a trial, flooding the court with documents that are only (if even) tangentially relevant, and could also rapidly escalate the costs of litigation. Procedural rules should accordingly be established to ensure that requests for electronic discovery are *proportionate to the stake* in a bid to secure substantive justice for the parties. Such a principle of proportionality would, ideally, work to ensure that the scope of requests is never too extravagant.[157] However, even with a principle of proportionality, a focused request for electronic discovery can sometimes quickly escalate the costs of compliance.[158] Courts and lawyers must therefore be cautious to ensure that discovery requests, especially for

156 Yeong Zee Kin, "Recent Developments in Electronic Discovery: Discovering Electronic Documents and Discovering Documents Electronically" (2007) 19 SAcLJ 101 ("*Recent Developments in Electronic Discovery*") at p 124.

157 *Ibid*, at p 125.

158 *Ibid*.

electronic documents, are not used to *oppress* parties to the dispute.[159] Possible solutions to the problems engendered by electronic discovery would include the making of *cost-shifting* or *cost-capping* orders in appropriate cases.[160]

69 At the trial stage, the conduct of a trial may be affected by technology insofar as *virtual hearings* (including both video-link technology and virtual courtrooms) are concerned. It was observed above that video technology may actually impede the "give and take" of communication, interfering with oral argument. On the other hand, it should be noted that most of these difficulties are resolvable with improvements in technology. For instance, video conferencing has come a long way since it was first introduced, with high-speed broadband Internet access allowing real-time streaming with negligible lag times and high definition video.

70 All in all, the discrete use of technology, in Singapore, has had a generally positive impact on the fair and efficient conduct of a trial. Some issues have arisen especially *vis-à-vis* electronic discovery and virtual hearings. However, it appears that *even if* technology may have raised some concerns at present, it is a matter of *when*, rather than *if*, proper regulation and improvements in technology will be able to overcome these problems.

2. The impact of technology on witness testimony and its evaluation

71 The main subject of discussion *vis-à-vis* the impact of technology on witness testimony and its evaluation centres on *virtual or partially virtual hearings*. It is clear from the earlier discussion on virtual hearings that very careful evaluation will be required to determine the impact of virtual hearings on the court's ability to dispense justice; more specifically, on the ability of judges (or fact-finders) to assess evidence, especially evidence relating to the credibility of witnesses. Some observers have suggested that judges and lawyers may evaluate a witness' culpability and credibility differently when the person appears remotely than when the person physically appears in court. Indeed, there is also some research which suggests that evaluations of videotaped confessions (and, by analogy, witness

159 *Ibid*, at p 126.

160 Cost-shifting was approved by the New Zealand Court of Appeal in *Commerce Commission v Telecom Corporation of New Zealand Limited* [2006] NZCA 252. It is also captured by Rule 26(c) of the US Federal Rules of Civil Procedure. See *Recent Developments in Electronic Discovery*, *supra* note 156 at pp 108–114.

testimony in a virtual hearing) can be significantly altered by seemingly inconsequential changes in the camera perspectives taken when the confessions are initially recorded.[161] Videotaped confessions recorded with the camera focused on the suspect (as opposed to other camera positions) led mock jurors to believe that the confessions were more voluntary and accordingly that the suspects were more likely to be guilty.[162] Deliberations among mock jurors did not obviate this effect, nor did warnings or judicial instructions about the possible biasing effect of the camera angle.[163]

72 There is presently no definitive study on whether virtual hearings are unduly prejudicial or favourable to witnesses. There could be a number of imponderables involved, some of which may also be linked to cultural sensitivities and or the literacy of witnesses. Although the research on videotaped confessions (discussed in the preceding paragraph) suggests that virtual hearings may result in erroneous assessment of witness testimony, it should be noted that those studies related to the effects of *camera positioning*. Therefore, the problems raised in those studies may be avoided with proper research and camera positioning when used in a virtual hearing. It should further be noted that four research studies actually show that fact-finders appear to perceive remote witnesses just as they perceive in-court witnesses, neither better nor worse.[164] It would be useful to conduct further empirical studies on the visual and auditory aspects of video conferencing technology, to see if judges and lawyers evaluate a witness' culpability and credibility differently when the witness appears remotely than when the witness appears in person, and whether any such difference is prejudicial.[165] It will also be useful to study whether video conferencing imparts unique characteristics to interpersonal communication which interfere with the goals of oral argument and if so, to what degree.[166]

73 Regardless of whether technology unduly impedes the fact-finder's ability to assess credibility of witnesses, it should be noted that this objection to the implementation of virtual hearings should not be taken too far. Today, it is a brave judge who makes a decision based on witness demeanour *alone* – recourse to logic and objective evidence is ordinarily

161 *What we need to know*, *supra* note 71, at p 737.
162 *Ibid*.
163 *Ibid*.
164 *The Road to the Virtual Courtroom*, *supra* note 1, at p 820.
165 *What we need to know*, *supra* note 71, at p 737.
166 *Ibid*, at p 739.

necessary to justify the fact-finder's decision. An assertion based on undifferentiated evidence often invites mistrust. Paul Ekman, a noted expert in evaluating clues to deceit, has found that judges and lawyers (among others) can do no better than chance in assessing whether people lie. Astonishingly, he found that most of them did not know that "they could not detect deceit from demeanour".[167] While there will certainly be some cases in which the evaluation of witnesses' demeanour may make a critical difference to the outcome, these cases certainly do *not* constitute the statistical majority. Indeed, it should be noted that in many jurisdictions, witness testimony is often given by depositions. The fact-finder is not present when the deposition evidence is given, and the only way to consider such evidence is through a record of the evidence which arguably provides a fact-finder with even *fewer* clues as to a witness' demeanour than does a virtual hearing. I think it can be said with some confidence that the element of a witness's physical presence is ordinarily not crucial in many cases, and courts could perhaps be more liberal in allowing virtual (or partially virtual) *civil* hearings, unless good reasons are given as to why such hearings would unduly prejudice or favour particular witnesses.

74 It should be added that business people today routinely conduct Internet-based meetings with clients and colleagues across geographical locations and time zones. It will only be a matter of time that properly equipped courts follow that lead in hearings involving commercial disputes, especially those involving multiple parties from different geographical locations. Caution is, however, urged in relation to the use of virtual hearings in *criminal* cases, where – more so than in civil proceedings – life and liberty are potentially at stake. Presently, in Singapore, virtual hearings are used in the criminal process for simpler procedural applications such as bail applications and pre-trial conferences. This is as it should be – given the present reliability of technology and knowledge about the consequences of a wholesale crossover to virtual hearings, courts should be slow to conduct *entire criminal trials* by way of virtual hearing.

75 Quite apart from the effect that virtual hearings might have on the *fact-finder*, some observers have noted that giving testimony in a virtual court may have a profound effect on the *witness*. For instance, some have suggested that video transmission from commercial video conferencing

167 Paul Ekman, *Telling Lies: Clues to deceit in the marketplace, politics and marriage* (WW Norton,1992) at p 285.

centres or business surroundings lack the traditional judicial setting thought to convey the seriousness of court testimony.[168] However, there is presently no empirical evidence that might indicate whether remote witnesses are more or less likely to tell the truth than in-court witnesses,[169] and more serious evaluative research has to be carried out in this regard. In any case, if evidence by disposition is permissible in some cases, *a fortiori*, there should be fewer objections to remote testimony in virtual hearings.

76 It is my view that an adversarial system *can effectively* function without the physical presence of all parties in the same location throughout the process. This is especially so in chamber hearings where no witness testimony is involved. Even where witness testimony is involved, it appears that the problems faced *vis-à-vis* the evaluation of such testimony may not be as great as some have imagined. While dramatic "live" cross-examination may captivate judges, lawyers and laypersons alike, it is clearly not *essential* to the adversarial system. With the passage of time and the attendant improvements in technology, it is entirely plausible that virtual hearings will become a widespread reality in most cases.

3. The impact of technology on litigants (or potential litigants) of differing financial and technological capacity

77 The legal system exists for all and must not exclude those who lack the financial resources to afford the use of technology or those who, for a variety of reasons, cannot use technology.[170] The pressing issue to be considered here is whether the introduction of technology in the courts and legal processes exacerbates the unequal playing field amongst litigants, or is in fact a "leveller". In other words, it is necessary to analyse the impact technology may have on access to justice for *litigants* or *potential litigants*. This would depend, *inter alia*, on whether the cost of equipment and the case-specific preparation that requires office access to technology effectively prohibits small firms, solo practitioners and litigants in person from technology use.[171] However, in this context, it must be also be acknowledged that the lack of availability of financial resources to access technology is often overstated. Lack of financial resources and unequal legal

168 *The Road to the Virtual Courtroom*, *supra* note 1, at p 820.
169 *Ibid*.
170 *Ibid*, at p 838.
171 *Ibid*, at p 831.

representation are perennial problems in any contest of wills. After all, in any adversarial system, those with deeper pockets will always have access to greater legal support.

78 The most commonly voiced concern is that the use of technologically-advanced litigation support can decisively influence the outcome of litigation. In these circumstances, there is a risk that the outcome of disputes will increasingly revolve around the issue of technological superiority.[172] It can be said that there is an appreciable risk that the development and deployment of information technology in legal settings will exacerbate existing divisions between the "information rich" and "information poor". In disputes between those who have access to litigation support and those who do not, the latter may be at a disadvantage and, therefore, more likely to accept settlement.[173] It has been rightly observed, the "*wealthier party* can leverage the wonders of technology to strengthen the audio-visual presentation of a case to overwhelm the senses and reasoning of the trier of fact. An *indigent party*, hindered by prohibitive costs of creating such high-quality and persuasive presentation, may be perceived as being unfairly disadvantaged" (emphasis added).[174]In the end, those whose legal representatives have sophisticated information and communication systems at their disposal may gain significant advantages over others.[175]

79 However, whilst there are certainly some problems of potentially exacerbating the unequal playing field amongst litigants, some have perceptively suggested that technology is in fact a "leveller". *First*, the financial costs of utilising technology decrease significantly over time. For instance, the creation of electronic submissions now costs a fraction of what it would have cost two decades ago; by the same token, high-technology developments such as IEPS and CGE will, in time, become increasingly affordable to litigants. *Second*, some have argued that the difference in ability between large and small firms is *quantitative* rather than *qualitative*. Many lawyers from small firms are more computer-adept than lawyers at

172 *Information Technology in Legal Services*, *supra* note 4, at p 22.

173 *Ibid*, at p 22, citing M Tantum, "The lawyer and the war" (1991) 5 Yearbook of Law, Computers and Technology 65.

174 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 669.

175 *Information Technology in Legal Services*, *supra* note 4, at p 26. Certain litigants could gain access to CGE while others would be denied access: *IEPS and CGE in the Courtroom*, *supra* note 56, at p 418.

large firms because they must rely on themselves rather than support staff.[176] *Third*, there are ways to ameliorate problems of injustice engendered by the use of technology. One solution to mitigate cost-equalisation problems associated with technology is, as is done in Courtroom 2000, for technology to be put in the hands of the court rather than lawyers and/or litigants.[177] Financing for such a plan can be obtained, for instance, by charging law firms or litigants a technology usage fee for the year.[178]

80 Indeed, it should be added that technology has helped *individual litigants* to have their day in court (when they may otherwise not have been able to do so). *First*, technology, if properly utilised, can substantially lower the costs of litigation. Paperless litigation cuts down on printing costs, while virtual hearings reduce the travelling and waiting time for lawyers, resulting in lower costs borne by clients. This has the direct salutary effect of making access to courts (and consequently, justice) more affordable for the public in general, and the less wealthy in particular.

81 *Second*, technology may be used to assist those with hearing, vision, mobility or other problems.[179] Internet-based video conferencing proved to be critical in a case decided by the New Jersey Superior Court – the judge in that case granted a plaintiff's application to testify and observe the trial from his apartment via a video conferencing link over the Internet. The plaintiff, who was paralyzed from the neck down and breathed with the aid of a respirator, was too weak to travel from Chicago to New Jersey for his medical malpractice suit against several New Jersey doctors, and the cost and time involved in enabling him to travel would have been prohibitive.[180] As the judge in that case shrewdly observed:[181]

> Why should this court, or any court, fear to tread into an area of advanced technology? To permit the plaintiff to testify via Real Time Video teleconferencing will enable the plaintiff to have the benefit of viewing the trial, and testify live via the Internet where he would otherwise not be present in court due to his medical condition. … Permitting this plaintiff to view the trial and testify via the Internet clearly supports our [c]ourt's public policy to permit handicapped individuals access to our courts. *This, in my opinion, is*

176 *The Road to the Virtual Courtroom*, *supra* note 1, at p 832.
177 *IEPS and CGE in the Courtroom*, *supra* note 56, at p 423.
178 *Ibid.*
179 *The Road to the Virtual Courtroom*, *supra* note 1, at p 824.
180 *Ibid.*
181 *Ibid.*

an essential and appropriate step for modern technology to assist in permitting all people equal access to justice. [emphasis added]

4. The impact of technology on appellate processes and practice

82 It was suggested above that despite the benefits of video transcripts, these may affect the appellate practice in that the presence of a video record itself would seem to encourage the appellate court to become a second trier-of-fact.[182] The move towards a multi-media or video transcript presents the real possibility of affecting the standard of appellate review.

83 Appellate courts traditionally defer to trial court findings of fact because the trial court views witness demeanour.[183] With a multi-media trial record, it is technically possible to provide an appellate court with the equivalent of a trial *de novo*. Of course it should be noted that while a multi-media court record may *permit* such a change, it certainly does not *dictate* it.[184] The tension here is between *justice* (which *may* be attained only by viewing a complete trial record) and *finality* (which would be defeated if appellate courts conduct *de novo* reviews of trials). With regard to the importance of *finality*, when the fact-finder's decision on the facts is likely to stand on appeal, parties can be expected to move from litigation to more productive activities more quickly.[185] More searching review on appeal may encourage litigants to delay dispute resolution, lengthening *inter partes* acrimony.[186] It should further be noted that a true *de novo* review would require a *complete* review of all the evidence, a questionable and (ordinarily) unnecessary waste of resources, as well as a grave threat to finality.[187]

84 Finality is, of course, a critical part of our legal system – review must end at some point.[188] Yet rectitude of decision is also important, and to

182 *Lost in Transcription*, *supra* note 104, at p 1124.

183 *The Effect of Courtroom Technologies*, *supra* note 50, at p 259. Consider the Federal Rule of Civil procedure 52(a), which mandates that findings of fact of the trial court would not be set aside unless clearly erroneous, and "due regard shall be given to the opportunity of the trial court to judge of the credibility of the witnesses".

184 *Ibid*.

185 *Ibid*.

186 *Ibid*, citing Francis Gindhart & Carl Moy, "High-Tech Appeals: Can Hypertext Briefs Aid Justice without Changing the System?" (1997) 83 ABA Journal 78 (arguing the pros and cons of electronic briefs).

187 *The Effect of Courtroom Technologies*, *supra* note 50, at p 260.

188 *Ibid*, at p 261.

constrain an appellate court in gaining access to potentially determinative information seems unjustifiable.[189] Efficiency and finality must thus always be balanced by accuracy in adjudication and public faith in the legal system.[190] Ultimately, the use of the video record at the appellate level does not necessarily mandate disruptive change; most issues on appeal are resolvable after reviewing just relevant (and often) small portions of the case below,[191] and maintaining the finality and efficiency that is currently in place through deference to the trial court certainly has its benefits.[192] So long as care is taken to strike the right balance, the existence of a video record could be beneficial to the justice process.

5. The impact of technology on the legitimacy of, and access to, court proceedings and the consequent enhancement of the rule of law

85 Technology can *enhance* the legitimacy of, and access to, court proceedings. It is suggested that increasing the amount of *publicly available legal material* will be invaluable in promoting the understanding and thereby the rule of law.

86 *First*, real-time reporting of trials (including, *inter alia*, "live" online streaming video coverage), hearings and judgments allows the public to witness legal proceedings, thus increasing the transparency and accountability of the judicial process. All of these steps, when employed judiciously, provide greater access to legal proceedings, which in turn might increase public awareness of the judicial system.[193] The jury is still out as to whether greater public trust is also fostered by this new means of virtual access.

87 *Second*, a freely available electronic archive of judicial decisions ensures that legal decisions are sufficiently publicised and accessible to members of the public. In the Singapore context, there are numerous Singapore law-related websites (as has been discussed above), although – as a preliminary assessment – there does not appear to be enough coverage or permanence of the material in these sources of information. It should be

189 *Ibid*.
190 *Ibid*.
191 *Ibid*, at p 260.
192 *Lost in Transcription*, *supra* note 104, at p 1125.
193 Cf *The Road to the Virtual Courtroom*, *supra* note 1, at p 826.

emphasised that a widely publicised corpus of law is necessary to enhance the rule of law. This brings to mind Professor Lon Fuller's celebrated work, *The Morality of Law*, where Fuller notes that one of the routes to failure of a legal system is the "[f]ailure to publicize or make known the rules of law".[194]

IV. CONCLUSION

88 The ongoing adoption of courtroom technology is such that we can expect massive systemic change in the coming years.[195] Technology, like time, has no respect for legal tradition or practices. Assumptions as to what is essential for a credible judicial process must be re-examined dispassionately by all justice stakeholders. In my view, the tide of change is inexorable, and will bring an increasing degree of "virtualism" to many of our court processes. In some jurisdictions, like Singapore and the United Kingdom, administrative offences are now resolved in virtual courtrooms whenever there is an admission of wrongdoing. As the physical presence of such offenders is not a sentencing imperative, fines can always be settled by electronic means. Pre-trial processes in both civil and criminal matters can also be often conducted in a virtual world if the physical presence of affected parties is not important. I would, however, caution against moving to virtuality in criminal matters until very careful consideration has been given to all its implications. Complete virtuality brings with it unwelcome shades of an Orwellian society. There is, nevertheless, no good reason why appellate advocacy cannot be moved from the physical courtroom to the virtual world, particularly in jurisdictions where distances cause inconvenience.[196] After all, no live witness evaluation is required in the appellate process. However, it should be cautioned that technology in the court will benefit the wider community only *where judges and lawyers are suitably trained and wholeheartedly embrace such developments*.[197] *Bench-bar partnerships* are essential for success.[198] We now see law school students for whom computer usage has been ingrained.[199] However, whilst familiarity and expertise would *encourage* a desire to use courtroom technology, it is

194 Lon Fuller, *The Morality of Law* (New Haven, Yale University Press, 1963).
195 *Ibid*, at p 843.
196 *The Effect of Courtroom Technologies*, *supra* note 50, at p 274.
197 *The Road to the Virtual Courtroom*, *supra* note 1, at p 829.
198 *Ibid*.
199 *Ibid*.

not *enough*.[200] Active efforts in educating on the value (and pitfalls) of legal technology and equipping the relevant persons to harness and handle effectively the latest technology, will be necessary in order to allow technology to have its (promised, and positive) impact on the reshaping of the courts.

89 I have attempted in this paper to give an overview of the impact of technology on court advocacy by the *description*, *projection*, *evaluation* and *justification* of its utilisation, analysing the possible trajectories of technology and the consequent reshaping of court processes. We all have to accept that change will be a constant in our professional lives and that it will occur often. *But change is not in itself a goal for courts. Courts exist for the primary purpose of dispensing justice in a manner that secures the public's enduring confidence.* Courts must therefore adapt to the requirements and aspirations of the societies they serve. Although these may not be the same everywhere, all courts try and improve on the efficiency of their processes. *However, when technology is added to process, justice must not be subtracted from the outcome.* Indeed, technology should be employed to increase rather than decrease the prospects of a just outcome. Fairness to the parties, integrity and efficiency of the justice process, reliability of evidence given with the aid of technology and public acceptance of technology in the justice process must be carefully weighed and considered when new technology is used in the courtroom.[201] The appearance of impartiality and due process must not be compromised. As Lord Devlin rightly observed, the judge who gives the right judgment while not appearing to do so may be thrice blessed in heaven, but on earth he is no use at all.[202] The value of seeing and hearing the judge is not to be underrated. Justice must not only be done but be seen to be done. Although we should prize and encourage anything that enhances efficiency and fact-finding accuracy, we should always be deeply concerned about adopting any technology that increases the appearance of the risk of questionable verdicts, or verdicts reliant more on emotion than fact.[203]

90 Just because we can do something is not in itself a justification to actually do it.[204] As observed earlier, technology must actually complement

200 *Ibid*.
201 *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 680.
202 Patrick Devlin, *The Judge* (Oxford University Press, 1979) at p 3
203 *The Road to the Virtual Courtroom*, *supra* note 1, at p 830
204 *Ibid*, at p 843.

tested and proven methods of administering *justice*.[205] In this regard, the incorporation of technology must be carefully considered in light of its *impact* on advocacy, the courts and the administration of justice. Singapore's experience demonstrates that striking the right balance requires the constant evaluation of the means and objectives of the justice system. If that is done, the measured sowing of the seeds of technology can indeed reap the tangible harvests of enhanced efficiency as well as elevated public confidence in the fair disposal of disputes. However, to do this on a sustained basis requires the constant engagement and involvement of all stakeholders in the justice system with the judiciary providing thought leadership. Crucially, the *implementation* of technology must depend on the *acceptance* of technology in society. New practices must accumulate credibility before they can be absorbed into consensus in place of the old. Different jurisdictions will travel different technological journeys at different velocities, the velocities being functions of, *primarily*, societal acceptance of technology and less human-centric judicial processes. Despite this, we should continue to share experiences with each other so as to make the difficult journey ahead easier for all of us.

---

205 See text accompanying note 7. See also *The Confluence of Law and Policy in Leveraging Technology*, *supra* note 1, at p 661.

INTERNATIONAL DEVELOPMENTS IN E-DISCOVERY

Steven WHITAKER
Senior Master of the Senior Courts of England and Wales
The Queen's Remembrancer

I. INTRODUCTION

1 This paper explores the issues that arise in relation to the disclosure of electronic stored information ("ESI"). First, I explore why the study and practice of an effective approach to the disclosure of ESI is so important, and suggest a general framework for improving the practice of electronic discovery ("e-discovery"). Second, I set out the practice in this area of law in England and Wales before going into some of the details of the new electronic disclosure Practice Direction and questionnaire that we now have in the Queen's Bench. Finally, I will survey the international position on e-discovery before concluding with some final observations.

II. WHY THE STUDY AND PRACTICE OF AN EFFECTIVE APPROACH TO THE DISCLOSURE OF ESI IS SO IMPORTANT

2 First of all, in the narrower sense, there is an obvious need to control disproportionate costs within individual claims that arise from the propensity of discovery, most particularly of ESI, to cause disproportionate amounts of work and costs. In the 1990s, Lord Woolf[1] thought that abolishing automatic train of enquiry discovery would go a long way to solving the spiralling extent and cost of discovery. What was not foreseen was the way that the change from the use of paper to ESI would have a tendency to reintroduce the problems of wide ranging train of enquiry disclosure by the backdoor in the process of defining and enforcing a reasonable and proportionate search for ESI in which parties insist on wide

1 See "Access to Justice", Interim Report to the Lord Chancellor on the civil justice system in England and Wales by the Right Honourable the Lord Woolf, June 1995 and "Access to Justice", Final Report to the Lord Chancellor on the civil justice system in England and Wales by the Right Honourable the Lord Woolf, Master of the Rolls, July 1996.

searches to pull in everything that might possibly be relevant. It is well known that the extent of a reasonable search for ESI as opposed to paper documents is hugely affected by the multiplicity of sources and formats in which ESI can be found and its sheer volume, location and the number of duplicates that can exist. In recent years, the list of emerging forms of ESI is increasing every year. To the basic word processed documents, email and Short Message Service ("SMS") messages must now be added the contents of handheld devices, digital voice recordings, social networking, and the growing propensity to store ESI in a "cloud". Indeed, the use of laptop and handheld devices that are little more than dumb terminals for a huge computer in a "cloud" may well be the direction in which both individuals and businesses are going.

3 Second, in the wider sense, I think there lurks a serious potential for common law jurisdictions to be put at risk as dispute resolution centres by the failure of their lawyers and courts to respond appropriately to the challenges that the discovery of ESI presents. The cost and disproportionality of discovery in litigation is a particular problem of common law civil dispute resolution systems where discovery is seen to be an indispensable tool of justice. This may have been both possible and acceptable historically when the common law nations dominated world trade and business. However, as increasingly that role extends to civil law entities (*eg*, the European Union in large measure and China), the attractiveness of common law systems of law for use in trade and business is, in my view, vulnerable to the exponential growth in the breadth and cost of e-discovery in litigation. Business people in general would obviously be concerned about the rising cost of e-discovery and the lack of predictability of the extent of the discovery process, and would be particularly so in the context of making pre-litigation decisions as to the viability of defending or prosecuting a claim.

4 Traditionally, the answers to these problems are thought to be case management, judicial training, and the use of the Civil Procedure Rules[2] ("the Rules") and the Practice Directions to the Rules ("the Practice Directions") to control e-discovery. However, I want to provoke thought on what else the common law courts can do to encourage other solutions and to somehow dispel the idea that we always have to be fire fighting. There is an almost fatalistic feeling at large that the problem can only get worse as

2 SI 1198 No 3132 (UK).

not only large national and international businesses but also small to medium enterprises turn almost exclusively to the use of systems that create nothing but ESI. It is somehow assumed that future litigation will involve greater and greater volumes of electronic material that are not easy to search for, that are not easily accessible except at disproportionate cost, and that all we can do is create mechanisms in the Rules to ensure that some sort of proportionate search for documents, acceptable to the courts and other parties, is carried out.

1. A suggested framework for improving the practice of e-discovery

5 In my view, our courts, by judges leading in individual cases, should be looking to encourage a different culture amongst businesses, particularly those that know well that they will be regular participants in litigation or are always at high risk of it. And we need to start looking back at the stage in the process before the "litigation hold" stage. We need to look back in the process even beyond document retention policies. We need to start with business practices in relation to the creation, storage and destruction of ESI. The courts need to take a greater interest in what information governance strategies these organisations have.

6 My suggested approach has five related aspects. First, I do not accept that it is inevitable that businesses should, when called upon to disclose documents in litigation, be able only to throw up huge amounts of problematical material in a totally disorganised state, which is difficult to access and makes finding what they and their opponents want virtually impossible without expensive software and review. Software that organises documents as they are generated are, I believe, not expensive in relation to the huge cost that can be thrown up if such software are not used. For example, it is well known that DuPont conducted an internal review some years ago and found that they had produced three years' worth of data representing 75 million documents, 50 percent of which could have been lawfully deleted at a cost saving of US$12 million dollars.[3] What is needed is management of ESI from creation to maintenance and disposal. This puts parties in a good position to search for and produce relevant documentation, and also controls volume and reduces storage. So my first

3 See Oracle White Paper, Lower E-Discovery Costs through Enterprise Records and Retention Management (March 2007) ("*Oracle White Paper*") at p 4.

point is that businesses, particularly those regularly exposed to litigation, should be better prepared for the discovery process by having their ESI well organised and readily searchable. They should create information governance strategies and the courts need to look at being less sympathetic in terms of the orders they make and the costs sanctions they impose on such entities when they have taken no steps in this regard. The courts need to take the lead here. If you want an example of the efficacy of judicial criticism and costs sanction, you need only to look at the case of *Timothy Duncan Earles v Barclays Bank Plc* ("*Earles v Barclays Bank*")[4] in which the judge's criticism of the successful bank's preparedness to produce ESI, and the costs sanction imposed, led the bank to institute a program of internal training in respect of e-discovery.

7 Second, the courts need to scrutinise the parties' document retention policies. The need for a defensible document retention policy in all businesses creating ESI should be "a given". In essence, when I speak in this context of a "document retention policy", I am really referring to a "document destruction policy". Many discovery disputes are about the destruction of data, often because of differing national laws in relation to the protection of personal data. In the United States of America ("US"), these disputes can lead to enormous monetary sanctions on those who are seen to have negligently failed to produce documents. This leads lawyers to encourage clients to disclose far more than is necessary for fear of being sanctioned. This is not a road that I think other common law jurisdictions should be going down. So my second point is that the courts, in appropriate cases, need to stress, by the orders they make, the need for transparency and reasonableness in the policies businesses adopt for the archiving and ultimate destruction of their ESI. If the policy is clear and defensible, the amount of data retained and easily accessible should be greatly reduced and be well organised. In this context, the court should not, except in exceptional circumstances, contemplate authorising the resurrection of and search of deleted material.

8 Third, there is, in my view, an unwarranted tendency on the part of parties to litigation, and particularly in high level cases, that simply because ESI is voluminous and often difficult to access (and therefore by its very nature making it easy to hide documents that are relevant and sometimes important), that when the processes of search are brought in, often using

4 [2009] EWHC 2500 (Mercantile).

sophisticated software, to go to extremes to ensure that every relevant document (let alone the "smoking gun") is not overlooked. Ironically, in the past when all we were concerned with was the discovery of paper documents, in a case in which a party disclosed that it had a building full of lever arch files likely to contain relevant documents, no judge would be heard to say that because the cost of retrieving these documents and reviewing them all was disproportionate to the amount at stake in the case, that the parties would only have to review 60 percent or 70 percent of them. If the paper documents were there, unless some sampling technique could be agreed, they usually had to be searched and reviewed because human review is the only sure way of actually searching for paper documents. In the world of ESI, we are able to use computer software to eliminate a significant proportion of ESI from ever being reviewed by a human. However, with the advent of ESI, even in a small case, if all the documentation that was potentially searchable was printed out it would often fill several rooms or even warehouses. That is part of the problem. The investigation of facts is the basis of common law litigation, and the review of documents is fundamental to that investigation. But computers create more stored information than would have been imaginable to previous generations of lawyers, and we cannot go on adopting the old methods of search and disclosure appropriate for the pre-computer age.

9 So my third point is that in cases where ESI is all over the place because it has not been organised when created, parties need to embrace modern computer technology such as predictive coding software for searching for and reducing the number of documents that need to be reviewed. Such search methods should be easily defensible even though they mean that perhaps as much as 60 percent or 70 percent of the documents identified will never be reviewed. Our courts need to gain an understanding of these systems and encourage their use and be ready to hold them defensible as reasonable methods of search.

10 Fourth, to quote David Lender and Judge Andrew Peck of the US Federal Court for the Southern District of New York in their recent article "10 Key E-Discovery Issues in 2011: Expert Insight to Manage Successfully" ("10 Key E-Discovery Issues in 2011"):[5]

5 See David Lender & Andrew Peck, "10 Key E-Discovery Issues in 2011: Expert Insight to Manage Successfully", *The Metropolitan Corporate Counsel* at <www.metrocorpcounsel.com/pdf/2011/April/01.pdf> at p 5.

> Thus, in order to make litigation more affordable and focused the entire paradigm of discovery needs to change. Litigants and courts should approach discovery differently depending on what is at stake in the case, and how complex the issues are expected to be. There simply is no reason in most cases to produce thousands upon thousands of documents from dozens of custodians, simply because they have touched an issue, when the dispute really centers around a handful of key players who will have most (albeit not all) of the documents that are potentially relevant to the case.

11 This is a process that is at the heart of the new English Practice Direction and e-disclosure questionnaire, which I will touch on later in this paper. So my fourth point is that the courts have to be prepared to set robust and sometimes rough and ready limits to the reasonable search for documents including the search terms or methods used and espouse the principle that in this new world of ESI, turning over every stone is no longer possible (which is why we speak in respect of a reasonable search for ESI in terms of a backdoor return to train of enquiry discovery). The courts have to constantly remind parties that the limitations placed on these exercises for the sake of proportionality may well leave the so-called "smoking gun" and more undiscovered. What we need is justice at proportionate cost and effort.

12 Fifth, while the penny has dropped in the US and at least appears to have dropped if you read the new Practice Direction in England and Wales, there is still insufficient awareness that because of the ubiquitous presence of ESI in all disclosure these days, the traditional approach to the disclosure exercise, that the parties carry out their searches in sealed compartments to the extent which they decide on unilaterally and without prior discussion, has now to be completely revised. So my fifth point is that parties to litigation will only begin to reduce the scope and cost of disclosure if they discuss and hopefully agree the extent of a reasonable search for documents before they undertake the search and if they cannot agree, involve a hopefully knowledgeable court in the process. The need for courts to insist on co-operation and prior discussion of the extent of search is vital. The efforts in the US to deal with what is for them a problem on an altogether higher level suggests that we could all do well to cite the Sedona Conference Cooperation Proclamation in its call for "cooperative, collaborative, [and] transparent discovery" and the expectation that parties will "reach practical agreement on search terms, date ranges, key players, and the

like".[6] That is what the e-disclosure questionnaire in England and Wales intends to assist to do.

III. THE PRACTICE IN RELATION TO DISCLOSURE OF ESI IN ENGLAND AND WALES

13 In England and Wales, the dual sources are of course the Rules and Practice Directions on the one hand and judicial decisions on the other. We have recognised the need for the former since 2005. We have few of the latter, but there is an encouraging trend and I will highlight some of the key cases.

14 In *Nichia Corp v Argos Ltd*[7] at [47], Jacobs LJ criticised "mass disclosure" because of the "real risk that the really important documents will get overlooked". He decried, at [50] and [51], "perfect justice" in which "no stone, however small, should remain unturned" because "the cost and time involved would make it impossible to decide all but the most vastly funded cases [because] the cost of nearly every case would be greater than what it is about." Then there is the case of *Digicel (St Lucia) Limited v Cable & Wireless Plc*,[8] which was the first English decision to highlight the then largely overlooked Practice Direction on e-disclosure and the requirement to discuss disclosure in advance and, in the case of difficulty or disagreement, to refer the matter to the court. I had earlier discussed the case of *Earles v Barclays Bank* in one of my earlier themes. In *Goodale v The Ministry of Justice*,[9] I emphasised that electronic documents differ only from paper in that there are a great many more of them and they are often not easily accessible or their whereabouts are unknown and never have been known. I expressed judicial approval for an approach which relies on technology to reduce volumes. I also stressed the need to limit disclosure, in particular respect of types of document and custodians and I called for more use of the staged approach starting with the material that is most readily available in the hands of key witnesses. Finally, the case of *Grahame Henry Bond v Dunster Properties Limited*[10] bears mentioning. This was a case in which late production of documents that should have been disclosed

6 See The Sedona Conference, *Cooperative Proclamation*, 10 Sedona Conf J 331 (2009 Supp).
7 [2007] EWCA Civ 741.
8 [2008] EWHC 2522 (Ch).
9 [2009] EWHC B41 (QB).
10 [2011] EWCA Civ 455.

earlier were allowed in and this resulted in an adjournment of a preliminary issue trial in a matter that had already been delayed. The Master of the Rolls held, at [110], that "parties should take their disclosure obligations seriously and timeously, and should be expected to be appropriately sanctioned if they fail to comply with that obligation." This is perhaps a sign of the shifting attitude to delay and failure to abide by the Rules which may well lead to a tightening up of the sanctions regime so that there is more predictability in the interlocutory process.

15 From October 2010, the Queen's Bench has been concentrating on the e-disclosure management of individual cases through Practice Directions and the e-disclosure questionnaire. We now have a much more useful Practice Direction road map and an e-disclosure questionnaire for exchanging information relevant to each party's proposed search.

1. Key features of the new Practice Direction

16 Touching first on the new Practice Direction, Practice Direction 31B – Disclosure of Electronic Documents (UK) (the "UK Practice Direction") the key features are as follows. At the outset, the UK Practice Direction emphasises that technology should be used in order to ensure that document management activities are undertaken efficiently and effectively. Electronic documents should generally be made available for inspection in a form which allows the party receiving the documents the same ability to access, search, review and display the documents as the party giving disclosure. Further, as soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include electronic documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business.

17 Importantly, the UK Practice Direction also provides that the parties and their legal representatives must, before the first case management conference, discuss the use of technology in the management of electronic documents and the conduct of proceedings. The parties and their legal representatives must also, before the first case management conference, discuss the disclosure of electronic documents. In some cases (*eg*, heavy and complex cases) it may be appropriate to begin discussions before

proceedings are commenced. The discussions should include (where appropriate) the following matters:[11]

> (1) the categories of electronic documents within the parties' control, the computer systems, electronic devices and media on which any relevant documents may be held, storage systems and document retention policies;
>
> (2) the scope of the reasonable search for electronic documents required by rule 31.7;
>
> (3) the tools and techniques (if any) which should be considered to reduce the burden and cost of disclosure of electronic documents, including—
>
> > (a) limiting disclosure of documents or certain categories of documents to particular date ranges, to particular custodians of documents, or to particular types of documents;
> >
> > (b) the use of agreed keyword searches;
> >
> > (c) the use of agreed software tools;
> >
> > (d) the methods to be used to identify duplicate documents;
> >
> > (e) the use of data sampling;
> >
> > (f) the methods to be used to identify privileged documents and other non-disclosable documents, to redact documents (where redaction is appropriate), and for dealing with privileged or other documents which have been inadvertently disclosed; and
> >
> > (g) the use of a staged approach to the disclosure of electronic documents.

18 If at any time it becomes apparent that the parties are unable to reach agreement in relation to the disclosure of electronic documents, the new Practice Direction provides that the parties should seek directions from the court at the earliest practical date.[12] If the court considers that the parties' agreement in relation to the disclosure of electronic documents is inappropriate or insufficient, the court will give directions in relation to disclosure. When doing so, the court will consider making an order that the parties must complete and exchange all or any part of the e-disclosure questionnaire within 14 days or such other period as the court may direct. If a party gives disclosure of electronic documents without first discussing with other parties how to plan and manage such disclosure, the court may require that party to carry out further searches for documents or to repeat other steps which that party has already carried out. The factors that may be

11 UK Practice Direction para 9.

12 UK Practice Direction para 32.

relevant in deciding the reasonableness of a search for electronic documents include (but are not limited to) the following:[13]

(1) the number of documents involved;

(2) the nature and complexity of the proceedings;

(3) the ease and expense of retrieval of any particular document. This includes:

(a) the accessibility of electronic documents including e-mail communications on computer systems, servers, back-up systems and other electronic devices or media that may contain such documents taking into account alterations or developments in hardware or software systems used by the disclosing party and/or available to enable access to such documents;

(b) the location of relevant electronic documents, data, computer systems, servers, back-up systems and other electronic devices or media that may contain such documents;

(c) the likelihood of locating relevant data;

(d) the cost of recovering any electronic documents;

(e) the cost of disclosing and providing inspection of any relevant electronic documents; and

(f) the likelihood that electronic documents will be materially altered in the course of recovery, disclosure or inspection;

(4) the availability of documents or contents of documents from other sources; and

(5) the significance of any document which is likely to be located during the search.

19 The UK Practice Direction states that the primary source of disclosure of electronic documents is normally reasonably accessible data.[14] A party requesting under rule 31.12 specific disclosure of electronic documents which are not reasonably accessible must demonstrate that the relevance and materiality justify the cost and burden of retrieving and producing them. However, it will often be insufficient to use simple keyword searches or other automated methods of searching alone. The injudicious use of keyword searches and other automated search techniques may result in failure to find important documents which ought to be disclosed and/or excessive quantities of irrelevant documents, which if disclosed would place an excessive burden in time and cost on the party to whom disclosure is

13 UK Practice Direction para 21.

14 UK Practice Direction para 24.

given. The parties should thus consider supplementing keyword searches and other automated searches with additional techniques such as individually reviewing certain documents or categories of documents (*eg*, important documents generated by key personnel) and taking such other steps as may be required in order to justify the selection to the court. Where copies of disclosed documents are provided in native format, some metadata will be disclosed with each document. A party requesting disclosure of additional metadata or forensic image copies of disclosed documents (*eg*, in relation to a dispute concerning authenticity) must demonstrate that the relevance and materiality of the requested metadata justify the cost and burden of producing that metadata.

2. The new e-disclosure questionnaire

20 As for the e-disclosure questionnaire itself, I think it is a sound checklist and I do not think there is a single question in this questionnaire that does not need to be addressed by a lawyer conducting a competent search for ESI. The questionnaire starts with the most obvious considerations but it does assume that at this stage after pleadings are closed, each party will have a good preliminary grasp of what the actual issues in contention in the case are. My practice is that in some major litigation (*eg*, the group litigation orders that I manage), I will ask the parties to draw up a list of issues that are agreed between them at this stage where it is possible for such a list of issues to in effect replace the pleadings. Sometimes in very heavy cases I will be asking them to prepare a disclosure and/or a litigation plan. As for the date range the search has to cover, sometimes there will be different date ranges for different issues for different custodians and this is the first and most simple way of beginning to narrow down what has to be searched for and collected. The next step is a consideration of who the custodians of the documents that need to be searched are. In other words, who are the "key players"? It is particularly at this stage that the parties need to be thinking about how they can put proportionate limits on the search. For example, there may have been 20 people involved with the particular core issues in the case but it may not be proportionate or necessary to collect all of their documents and subject all of them to review in the first instance. There is much to be said for imposing a staged approach even at this early stage of litigation (which the UK Practice Direction recommends). For example, it may be reasonable to take the view that searching for and reviewing the documentation of five

major "key players" out of the 20 is likely to produce all the necessary relevant documents and indeed that can be cross checked to some extent by sampling in respect of a few of the others.

21 The next consideration is the types of communications or documents that were created or stored during the relevant date range. Obviously email and word-processed documents are the most likely candidates but the footnotes to the questionnaire draw attention to a multiplicity of different types of ESI. This questionnaire then asks the lawyer to consider, with the client, where and on what type of software, equipment or media is the information actually stored and it prompts at least a provisional decision for the purposes of informing their opponents, when they come to confer, about whether it is intended to search for documents in a particular category or not. There is also a useful statement to be made about whether any of the materials are backups or archives and whether it is intended to search those. From my point of view, this is a key area for giving consideration to distinguishing between the ESI which is easily accessible and that which is not or is more expensive to access because it is in relation to that sort of information that it is necessary for the court, if it is asked to rule on the extent of search, to consider the issue of proportionality. Before leaving the general topic of what there is to search for and where it is, the questionnaire inevitably turns to the subject of whether there is structured data and it asks about databases. This is very much a "last but not least" question because some cases turn almost entirely on what is contained in a company or public authority's structured databases. So that is the effective checklist for what there is, where it is and who has it. The next thing parties have to turn their minds to is how they are going to go about the search.

3. Personal experience in managing e-discovery

22 A year on, the e-disclosure questionnaire seems to be working well. My experience is mainly from multi-party litigation and group litigation orders. In those cases, the e-disclosure questionnaire provides the necessary framework for exchange of information so that rational decisions can be made on the extent of a reasonable and proportionate search. I think the same is true in most major litigation. Anecdotal evidence from practitioners is that there is a fair amount of use of the questionnaire, as a checklist, even where it has not been ordered. There is not much evidence of misuse other than perhaps a little tactical threats as to alleged inadequacy of answers.

23 However, I have noticed several common mistakes that parties make in relation to e-disclosure, and they are as follows. First, parties sometimes misunderstand the building blocks of the process. There is still some general ignorance of what the process is about and the need for a structure for a reasonable and proportionate search for electronic documents. Further, some parties wrongly assume that e-disclosure is a method of disclosure of electronic documents and not a reference to a search for such documents. Second, there is sometimes a lack of understanding that the collection process to gather potential documents for disclosure is a key stage at which to restrain the scope of search and make it proportionate. This should be the stage at which parties should be limiting date ranges, custodians and types of documents as far as possible and eliminating documents which are not easily accessible from the search. Third, there is a lingering reluctance to use software to eliminate duplicates, near duplicates, thread emails and a general reluctance to use modern software search techniques before review. Parties still assume that keyword searching, particularly in structured databases, is the best method. Finally, I have noticed an over-reliance on human review where the results of collection in terms of numbers of documents make it quite clear that something else has to be done or the exercise will be totally disproportionate.

24 In my view, the court has a role to play in assisting parties with the e-disclosure exercise. The court is in a good position to stand back and take a non-partisan view of what is proportionate. Its role is to help the parties frame a reasonable and proportionate search and if necessary rule on it. In order to do this the court needs to be asking questions about the date range of the issues, who the key custodians of documents are, what sort of documents or media are the most important, how accessible the documents are, and how much will it cost to get at those that are not readily accessible. The key stages in the disclosure process where the parties are most likely to seek the court's guidance in resolving a particular dispute are as follows.

> (a) First, at the outset, where typically the party with the least to disclose will want the widest possible disclosure from the party that has the most to disclose! At this stage the court should, if possible, adopt a staged approach and in any event narrow down the search as far as possible after considering with the parties its component parts.
>
> (b) Second, having decided or agreed what documents to go for, the question of agreeing a search methodology arises. This often produces

arguments about keywords. Here the court should look carefully at whether keyword searching, particularly in big cases, is appropriate and whether more sophisticated techniques and software should be used. In any event I never find it appropriate to rule on keywords without evidence of the number of "hits" particular terms throw up. The UK Practice Direction warns against the dangers of keyword searching. On the subject of keywords, I can do little better than cite from 10 Key E-Discovery Issues in 2011:[15]

> Following on decisions by Magistrate Judges Facciola and Grimm, Judge Peck's decision in *William A. Gross Construction Assoc. v. American Manufacturers Mutual Ins. Co.*, 256 F.R.D. 134, 134, 136 (S.D.N.Y. 2009) (Peck, M.J.), constituted a "wake up" call to the Bar, as follows:
>
> > This Opinion should serve as a wake-up call to the Bar in this District about the need for careful thought, quality control, testing, and cooperation with opposing counsel in designing search terms or "keywords" to be used to produce emails or other electronically stored information ("ESI") …
> >
> > …
> >
> > Electronic discovery requires cooperation between opposing counsel and transparency in all aspects of preservation and production of ESI. Moreover, where counsel are using keyword searches for retrieval of ESI, they at a minimum must carefully craft the appropriate keywords, with input from the ESI's custodians as to the words and abbreviations they use, and the proposed methodology must be quality control tested to assure accuracy in retrieval and elimination of "false positives." It is time that the Bar – even those lawyers who did not come of age in the computer era – understand this."
>
> Even if the steps suggested in the *William A. Gross* decision are followed, keyword searching will produce less than 50% of responsive ESI. There are more sophisticated search tools available, such as clustering and concept searching techniques instead of or in combination with keyword searches that may be considered. We are not aware of any published judicial decision addressing these tools …

25 The courts' role will, in the appropriate case, be to rule on whether methods such as predictive coding software *are* reasonable and

15 *Oracle White Paper*, *supra* note 3, at p 5; 10 Key E-Discovery Issues in 2011, *supra* note 5.

proportionate and whether the parties may review only a selected corpus of the documents they have collected.

IV. A LOOK AT THE INTERNATIONAL POSITION

1. The US position

26 In the US, there is frequent use of adverse jury instructions and large monetary sanctions in respect of discovery. Both parties and their lawyers may pay the price for mistakes made during the course of the discovery process leading to failure to preserve or collect ESI or incomplete or delayed production. For example, in *Qualcomm Inc v Broadcom Corp (Qualcomm I)*,[16] a penalty amounting to US$8 million was imposed for failure to comply with discovery obligations. In *Merck Eprova AG v Gnosis*,[17] attorney's fees of US$25,000 were disallowed for the failure to preserve adequately. Furthermore, a prison sentence of up to 2 years for civil contempt was imposed on the spoliating party in *Victor Stanley v Creative Pipe*.[18]

27 And there is now news of a professional negligence suit filed against a large firm of US Attorneys for alleged failure to supervise privilege review properly with the result that 3900 privileged documents were allegedly handed to the US Government.

28 In *Rimkus Consulting Group Inc v Cammarata* ("*Rimkus v Cammarata*"),[19] it was held that the court should apply the concept of proportionality to the scope of preservation. The court observed that "whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done – or not done – was proportional to that case and consistent with clearly established standards." I would merely interpolate that we do not want to be faced with many cases in which we have to decide (with hindsight) whether what was done and now cannot be undone, was done proportionately. We want to structure the management of claims so that what is proportionate is agreed or decided before searches are done. In

16 No 05cv1958- B, 2008 WL 66932 (SD Calif January 7, 2008).
17 2010 WL 1631519 (SD NY April 20, 2010).
18 2010 WL 3530097 (D MD September 9, 2010).
19 688 F Supp 2d 598, 613 n 9 (SD Tex 2010).

Orbit One Communications v Numerex Corp,[20] the court found the standard set out in *Rimkus v Cammarata*[21] to be "too amorphous" and held that "until a more precise definition is created by rule, a party is well-advised to retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches."

29 Finally, the case of *Pension Committee of the University of Montreal Pension Plan v Banc of America LLC*,[22] which deals with issues of preservation and spoliation, bears mentioning. There is concern about the judge's view that preservation requires collection as opposed to an instruction to, and appropriate follow-up, to preserve and not destroy potentially relevant documents. The judge held that counsel's oral instruction to the plaintiffs was insufficient because it did not direct employees to preserve all documents "nor [did] it provide a mechanism for collecting the preserved records so that they can be searched by someone other than the employee." There is no doubt that particularly under the US regime of train of enquiry disclosure, a requirement for litigants to collect documents as part of preservation would exponentially increase the costs of litigation.

2. Recent developments in Australia

30 On 31 March 2011, the Australian Law Reform Commission ("ALRC") presented to the Attorney-General of Australia its comprehensive review of the law, practice and management of the discovery of documents before the Australian federal courts.[23] There is an interesting proposal to collect empirical evidence of the proportionality of costs associated with the discovery of documents in terms of discovery relative to the total litigation costs, the value of what is at stake for the parties in the litigation and the utility of discovered documents in the context of the litigation.

31 Several interesting recommendations touched on the issue of discovery. In particular, recommendation 6-1 recommends that the Federal Court Rules (Cth) should provide that, before the Federal Court of Australia makes an order for a party to give discovery, a party may apply for

20 2010 WL 4615547 (SD NY October 26, 2010).

21 *Supra* note 17.

22 685 F Supp 2d 456 (SD NY 2010).

23 See Australian Law Reform Commission Final Report, *Managing Discovery: Discovery of Documents in Federal Courts* (25 May 2011) ("ALRC report").

an order that the parties file a practical discovery plan setting out the matters on which the parties agree or disagree in relation to the scope and process of any discovery (*ie*, a discovery plan order). Recommendation 6-8 further recommends that the guidelines on the content of discovery plans should direct the parties to include in a discovery plan:

> (1) the repositories or custodians of documents to be searched in the discovery process;
>
> (2) specific categories of documents, relevant to the crucial issues in dispute, to be searched for in the discovery process;
>
> (3) specific categories of metadata, relevant to the crucial issues in dispute, to be searched for in the discovery process, and the methods used to extract the metadata;
>
> (4) the terms or functionality of any strategies to be used for carrying out a reasonable search in the discovery process—for example, the keywords or concepts to be used in automated searches;
>
> (5) any repositories of documents to be excluded from the conduct of a reasonable search in the discovery process—for example, backup tapes or data recovery systems;
>
> (6) the methods and technologies to be used to de-duplicate discoverable documents;
>
> (7) the methods and technologies to be used to redact privileged documents;
>
> (8) the form in which the party giving discovery will provide a list of documents;
>
> (9) the format in which documents will be produced for inspection—including examples of document management protocols for the production of electronic documents in proceedings; and
>
> (10) a timeframe and an estimate of the costs of discovery.

32 Other aspects of the ALRC report[24] included judicial training, the costs of discovery, and pre-trial oral examinations. As regards judicial training, recommendation 7-1 recommended that the Federal Court of Australia, in association with relevant judicial education bodies should develop and maintain a continuing judicial education and training program specifically dealing with judicial management of the discovery process in Federal Court proceedings. Recommendation 9-2 dealt with the costs of discovery. The ALRC recommended that the Federal Court of Australia Act 1976 should be amended to provide that, without limiting the

24 *Ibid*.

discretion of the court or a judge in relation to costs, the court or judge may make an order that some or all of the estimated cost of discovery be paid for in advance by the party requesting discovery, that a party requesting discovery give security for the payment of the cost of discovery, and may specify the maximum cost that may be recovered for giving discovery or taking inspection. As regards pre-trial oral examination, the ALRC recommended that the Federal Court of Australia Act 1976 (Cth) should be amended to provide that the court may order pre-trial oral examinations about discovery, and that the Federal Court Rules should provide expressly the limited circumstances in which the court may order pre-trial oral examination about discovery (*eg*, to identify the existence and location of potentially discoverable documents; to assess the reasonableness and proportionality of a discovery plan; or to resolve any disputes about discovery).

33 In my view, the ALRC report[25] is an excellent survey with a deep appreciation of the problems of disclosure in the electronic age (and with ideas on how to solve the problems), which makes it a tremendous contribution to the international fund of knowledge. Only two matters struck me as debateable. The first relates to the references to metadata and in particular proposals for search for and extraction of metadata. Although the UK courts used to get hot under the collar about metadata, it is now usually a non issue since parties are generally going to preserve and to produce in native format. We recognise that the metadata which is actually in documents is disclosable as part of the document. Second, the proposals to set up a specific structure for pre-trial oral examination about discovery appears to be uncomfortably analogous to the ubiquitous US deposition procedure, and thus may not be, in my view, the best way forward.

3. Recent developments in New Zealand

34 In New Zealand, the New Zealand Rules Committee has been looking at the reform of the law of discovery for some time and the consultation to the profession on the final draft rules has just been completed. As the draft is confidential, I will limit myself to comment. There is a proposal for standard disclosure as in England but there is also, as

25 *Ibid.*

is now proposed in Lord Justice Jackson's Report on litigation costs,[26] a proposal in appropriate cases for tailored disclosure, that is, an order involving more or less discovery than standard discovery would involve. The circumstances in which there would be a presumption for tailored disclosure is very similar to that proposed by Lord Justice Jackson and in effect his "menu option" ranging from no disclosure to good old train of enquiry disclosure is there as well.

35 I regard this reform as a very important one for e-disclosure because in appropriate cases it will ensure that the court and the parties give positive thought to the scope of disclosure. However, the most important reform from my point of view is the proposed "Discovery Checklist" which has many elements in it similar to those in the e-disclosure questionnaire.

V. FINAL OBSERVATIONS

36 It is perhaps apposite that I end in the antipodes where one could not be further away from the source of the common law system. We, including the courts of this jurisdiction, share the common law heritage and consequently, in some measure, we all share the same problems such as the high level of the cost of litigation and in particular of disclosure. But wherever the jurisdiction, the approaches to the solution have of necessity to be broadly the same:

> (a) The courts must encourage better document management in business, to reduce the future burden of disclosure of electronic documents;
>
> (b) Parties to litigation must better appreciate the concept of proportionality in disclosure and realise that in the world of electronic documents, that will often mean limited disclosure;
>
> (c) Parties to litigation must co-operate and discuss the extent of and scope of search before they search for documents; and
>
> (d) Parties to litigation must tailor their disclosure to the issues that the court has to decide.

---

26 See The Right Honourable Lord Justice Jackson, *Review of Civil Litigation Costs: Final Report* (Norwich: The Stationery Office, 2010).

ELECTRONIC DISCOVERY: AN EVOLUTION OF LAW AND PRACTICE

YEONG Zee Kin
LLB (National University of Singapore),
LLM (Computer & Communications Law) (Lond)

Serena **LIM***
LLB (National University of Singapore)

I. INTRODUCTION

1 The Supreme Court Practice Direction No 3 of 2009 was introduced to provide guidance to litigants on the application of existing discovery rules to electronically stored documents. Practice Direction No 3 of 2009 was eventually inserted into the main body of the Supreme Court Practice Directions ("Practice Directions") as Part IVA ("Part IVA"). In prescribing the rules for the collection and exchange of electronic documents in digital format during the discovery process, Part IVA not only modernises discovery rules and brings the practice of discovery up-to-date, it also encourages lawyers to develop new trial preparation methodologies that keep the evidence in digital format throughout the life cycle of the trial. Part IVA seeks to keep electronic documents in soft copy during the discovery process and to facilitate eventual electronic presentation during trial.

2 Similar to the United Kingdom ("UK") and the United States of America ("USA"), one of the more notable features of Part IVA is the identification of relevant documents using search and indexing technology. This methodology envisages that keyword searches, date ranges and other

* The authors express their deepest appreciation to Brad Mixner for his comments and contributions to this article. Some of the ideas in this article springboard from discussions of the panel on "Electronic Discovery Law and Practice in Singapore & UK" chaired by Yeong Zee Kin, with members: Ms Indranee Rajah, SC, Tan Hee Joek, Brad Mixner and Chris Dale. This article also re-uses some material from Yeong Zee Kin & Shaun Leong, "A Commentary on the Supreme Court Practice Directions Amendment No 1 of 2012" *Law Gazette*, March 2012 and an unpublished paper presented by Yeong Zee Kin at the E-Discovery Exchange Platform 2010. Reference was also made to Tan Hee Joek, "Developments in Law of Discovery of Electronic Documents" *Law Gazette*, November 2011.

criteria are used to identify discoverable documents from identified repositories. The primary imperative for electronic discovery is the recognition of the effective use of technology to counter the increasing costs of litigation resulting from the explosion of evidence, both in volume and in new sources such as email, mobile instant messages, mobile phones, and other electronic storage devices.

3 The potential cost benefits are derived not only from using keyword search engines in place of the manual review of each document. Simply put, search technology is used to winnow the vast amount of data that lawyers will otherwise have to read. Additionally, where electronically stored documents remains in electronic form from beginning to end, litigants are able to enjoy significant cost savings in terms of printing, reproduction, storage and handling costs traditionally associated with exchanging paper or printed documents during discovery and for the trial. This is especially true for document-intensive litigation.

4 Lastly, electronically stored documents contain document metadata. Such metadata, especially if the electronic document is retained in its native format, is useful in several ways – firstly, they can comprise, in themselves, valuable evidence (for example, formulae in spreadsheets, history of editorial changes, document author or creation dates); secondly, they can be used by trial preparation software to generate document indexes quickly and accurately without the need for human input; thirdly, they are supremely useful as search parameters (for example, author, recipient, and date information in emails) to help filter useful information.

5 Part IVA sets *de facto* minimum standards within the matrix of traditional discovery principles. For example, underpinning Part IVA is a fundamental concept that the "original" document *is* the electronic document which is in the client's possession, power or custody, and therefore this is the version (in native digital format and with metadata intact) which should be disclosed and provided for inspection.

6 Since Part IVA took effect on 1 October 2009, there have been a number of decisions in the High Court of Singapore, clarifying misconceptions and providing vital judicial guidance on its scope and operability in specific situations. As the practice of discovery evolves to meet the challenges that come along with the accelerating increase in the corpus of electronically stored documents, so must the existing legal framework be improved upon. Following a public consultation in October and November

2011 by the Rules of Court Working Party, Part IVA was amended in February 2012. This paper discusses the recent development in the law and practice relating to electronic discovery in Singapore, and, where relevant, refers to parallel developments and lessons drawn from the UK and USA experience.

II. OPT-IN: CONFUSION, CLARIFICATION & DISAMBIGUATION

7 One of the unique features of Part IVA is its opt-in framework – this essentially means that Part IVA can apply either by mutual agreement of the parties or by way of an application to the court by a party wishing to opt-in. In the first case to apply Part IVA – *Deutsche Bank v Chang Tse Wen and others* ("*Deutsche Bank*")[1] – the operation of the opt-in framework was put to the test. One party wanted to opt-in; the other did not. It was argued that Part IVA can only be called upon to settle the terms of the e-discovery protocol after both parties have chosen to opt-in. This argument was rejected and Part IVA was applied. The case makes it clear that opt-in means either party opting-in; or to put it in another way, both parties must agree to opt-out. Even in the latter case, it may be presumed that the court can still direct the application of Part IVA, although it would seldom be helpful to do so in such cases.

8 Following the decision in *Deutsche Bank*, the court in *Surface Stone Pte Ltd v Tay Seng Leon and another*[2] ("*Surface Stone*") held that compliance with an inspection protocol would usually be required for inspection of compound documents to ensure proportionate inspection, even if the parties had not opted into Part IVA. The 2012 amendments to Part IVA synchronized it with these jurisprudential developments by removing the term "opt-in" under paragraph 43A(1) of the Practice Directions. This removes any room for confusion that the term "opt-in" may still have posed despite the case law. Hence, the court's power to order the application of Part IVA either on its own motion or on a party's application is now expressly articulated in Part IVA. These amendments unequivocally dispel the misconception that Part IVA is limited only to cases where all parties have consented to its application.

1 [2010] SGHC 125.

2 [2011] SGHC 223.

9 The amendments do not end with the removal of perceived ambiguity presented by the deleted term "opt-in". The inherent benefits of electronically stored documents in native format makes a compelling case for the inspection and supply of electronically stored documents in electronic or native form in all cases involving electronically stored documents. Doing so would enable the litigants to enjoy the inherent productivity benefits of working with electronic documents throughout the discovery, affidavit and trial preparation stages of litigation. To further dispel the apparent "fog of war" and to assist parties and their solicitors in deciding whether electronic discovery should be considered, a list of the types of cases where electronic discovery would be appropriate has been provided in paragraph 43A(1A) of the Practice Directions:

> (a) where the claim or the counterclaim exceeds $ 1 million;
>
> (b) where documents discoverable by a party exceeds 2,000 pages in aggregate; or
>
> (c) where documents discoverable in the case or matter comprise substantially of electronic mail and/or electronic documents.

10 These are cases where technology can most likely assist in increasing the productivity of lawyers and may lead to costs savings for clients. Thus, while Part IVA potentially applies to all civil proceedings in general, parties *should* consider the application of Part IVA if their case falls within one of the categories in the list. By highlighting these categories of cases, what Part IVA seeks to achieve is a change in behaviour: you *should* proceed with electronic discovery under Part IVA unless there are good reasons not to. One may go so far as to posit that for these categories of cases, it is *mandatory to consider* the application of Part IVA.

11 From the perspective of the courts, the cases where Part IVA had been most frequently employed is in suits between banks and customers, where *Anton Pillar* orders have been executed and in contractual disputes where parties had conducted the majority of negotiations using email. From the perspective of electronic discovery practitioners, it is observed that clients consider the following factors in deciding whether to proceed with electronic discovery:

> (a) Whether the amount of electronically stored documents involved is voluminous;
>
> (b) Whether forensic examination of electronically stored documents is anticipated to be necessary; or

(c) Whether document metadata is a source of valuable information or evidence.

1. Volume of electronically stored documents

12 The larger the volume of electronically stored documents, the more likely that Part IVA will be invoked. This is essentially a recognition that there reaches a point where ocular review of documents provides diminishing returns, and technology – which is the progenitor of the exploding volume of documents in the first place – has to be relied on to tame this beast. Electronic discovery has very much to do with increasing the productivity of lawyers and the saving of costs for their clients. This is a matter that the 2012 amendments have recognised. Part IVA now places on litigants a greater obligation to consider its application where the volume of documents exceeds 2,000 pages in aggregate.

13 That is, however, not to say that electronic discovery is suitable only for cases involving voluminous documents. The case of *Deutsche Bank* is judicial authority for the proposition that the electronic discovery framework is beneficial in cases where electronically stored documents form a "substantial proportion" of the total volume of documents, even if the volume of electronically stored documents is, by itself, relatively small ("Small Cases"). However, in practice, litigants are unlikely to invoke Part IVA in Small Cases unless there are other (non-cost related) strategic reasons to do so, as the prevailing perception is that the cost of electronic discovery in Small Cases will often outweigh its benefits in the saving of legal costs associated with lawyer's time spent on ocular review.

2. Forensic examination of electronic documents

14 Where a case requires forensic examination of electronically stored documents to be carried out, the electronic discovery framework would be a natural discovery methodology since the electronically stored documents are already available and accessible in their native electronic form. The cases that have come before the courts, and for which Part IVA has been applied, have predominantly been in the following categories:

(a) Cases where the forensic examination of hard disks has been necessary to recover evidence of, for example, theft or

misappropriation of confidential information where parties involved are likely to be trying to cover their tracks: see *Surface Stone*.

(b) Cases involving the execution of *Anton Pillar* orders which increasingly involve the forensic imaging of hard drives and other portable electronic devices: see *Robin Duane Littau v Astrata (Asia Pacific) Pte Ltd* ("*Robin Duanne Littau*").[3]

3. Metadata information

15 One of the more significant benefits of electronic discovery arises from keeping the electronically stored documents in their native formats with the document metadata intact. This would typically preserve the majority of the system metadata (such as the date of creation, last access and modification of a file) and usually all of the application metadata (such as formulae in spreadsheets; and author, recipient and date information in emails). When electronic documents are produced as hard copy printouts or even in Portable Document Format ("PDF"), this means losing valuable document metadata information. An example of a case where the inspection of metadata was considered is *Fermin Aldabe v Standard Chartered Bank* ("*Fermin Aldabe*"),[4] where the email header information was not produced when emails were provided in PDF format. The plaintiff requested for inspection of the original emails in order to take copies of the email header information.

4. Small Cases

16 While electronic discovery has a large potential to reduce the cost of litigation, there are nevertheless converse hidden costs of deploying electronic discovery which are not part of traditional paper-based paradigms. It has been the experience of electronic discovery practitioners that for lawyers who are new inductees into this area, there is a certain amount of time and cost incurred by clients as their lawyers may not be educated in the nuances in the law, practice and technologies associated with electronic discovery. The education and re-tooling of lawyers is a necessary precursor to lawyers being able to advise on and put into practice

3 [2011] SGHC 61.

4 [2009] SGHC 194.

the electronic discovery methodologies envisaged by Part IVA, such as scoping and crafting an effective protocol or keyword search parameters. Lawyers also need to become comfortable with the technology and software-driven aspects of electronic discovery: from identifying relevant document repositories and specifying the mode of collection and formats of exchange to engaging experts and evaluating outputs.

17 Law practices may also need to acquire requisite document review technologies to assist their lawyers in carrying out their new electronic discovery responsibilities. Just as each modern law office now cannot dispense with a facsimile machine, access to online legal research services like LawNet, email platforms and word processor software, the day is quickly dawning where law offices may need to have at their disposal – whether in-house or otherwise – access to document review platforms and discovery tools for the management of large-volume litigation.

18 One of the areas where lawyers' new skills in electronic discovery can be deployed effectively is the management of disagreements over search terms when these are used as a means of identifying electronic documents for general or specific discovery. It has been held in *Sanae Achar v Sci-Gen Ltd* ("*Sanae Achar*")[5] that where a search term is used to describe a category of documents, the obligations of the party giving discovery are fulfilled once the search is carried out in accordance with the terms of the court order. The same principle applies where search terms are used as part of general discovery: see *Breezeway Overseas Ltd v UBS AG* ("*Breezeway*").[6] Lawyers who are properly informed of the legal obligations and who have an understanding of search and indexing technology will be in a position to avoid protracted arguments over keyword selections, privilege review methodologies, *etc*. This will avoid prolonging discovery and thereby control costs.

19 The experience of the UK and, in particular, the USA, demonstrates how costs associated with electronic discovery can spiral out of proportion to the size of the claim. Proper project management of electronic discovery in litigation has a large potential to influence overall litigation costs. In these early days of adoption of Part IVA, it is not surprising that the presence of these factors may have caused a perception amongst litigation

5 [2011] 3 SLR 967; [2011] SGHC 87.

6 [2012] SGHC 41.

practitioners that the costs of electronic discovery is disproportionate to its benefits, in particular for Small Cases.

20 Some of these perceptions will naturally diminish over time, as litigation practitioners and their support paralegals make their way up the learning curve, acquiring new skills in managing electronic evidence as well as competence in the use of litigation support software; and generally becoming more familiar working within the electronic discovery environment. To accelerate the development of electronic discovery expertise in Singapore, it may be apposite to consider the establishment of an active support group of independent electronic discovery practitioners and litigation support specialists. Part IVA is less than 3 years old, and the electronic discovery regime in Singapore will, no doubt, continue to mature and evolve through refinements and developments in the law and industry practices.

III. IN PRAISE OF GOOD FAITH COLLABORATION

21 The other aspect in Part IVA that practitioners faced initial difficulties with was the exhortation for good faith collaboration. These words do not sit well with litigators steeped in an adversarial tradition. The experience thus far has been that if parties collaborate at all, this is usually limited to agreement on procedural issues (with the courts' guidance) during pre-trial conferences, such as agreeing on soft copy formats to be used and the time and place for inspection. But the case of *Fermin Aldabe* demonstrates that oftentimes, there are very practical reasons to do so: in that case, the method of exchanging soft copy documents and the file formats to be used all had to be discussed with the relevant technical employees of the client bank. In dialogues of this nature, lawyers can play a facilitative role but the participation of the employees of the client with the correct technical know-how is crucial.

22 The benefits of good faith collaboration were first elaborated in *Deutsche Bank*:[7]

> … the time spent in discussing the ambit of general discovery will result in a better understanding of what categories of documents the opposing party considers to be discoverable in this matter. This may avert or reduce subsequent requests and applications for further discovery (if there is

7 *Supra* note 1, at [38].

> agreement or compromise), or at the very least serve to accelerate such applications since parties will know at a fairly early stage their respective positions on entitlement to disputed categories of documents. In either case, there is the potential of saving time and costs in the discovery process. …

23 The need for parties to collaborate and to agree in good faith was further emphasised by Lee Seiu Kin J in *Sanae Achar*:[8]

> … it would be best if the parties can, prior to any search, agree on which search engine or software is to be used, the preparation of the search engine prior to conducting the searches (eg, updating the search index or causing a fresh search index to be made) and how searches are to be conducted. This would minimise potential disputes as to whether the parties have discharged their discovery obligations.

24 Hence, the parties in *Robin Duane Littau* were similarly directed to conduct collaborative discussions in order to agree on a list of keywords to be used in the search for relevant documents.

1. Encouraging good faith collaboration

25 In a good faith discussion of electronic discovery issues, the electronic discovery protocol template in Part IVA provides a *de facto* check list of areas to traverse. When carried out in the right spirit, it also places both parties' cards on the table insofar as the expected scope of discovery is concerned. This was clearly demonstrated in the *Deutsche Bank* case where the draft electronic discovery protocol annexed to the summons application set out very clearly what the defendants expected the bank to provide. Even though the bank's costs incurred in preparing a set of documents for disclosure was not thrown away, it was nevertheless ordered that part of the protocol stood as a request for further or specific discovery. Hence, the protocol not only provided an insight into the expected extent of discovery, it also accelerated the next stage of discovery.

26 In order to provide further assistance to parties in their good faith discussions and to facilitate agreement on issues relating to the discovery and inspection of electronically stored documents, a checklist of questions was introduced in Appendix E Part 1 as part of the 2012 amendments to Part IVA. This is a detailed checklist of issues which the parties should address in their good faith discussions. The checklist contains helpful

8 *Supra* note 2, at [23].

guidelines that introduce or highlight industry best practices and technologies which parties are recommended to consider for more efficient and cost-effective electronic discovery.

27 An obligation is also placed on counsel to complete the checklist with their clients and exchange responses before meeting for good faith discussions. This complements the amendments in paragraph 43B(1) of the Practice Directions, where parties are expressly encouraged to collaborate in good faith and agree on issues relating to the discovery and inspection *within two weeks after the close of pleadings*. Parties are encouraged to have regard to the checklist in their good faith discussions.

28 The introduction of the checklist takes discovery another step further from its adversarial roots, into a more collaborative atmosphere necessitated by the enormity of the task. As has been observed of the exchange of draft electronic discovery protocols in *Deutsche Bank*,[9] the exchange of the checklist will, even where consensus is not reached in all areas, provide both parties with a preview of what their adversary considers to be discoverable.

2. Areas to be traversed in good faith discussions

29 It is hoped that with the introduction of the checklist, parties will be able to agree on an electronic discovery plan without the intervention of or resort to the courts. This measure follows a similar approach adopted in the UK where the "Electronic Documents Questionaire" – which was initially disclosed in *Goodale & Ors v The Ministry of Justice & Ors* ("*Goodale*")[10] – was eventually published pursuant to The Civil Procedure Rules 1998 ("the UK CPR")[11] as Practice Direction 31B in the UK.

30 It has been the experience of electronic discovery practitioners that for parties' good faith collaboration to achieve proper search methodology, the following issues have to be addressed during the good faith discussions:

> (a) The physical or logical locations, media or devices that the search should cover. Generally, keyword search should not reach into unallocated space unless discovery of the recording device had been

9 *Supra* note 1.

10 [2009] EWHC B41 (QB).

11 The Civil Procedure Rules 1998 No 3132 (L 17) (UK).

given and an order for forensic inspection obtained: see *Robin Duane Littau*;[12]

(b) The reasonable time periods in which the electronic documents were created, received or modified for the search to cover: see *Sanae Achar*;[13]

(c) The specific keywords to be deployed in the search for relevant documents – the test of relevancy in the selection of keywords is determined through the substance of the parties' pleaded case or allegations: see *Sanae Achar*;[14]

(d) The capabilities of the search engine or software to be used to conduct the search: see *Sanae Achar*[15] and *Robin Duane Littau*;[16]

(e) The format in which copies of documents should be provided, and the arrangements for inspection of the same.

3. Good faith collaboration and discovery in stages

31 Another benefit of good faith discussions is the possibility of managing the scope and extent of general discovery. In *Breezeway*,[17] parties had engaged in good faith discussions that did not result in any agreement. However, the process sharpened the issues and when the application under Part IVA for the adoption of an electronic discovery protocol came up for hearing, it was possible for the court to order that discovery be carried out in stages.

32 The approach in conducting discovery in stages is outlined in *Breezeway* as follows:[18]

> **How discovery may be conducted in stages**
>
> 9 Conducting discovery in stages requires that parties identify at the close of pleadings both the issues in dispute and the witnesses that are key to these disputed issues. For the purpose of electronic discovery, these witnesses are referred to as custodians: an emphasis on their role as custodians of both

12 *Supra* note 3, at [29].
13 *Supra* note 5, at [19] and [21].
14 *Supra* note 5, at [17].
15 *Supra* note 5, at [23].
16 *Supra* note 3, at [26].
17 *Supra* note 6.
18 *Supra* note 6, at [9]–[11].

> knowledge of the relevant facts as well as custodians of the relevant documents.
>
> 10 Once the key custodians are identified, attention is turned to the repositories of electronic documents in their possession, custody or power. The repositories will typically include their e-mail accounts, hard disks on their desktop and notebook computers, removable storage media, online storage locations on the network, etc. …
>
> 11 Having identified the custodian and the repositories, it is open to parties to either identify the relevant storage media or folders within storage devices (eg hard disks) to be disclosed or parties can agree that a reasonable search be conducted on the identified repositories. …

33 The benefits of conducting discovery in stages, in this case at least, were that it enabled the scope of discovery to be managed by confining it to the key witnesses – or custodians – and identified repositories in their possession, such as online profiles, email accounts and notebook computers. In so doing, it was possible to address the problem of proliferation of copies of the same electronic document in the possession of multiple custodians by confining discovery initially to the key witnesses or custodians. As was observed in the UK case of *Goodale*:[19]

> In terms of a search one should always start with the most important people at the top of the pyramid, that is, adopt a staged or incremental approach. Very often an opposing party will get everything they want from that without having to go down the pyramid any further, often into duplicate material.

34 At the end of the initial stage, parties may decide whether to proceed with a subsequent stage or agree that general discovery is complete. Adopting such an approach does not shut the door on specific discovery for, for example, "train of inquiry"[20] documents.

IV. COLLECTION AND PRESERVATION OF ELECTRONIC DOCUMENTS

35 One of the issues that litigation practitioners routinely grapple with, and which has an impact on the litigation budget, is whether or not the data should be forensically collected. Forensic collection entails the use of forensic software to create an image of the media. The advantage of a

19 *Supra* note 10, at [22].

20 Or the *Peruvian Guano* test, see *The Compagnie Financiere et Commerciale du Pacifique v Peruvian Guano Company* (1882) 11 QBD 55.

forensic collection is that it produces a forensic image of the entire hard disk, capturing both the active and deleted data.

36 A distinction needs to be drawn between a forensic collection and a forensic investigation. While it is not the norm today, the day may soon come when most IT professionals (whether in the client organisation or law firm) will have ready access to software tools that can make a forensic image of the recording device or storage medium. It would be good practice to make a forensic image – a forensic collection – and to work off copies of the forensic image. This will enable the proper preservation of the original electronic documents.

37 Unless the requisite expertise is available within the client organisation or law firm, a forensic collection oftentimes entails the engagement of an external forensic expert trained in the employment of forensic tools. In such cases, the external forensic expert's costs will add to the overall cost of litigation.

38 On the other hand, a forensic investigation into the data using forensic tools is undertaken where authenticity or authorship of the documents is an issue. In these situations, the external forensic expert is required, not only for his specialist skills in data investigation, but also for his eventual role as an expert witness. Where a forensic investigation is required, it would be prudent to engage an external forensic expert for this latter reason.

39 The current state of affairs is such that the ability to conduct a forensic collection is not within the knowledge and skill of most IT professionals. The question therefore is whether a forensic collection should be considered for all cases. Since an external expert needs to be engaged, it may not be proportionate in all cases to conduct a forensic collection having in mind the costs that would have to be incurred, particularly when the issues in dispute do not require forensic data investigations. For the present, the balance ought to be struck in favour of requiring a forensic collection only when the issues in dispute point to the potential need for forensic data investigation. For the majority of cases, a forensic collection would probably not be necessary although it remains, if achievable at reasonable costs, a prudent measure.

1. Forensic collection *vs* forensically sound collection

40 This approach finds support in *Deutsche Bank*, where caution was sounded against the automatic association of forensic collection with the preservation of evidence:[21]

> … It is not in every case that forensic techniques are required for the preservation of evidence when litigation is contemplated or when litigation has commenced. … It may oftentimes be sufficient to make a copy of potentially discoverable documents in an optical read-only medium (eg CD or DVD RW discs) and to take care not to delete the originals. Once the cost of forensic acquisition is obviated, the purportedly high cost of electronic discovery diminishes significantly. To draw an analogy with discovery of paper documents, one would not employ forensic techniques to preserve paper documents and look for fingerprint evidence in every case. …

41 The opposing view makes an argument on the grounds of prudence and necessary precaution – that a forensic collection should always be undertaken because an issue of deleted data could arise at a later stage in the trial, or events at the trial could transpire to make a search of deleted data a necessity.

42 The alternative to a forensic collection is a "forensically sound collection" of active data, which preserves the metadata of the collected data and follows best practices for data collection and preservation, such as documenting the chain of custody and hashing the dataset for the purposes of identification and verification.

43 In a collection of electronically stored documents from a server (or other shared storage media) containing data belonging to custodians as well as non-custodians, a targeted collection of the shared drives containing the custodian's data conducted in a forensically sound manner will often suffice, and may in fact be the only "reasonable" mode of data collection given the need for proportionality. However, where the data is sitting in a single desktop or laptop computer, the cost of a forensic collection of the hard drive may be only slightly higher than the cost of a forensically sound collection. For this reason, a forensic collection may well be advisable in those circumstances.

44 Lastly, the identity of the custodian and the importance of the documents in his possession to the issues at the trial is another qualifying factor when considering if a forensic collection is a reasonable expense.

21 *Supra* note 1, at [24].

Undertaking a forensic collection of documents belonging to key custodians is justifiable as the evidence is more likely to have a bearing on the outcome of the trial. Less critical custodians may only require a forensically sound data collection approach.

2. Failure to preserve and its consequences

45 A discussion of collection cannot be complete without discussing the issues relating to the preservation of evidence. To round off the discussion, we have to touch on two High Court decisions that speak of the consequences of the failure to preserve electronic evidence: *Alliance Management SA v Pendleton Lane P and Another* ("*Alliance Management*")[22] and *K Solutions v National University of Singapore* ("*K Solutions*")[23]. The issues raised by the ephemeral nature of digital evidence and the consequences of destruction – whether accidental, intentional or deliberate – are better dealt with in a more in-depth article. For the present discourse, focus need only be placed on the consequences of the failure to preserve. The analysis in *K Solutions* suggests that there can be at least three categories of destruction: accidental, intentional and deliberate.

46 The most egregious form would be deliberate destruction, where destruction is accompanied with the intent to put the documents out of reach of the other. In this most extreme case of misconduct, even where a fair trial is possible, the court has powers to dismiss or strike out the case. In *K Solutions*, the plaintiff was found to have deliberately destroyed emails with the intention of concealing them from the defendant. It mattered not that this was done before litigation commenced or that these documents were potentially available for other repositories. Its case was dismissed.

47 That leaves accidental and intentional destruction. Not much light was thrown on these, but there were *obiter dicta* to the effect that "intentional" does not mean "accidental".[24] Pending judicial clarification, it may be postulated that routine (and planned) destruction in accordance with a file destruction policy would amount to intentional destruction; while accidental destruction would be what takes place where, for example, a document is copied and in the process some of the system metadata (such

22 [2008] 4 SLR(R) 1; [2008] SGHC 76.
23 [2009] 4 SLR(R) 254; [2009] SGHC 143.
24 *Ibid*, at [107].

as file creation, access and modification dates) are modified. For these latter categories of destruction, the court will consider whether a fair trial is still possible and if so, whether the failure to produce evidence may be addressed by, for example, making an adverse presumption against the party that fails to produce it under section 11(g) of the Evidence Act.[25] Another step up in culpability would be for the pleadings to be struck out as in the *Alliance Management* case, where the defendant was found (by the Court of Appeal) to be in possession of the original hard disk but it deliberately and persistently failed to produce and return the said hard disk, despite prior orders of court to do so. Instead, the defendant sought to challenge the finding collaterally. This was held to amount to contumelious conduct and an abuse of the court's process. Its defence was struck out.

V. PROPORTIONATE AND ECONOMICAL DISCOVERY – MANAGING SCOPE AND COSTS OF DISCOVERY

48 Practitioners are probably familiar with the approach taken by the courts in ensuring that, for the numerous discovery applications that come up for hearing, orders for discovery are proportionate. Proportionality, although not articulated as a fundamental principle like in the UK CPR, is nonetheless recognised, in practice as much as in jurisprudence, to be a fundamental tenet of the Rules of Court in Singapore. In this regard, the *zeitgeist* of Order 24 of the Rules of Court[26] – *viz* proportionate discovery – is made manifest in the 2012 amendments. Paragraph 43A(1) of the Practice Directions has been amended to clarify that Part IVA is intended to provide "a framework for proportionate and economical discovery".

49 This theme is carried through to the introduction of a definition of "not reasonably accessible documents" in Part IVA – *ie*, backup tapes, and deleted files or file fragments recoverable by using forensic tools[27] – and the adoption of a two-tiered approach when a reasonable search is requested. At first instance, "requests for reasonable searches shall not extend to electronically stored documents which are not reasonably accessible".[28] Similarly, general discovery will, generally speaking, not include documents which are not reasonably accessible. It has also been provided in the

25 Evidence Act (Cap 97, 1997 Rev Ed).

26 Rules of Court (Cap 322, R 5, 2006 Rev Ed).

27 See Part IVA, paragraph 43A(4).

28 See Part IVA, paragraph 43D(2).

electronic discovery plan that such non-reasonably accessible documents are not within the scope of general discovery.[29]

50 Should the party requesting for discovery seek an extension of the reasonable search to documents which are not reasonably accessible, he "must demonstrate that the relevance and materiality of the electronically stored documents justify the cost and burden of retrieving and producing them".[30] In other words, it is insufficient that the documents sought are merely relevant: they must be shown to be material to such an extent as to justify the costs and burden of retrieval. Thus, if the piece of evidence is sufficiently material to warrant the expenditure of such resources, it is possible to turn up every stone in search for it.

1. Reasonable searches: proportionality and productivity

51 With the vast proliferation of emails and electronic documents in the past decade, there has been a dramatic increase in the creation of massive volumes of electronic documents, so much so that ocular review of printed documents would (if at all possible) no longer be practicable in terms of time and costs. It would not be surprising for a large corporation to generate and receive millions of electronically stored documents in a day.[31] Where the traditional filing cabinet could store hundreds of paper documents, an external hard disk the size of a note book could store the equivalent of millions of paper documents, and it is not uncommon for companies to store hundreds of such hard disks in their archives.[32] To add on to the challenge, electronically stored documents can be easily and quickly duplicated. For example, the same email can be forwarded multiple times along an email chain in a matter of minutes. Furthermore, electronically stored documents are incredibly persistent – documents that have been "deleted" continue to exist and are retrievable. This adds on to the vast accumulation of overall information found in a recording device or database.

52 In the face of such challenges, the time expended and costs incurred in the physical handling, management, and manual search and review of

29 See Practice Directions, Appendix E Part 2, paragraph 1(c).

30 *Ibid*.

31 See generally, The Sedona Conference Working Group 7, *The Sedona Canada Principles: Addressing Electronic Discovery* (January 2008) at p 2.

32 *Ibid*.

relevant information from the printed copies of these voluminous electronically stored documents would be unsustainable, and worse, may even exceed the amounts at stake in the claim. In this regard, the use of keyword search terms and search engines, which provide a convenient and efficient method for identifying relevant and necessary documents, can result in much time and costs being saved. As Lee Seiu Kin J observed in *Sanae Achar*:[33]

> … One of [Part IVA's] objectives is to promote the exchange of electronically stored documents in a text searchable electronic form (in lieu of printed copies) so that parties may capitalise on the twin benefits of digitisation, viz, the ability to run keyword searches on the documents in question as well as easy management of the same. …

2. Reasonable searches: not to be confused with a reasonable search

53 The *raison d'être* for the concept of a reasonable search in Part IVA is to ensure that the principle of proportionality is adhered to. The search for electronic documents using search terms formulated by keywords and search parameters has to be reasonably constrained:[34]

> … The term "reasonable search" as it is used in Part IVA should not be confused with a similarly named concept under the UK Civil Procedure Rules, which is used to denote a search for documents, electronic or pulp, for the purpose of disclosure. Under Part IVA, the term "reasonable search" means that the keyword search for electronic documents has to be reasonably constrained by, at least, limits on the time period and the number of repositories of electronic documents. …

54 The constraints were further elaborated in the following manner in *Breezeway*:[35]

> …
>
> (a) First, parties have to decide whether the entire storage device (eg hard disk) or storage medium is to be searched, or only certain folders and sub-folders. For hard disks, parties should usually identify the relevant folders and sub-folders as modern operating systems usually establish a set of folders where documents are stored. This will obviate the necessity of searching a multitude of folders where operating system, application software, library and configuration files are stored.

33 *Supra* note 5, at [11].

34 *Supra* note 3, at [22].

35 *Supra* note 6, at [12].

(b) Second, parties have to agree on the time period during which the relevant documents were created or received. This will serve to exclude documents responsive to the search term but which are likely to be irrelevant. The time period may differ for different key words, repositories or custodians.

3. The proper use of search terms

55 With the explosion in the volume of potentially discoverable documents, it was observed in *Sanae Achar* that "the traditional manner in which discovery has been carried out is proving increasingly inefficient in achieving the purposes for which the discovery process was developed."[36] The answer to the exploding volume lies in modern search and indexing technology. The benefits are succinctly put in the following manner in *Breezeway*:[37]

> … parties need not manually trawl through heaps of printed documents in order to identify relevant documents and weed out irrelevant ones. Running simple keyword searches using easy-to-use desktop search engines would suffice. …

56 Part IVA was relied on in *Sanae Achar* for a specific discovery request, wherein search terms were used to describe the category of electronic documents for which the request for specific discovery was made. After determining the relevant search terms and limits which were required by Part IVA to be imposed, Lee Seiu Kin J went on to hold that the party carrying out the search would have fulfilled its obligations once the search was conducted to the extent ordered and documents locates as a result of that search are disclosed. The courts would be tolerant that it is possible that relevant documents, but which are not responsive to the search terms ordered, may not be caught by the search engine employed. Lee Seiu Kin J endorsed[38] the point made by Jacob LJ in *Nichia Corporation v Argos Limited* ("*Nichia*")[39] and articulated in *Digicel (St Lucia) Ltd and Others v Cable & Wireless Plc and Others*:[40]

36 *Supra* note 5, at [13].
37 *Supra* note 6, at [14].
38 *Supra* note 5, at [23].
39 [2007] EWCA Civ 741 at [50]–[52].
40 [2008] EWHC 2522 (Ch) at [46].

> … [T]he [discovery] rules do not require that no stone should be left unturned. This may mean that a relevant document, even 'a smoking gun' is not found. This attitude is justified by considerations of proportionality. …

57 The cases have therefore drawn a distinction between relevance and the fulfilment of a party's discovery obligations. Where search terms are used – whether during general discovery or in requests for specific discovery – there is no need to review the search results for relevance. A party's discovery *obligation* is fulfilled once the search is conducted in accordance with the search terms and limits agreed or ordered.

58 The 2012 amendments to Part IVA adopt this statement of law in *Sanae Achar*. Thus, a party responding to a discovery request to conduct a reasonable search need not review the search results for relevance provided that he has carried out the reasonable search to the extent stated in the request.[41] Following the conduct of a keyword search, we are no longer concerned with the relevance of the search results, thereby obviating the need for a tedious further review of search results for relevance. Nevertheless, a privilege review may be conducted within a reasonable time by the party giving discovery, to ensure that privileged matter is not inadvertently disclosed to its opponent. This potentially renders the painstaking – and time consuming – trawling through of electronic storage media and repositories for discoverable material a thing of the past.

59 Another area where search terms have been held to be necessary is when there is a request for discovery of a compound document like a recording device or storage medium. In *Surface Stone*, it was observed that:[42]

> … where an applicant seeks specific discovery of a compound document, such as [a hard disk], the essential document(s) sought to be discovered is not the compound document itself (as it serves only as a storage medium), but the discrete documents found within the compound document. …

60 It will therefore be necessary for the documents sought to be described with sufficient specificity. This may be done either descriptively or with the use of search terms, with the latter being the more pragmatic measure.

41 See Part IVA, paragraph 43D(3).

42 *Supra* note 2, at [51].

4. Crafting search terms

61 It is in the context of the use – or abuse – of search engines and indexing technology for carrying out discovery that the issues of proportionality and costs are most frequently encountered. Not surprisingly, there are litigants who seek to use search terms designed to catch as many documents as possible. It has therefore been observed that:[43]

> In selecting keywords and formulating search terms, we ought to guard against the tendency to cast as wide a net as we can in order to obtain the highest number of documents in the search results. This has emerged as a pattern of behaviour in certain types of cases, where the party seeking discovery tries to use searches to draw out as many documents as possible from his adversary, with the hope that he may find the proverbial smoking gun. That would, to my mind, be tantamount to trawling or the emptying out of the adversary's filing cabinets while hiding behind the mask of search terms.

62 USA courts have recognised the difficulty of crafting keyword selection for the purposes of electronic discovery. As may be noted from Magistrate Judge John M Facciola's dire warnings in *United States v O'Keefe*:[44]

> Whether search terms or 'keywords' will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics. … Given this complexity, for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread. This topic is clearly beyond the ken of a layman…

63 This approach was also endorsed by other American judges including Magistrate Judge Paul W Grimm in *Victor Stanley Inc v Creative Pipe Inc*.[45] The courts in Singapore have, nevertheless, bravely ventured where angels fear to tread by providing judicial guidance on keyword search selection for electronic discovery. The following signposts have been planted to assist in navigating the maze of search term formulation.

64 First, the formulation of search terms by the selection of keywords and appropriate search operators has to be carried out with reference to the pleadings and the issues in dispute.[46]

---

43 *Supra* note 6, at [25].

44 537 F Supp 2d 14 (Maryland District Court, 2008) at [24].

45 269 FRD 497 (Columbia District Court, 2008).

46 *Ibid*.

65 Additionally, the following approach was espoused in *Breezeway*:[47]

(a) Commence with specific keywords before expanding to consider broader terms. Specific keywords would include unique reference numbers like bank account numbers and file reference numbers, names of specific projects, keywords like email addresses, contact numbers, names and initials that identify individuals.

(b) Broader keywords would depend very much on the facts of the case. For example, search terms may be formulated based on instructions from clients relating to significant events or locations. Similarly, key words that are unique to the facts of the case, such as product names and unique terms or phrases, may be used.

66 Words that are commonly used, either in normal daily usage or in the context of the industry that forms the factual backdrop of the dispute, should be avoided. The reason is obvious: this is to avoid a situation where an inordinately large number of documents are returned as part of the search results. This would defeat the purpose of making use of keyword searches.

67 Similarly, keywords which commonly form part of a word should be avoided or should only be used where the search engine is capable of identifying their occurrence as a discrete word and not as part of the word.

68 Finally, preliminary searches intended solely for the purpose of identifying the number of hits (*ie*, instances of documents which corresponded to the keyword) are likely to be very helpful in determining whether a particular keyword should be permitted or how it should be modified or constrained. Certainly, the number of hits returned in the preliminary search results does not have any bearing on relevance. However, they may be helpful in determining whether a particular keyword is unsuitable, as too many hits would indicate that a proposed keyword is too broad or generic, and needs to be refined or restricted.

69 This is a practical and pragmatic approach, and litigation lawyers should include these recommendations in their list of "dos and don'ts" in keyword selection. When it comes to the delicate balance between perfect justice and (affordable) access to justice, the courts in Singapore have shown themselves to be pragmatically inclined towards the latter.

47 *Supra* note 6, at [28].

70 Given the imperfections of keyword search selection and results, the recommended approach to cost-effective electronic discovery lies in parties adopting a commonsensical approach towards keyword selection, including a tolerance level for such imperfections. It cannot be gainsaid that the most effective way to contain electronic discovery costs is never to take a unilateral approach to the keyword selection process, and to recognise that your client is best served by taking a collaborative approach to keyword selection and other electronic discovery arrangements with the adversary.

5. Conducting reasonable searches

71 In carrying out searches, the case of *Robin Duane Littau* prescribed a three stage process:

> (a) The relevance of key words is determined with reference to the pleadings. In determining the search term to be used, the capabilities of the search engine would be a relevant consideration. For example, the availability of proximity search capability may permit the formulation of a more useful search term. Parties should also conduct a preliminary search using the disputed keywords, as the number of hits (or lack thereof) will be a relevant consideration in determining whether a keyword is suitable or in formulating search terms.
>
> (b) The search is conducted using the search terms as agreed or ordered. In the usual case, the search will be carried out on the identified repositories and should not extend to unallocated spaces on the recording device or storage medium.
>
> (c) After the search is conducted, the party giving discovery will be given time to conduct a review to identify privileged documents over which he may wish to assert privilege or documents containing privileged information which he may wish to redact.

72 It was also noted in *Sanae Achar* that parties should agree on the search engine to be used and how it is to be prepared (*eg*, re-indexing) before the search proper is conducted.[48]

73 The underlying premise in Part IVA is the notion that keyword searches provide a convenient and efficient method for identifying discovery

48 *Supra* note 5, at [26].

documents. The question then arises as to whether the keyword search results should be subject to further human review for relevance.

74 While Part IVA is silent on this point, the High Court in the cases of *Sanae Achar*[49] and *Robin Duane Littau*[50] clarified that there is no necessity for ocular review for relevance, where parties have mutually agreed to the search terms, and a proper search has been conducted pursuant thereto. This approach obviates the necessity for a further review of search results for relevance. However, a review for "privilege" may be undertaken within a reasonable time by the party giving discovery to ensure that privileged information is not inadvertently disclosed to the opposing side.

6. Imperfections of keyword searches

75 The reason for not requiring ocular review is a pragmatic one which recognises that the volume of electronically stored documents has grown exponentially huge, that the cost of litigation would be prohibitive (and access to justice denied to litigants) if litigation lawyers continued with the traditional paper-based approach of eyeballing every single piece of electronically stored document.

76 The courts recognise the imperfections of keyword searches and have acknowledged the possibility that keyword searches may lead to irrelevant documents being included and relevant documents being excluded. The call for pragmatic acceptance of such imperfections has been articulated in the cases of *Sanae Achar* and *Robin Duane Littau*.

77 In *Sanae Achar* (a case involving specific discovery), it was held that parties would have satisfied their specific discovery obligations in respect of electronic documents retrieved pursuant to an agreed keyword search, notwithstanding that there could well be other relevant electronic documents not caught by the search.[51] In *Robin Duane Littau* (a case involving general discovery), the court held that documents which are uncovered through the search of relevant keywords (either agreed by parties or ordered by the court), less those that are privileged or otherwise unnecessary for disclosure, would form part of general discovery without a further need to review for relevance. However, this did not bar parties from

49 *Supra* note 5, at [23].

50 *Supra* note 3, at [32].

51 *Supra* note 38, and the discussion in the accompanying main text.

applying subsequently for specific discovery of further documents under the "train of inquiry" concept and possibly through further keyword searches where necessary.

78 While it is still open to parties to mutually agree to an electronic discovery plan which provides for ocular review of the documents for relevance, the default position which the courts in Singapore have adopted is very clear. In this regard, the courts in Singapore are perhaps mindful of the USA experience where electronic discovery has had the adverse effect of increasing the cost of litigation, despite good intentions to the contrary. Unfortunately, affordable justice does come at the price of perfect justice, and the challenge is to find a balance that works.

7. Summary of when keyword searches may be used

79 Search engines and keyword searches are useful in many aspects of the litigation life cycle. In Part IVA, keyword searches may be executed as part of the electronic discovery plan. In this case, the keywords are mutually agreed between parties and executed by a search operator. Unless the plan specifically provides otherwise, parties' obligations for general discovery can be discharged by the conduct of the keyword searches in accordance with the terms of the plan and the documents identified by the search are deemed to be relevant and no further human review for relevance is necessary. Search methodologies at this stage include a mix of keyword searches through full text or selected fields, agreed filters and search parameters, as well as Boolean searches.

80 Even where general discovery was conducted in the traditional fashion, Part IVA allows a party seeking specific discovery to make a request by using search terms to describe a category of electronic documents. It was in the context of the use of reasonable searches to describe categories of documents in a specific discovery request that the seminal case of *Sanae Achar* was decided.

81 Keyword searches may also be preceded by a "preliminary search", which is executed for the sole purpose of identifying the number of hits against each keyword, but without (at this stage) the right to review the underlying documents shown up in the search result. This "preliminary

search" approach was suggested in *Robin Duane Littau*[52] to identify search terms that are irrelevant or too broad (or, bringing up too many hits), and should be conducted using the list of disputed keywords before a contested application under Part IVA comes up for hearing.

82 Keyword searches may also be performed by clients with their solicitors for the purpose of identifying documents that are potentially discoverable. This may be conducted unilaterally during the time before the service of the list of documents, or even before the commencement of the action. It is not uncommon, in the context of employer-employee disputes involving the misuse of confidential information, that keyword searches may be conducted by the employer at an early stage to identify the existence of relevant or incriminating evidence in the computer used by the errant employee. The nature and purpose of such searches are investigative, and conducted at preliminary stages for the lawyer to assess and deduce the possible causes of action.

83 Early case assessment tools provide search analytic information which may be invaluable in enabling clients and their lawyers to analyse the dataset quickly, prioritise areas to be reviewed, assess the strength of their evidence and locate pivotal documents quickly. Search technologies deployed at early stages – before the writ is filed – enable litigants to master their evidence faster, as an early synopsis of the custodians, volumes, keywords *etc*, is now available to them. The algorithms deployed in modern search engines are increasingly sophisticated and are even able enhance the keyword list by fetching relevant documents based on relevant documents that were previously adduced. These smart search engines have become increasingly commonplace in the genre of electronic discovery technology called early case assessment software. Most early case assessment software deploy fuzzy searching (based on exact keyword matches as well as similarities), concept searching (based on an analysis of the words in the documents that the keyword search has retrieved), synonym searching (based on synonyms of your selected keyword search terms), machine assisted searching (based on an analysis of the documents that you have previously identified as being relevant).

84 Although the employment of such early case assessment tools is solely at the cost (at least initially) of the plaintiff since they are intended to assist in his assessment of the strength of his case based on the evidence that he

52 *Supra* note 3, at [19] to [21].

can muster, the day may soon arrive when a successful plaintiff may attempt to recover such costs as part of his party-and-party costs. In the context of the use of broad keywords by a party unilaterally, in order to discharge his discovery obligations, it has been observed in *Breezeway* that:[53]

> … a party makes use of search terms to identify documents which he then puts through a process of review in order to identify discoverable document as a means of discharging his discovery obligations … As he is not imposing this on his adversary, he can choose to manage the discovery of his own documents in any manner he deems necessary. However, there may potentially be the question whether, if he had adopted a patently inefficient and resource-intensive method of managing discovery, the entire costs of the discovery effort ought to be recoverable as part of party-and-party costs. …

VI. INSPECTION

85 Part IVA mandates that the party producing electronic documents for inspection shall also provide reasonable means and assistance for inspection of such documents in their native format. Practically this means that the party providing discovery has to provide a computer for the inspecting party to review the electronic documents.

86 In *Fermin Aldabe*, the inspecting party requested inspection of emails in native format in order to view the email header information which would show the routing history of the emails. The court rejected the submission that inspection of electronic documents could be satisfied by the mere provision of electronic copies or printed copies. To address the concerns of the party providing discovery that privileged or confidential information may be disclosed, the court recommended the following inspection framework:[54]

> (a) reasonable access will be provided to the emails which are to be produced for inspection;
>
> (b) the inspection will be carried out in the presence of parties and their solicitors;
>
> (c) the party providing discovery will provide an operator who will retrieve and call up the emails which have been identified for inspection and to present the emails on screen;

53 *Supra* note 17, at [26].

54 *Supra* note 4, at [43]

(d) the inspecting party may request for the display of hidden or non-visible metadata information such as header information. However, the party providing discovery will be entitled to seek advice on privilege, banking secrecy or any other basis for objection before giving instructions to the operator to present the metadata information on screen for inspection.

87 Where copies of discoverable electronic documents have been delivered in their native format with metadata intact, the need for inspection is minimal as there is very little that an inspection will disclose which is not already available in the soft copy. For this reason, inspection may, as a matter of practice, be deferred by agreement between the parties, with the parties reserving the right to inspect later where necessary.

1. Inspection of electronic documents: is this necessary?

88 One of the areas which Part IVA sought to improve is how electronic documents are enumerated in the list of documents. Increasingly, the current form of a list of documents, as a relic of the past, is stressed and strained when shoehorned to conform to modern discovery practices. A bolder approach in tackling the issues attendant to enumerating electronic documents in the list of documents has slowly been developing, and has now found its place in the 2012 revision of Part IVA. Consider the difficulties the enumeration of emails caused in the *Fermin Aldabe* case where parties ended up quarrelling over how to properly list emails, particularly email chains. This was compounded by the fact that email chains were produced in PDF documents.

89 The *Fermin Aldabe* case was also notable for the issues that surfaced in relation to the inspection of electronic documents. How does one actually inspect an electronic document – in this case, emails and their header information? A balance has to be struck between inspection of a document and inspection of the entire email account, which is tantamount to inspection of a database, with its attendant concerns of trawling and privileged material. Part IVA does require that reasonable means and assistance ought to be provided. In *Fermin Aldabe*, "reasonable means" translated into providing access to the email account via a computer on the bank's network with the email client properly configured; and "reasonable assistance" translated into the provision of an operator who can call up each email to be inspected and set the function that displays the header

information for the defendant to inspect. In this manner, the right balance was struck for inspection of documents in the digital age.

90 More fundamentally, where copies of discoverable electronic documents are provided in their native format with metadata intact, the need for inspection is minimal. There is going to be very little that inspection will disclose which is not already available in a properly-made soft copy. With this in mind, inspection may, as a matter of practice, be deferred where native copies are provided, with the right to inspect reserved and exercisable later should inspection become necessary.

2. Direct exchange of electronic copies with inspection deferred

91 Where the "traditional" discovery regime is applied to voluminous electronic documents, much time and expense would be incurred if parties have to compile a detailed list of all the electronic documents, and to take photocopies after the inspection of each document. With the new optional framework introduced under paragraph 43J of Part IVA of the Practice Directions pursuant to the 2012 amendments, parties can discharge their discovery and inspection obligations by simply supplying electronic copies of the discoverable documents. A detailed list of documents is dispensed with in favour of a meaningful description of each category or sub-category of documents. Inspection will also be deferred and ordered when necessary. Much time and costs is saved by having inspection deferred and parties relieved of the laborious task of enumerating countless electronically stored documents into a list.

92 This amendment provides parties – particularly where the client and lawyer have adopted an electronic workflow – an option to gain real efficiency and costs savings. The time previously spent preparing and checking the list of documents against the documents in the "discovery file" can now be drastically reduced. With direct exchange of soft copies, time is spent where it really matters: in ascertaining that the soft copies on the exchange medium are complete and correct. The need for inspection is also obviated as soft copies are true and accurate copies of the "digital original". The need for inspection, particularly where exchange in native format has been conducted, will be rare indeed. Hence, parties may seek an order from the court that discovery be given by the supply of electronic copies of discoverable electronically stored documents in lieu of inspection, where to do so would facilitate the just, expeditious and economical disposal of the

matter. To complement this amendment, a list of common orders given in relation to discovery by supply of electronic copies has been set out in paragraph 43J(2) of the Practice Directions. This includes the dispensation of an enumeration of electronically stored documents in a list of documents, where a meaningful description of each category of documents would suffice.[55] Lawyers who are engaged in handling document intensive litigation matters will do well to consider this option with their clients seriously.

3. Part IVA and *Anton Piller* orders

93 In the paper-based paradigm, after the execution of an *Anton Piller* order, it is standard procedure for copies of documents to be made and the originals returned. Only relevant documents may be copied. The fundamental objective of such orders is to preserve relevant documents from imminent destruction. Originals have to be returned once copies of relevant documents are made, and the fundamental objective achieved. These are draconian orders and the courts in Singapore have traditionally insisted on strict compliance with the terms of the *Anton Piller* orders.

94 In this digital age, it is frequently the case that the execution of an *Anton Piller* order will involve the forensic imaging of recording devices like hard disks, thumb drives, mobile phones, storage media, etc. Forensic collection experts are almost always engaged to carry out the forensic imaging. After a forensically sound image is made, the original recording device or storage media is returned. With modern technology, it is now possible to make a copy of the filing cabinet, for example, the hard disk. Care must therefore be taken to prevent trawling of the forensic image for evidence.

95 It is in the area of the execution of *Anton Piller* orders that Part IVA has seen the most prolific use. An inspection protocol is always in place whenever forensic collection takes places as part of the *Anton Piller* order execution.

96 *Anton Piller* orders are made usually on an *ex parte* basis, when the plaintiff is able to demonstrate the high likelihood that evidence will be destroyed. It is not uncommon that such orders are obtained when the writ

55 See Part IVA, paragraph 43J(2)(d).

of summons is initially filed. Hence, by the time the forensic image is made, the defendant may not even have filed his defence. Since a forensically sound image has been made and is (usually) secured and placed in the custody of the supervising solicitor, one of the questions that needs to be addressed is whether the review of the forensic image can be carried out at this stage (*ie*, when the *Anton Piller* order is executed) or can the review be carried out later (*ie*, during general discovery)?

97 The approach adopted by the courts in Singapore appears to prefer that the forensic image be retained in the safekeeping of the supervising solicitor and the originals returned. Further, review of the forensic image should not take place at the stage of the execution of the *Anton Piller* order, but should take place after pleadings have closed and during general discovery. Further, the review would be subject to an electronic discovery plan, *viz* parties need to agree on keywords that are relevant and the search should be subject to reasonable constraints.[56]

98 Related to this is the question of whether the search should extend to deleted data. In *Robin Duane Littau*, it was held that a search through deleted data is not within the scope of general discovery.[57] However, pursuant to the specific wording of the *Anton Piller* orders in that case, a keyword search was permitted to be performed on the unallocated space of the seized items.

99 The practice of the execution of *Anton Piller* orders is expected to evolve further.

VII. CONCLUSION

100 Today's global marketplace has connected continents with transactions that generate voluminous amounts of data within the normal course of business. Countless numbers of emails, instant messages, letters, spreadsheets and presentations are created, transmitted and stored across the world each and every day. This proliferation of data and the resulting explosion of evidence has significantly increased the cost of litigation as parties often struggle to identify, collect, review and exchange documents during discovery.

56 *Supra* note 3, at [10].

57 *Supra* note 3, at [28]–[30]; Part IVA, Appendix E Part I, paragraph 1(c).

101 In recognition of the changing landscape of discovery, the Supreme Court Practice Direction No 3 of 2009 was introduced to provide guidance on the discovery of electronically stored documents, and was eventually inserted as Part IVA of the Practice Directions. In addition to promoting good faith collaboration between the parties, Part IVA championed the effective use of electronic discovery technology to mitigate the cost of litigation, and specifically the use of search tools to reduce manual review time and the retention of the evidence in electronic format to maximize efficiency.

102 Industry practice in Singapore in relation to electronic discovery has matured since the introduction of Part IVA in 2009. Pushing past the initial perception that the cost was disproportionate to the benefit, litigation lawyers are gradually embracing the use of electronic discovery technology. These efforts have been guided by court decisions that have provided vital judicial guidance on not only the application of electronic discovery technology, but also the need for parties to collaborate and agree in good faith.

103 Education will play a critical role in the growth and development of electronic discovery in Singapore. Paralegals and lawyers will need to be educated on the types and application of legal technology as part of their practical training to create a generation of savvy legal technologists with a firm understanding of the best practices, strategies and applications of electronic discovery within law firms and corporations.

104 Electronic discovery will continue to evolve in Singapore as lawyers and litigants strive to manage the exponential growth of electronic evidence. Lawyers will gain knowledge about litigation technologies, both in concept and strategy, as electronic discovery becomes more deeply integrated within litigation and arbitration processes. Lastly, despite the growth in the volume of data, costs can decrease provided electronic discovery practitioners leverage upon valuable insight from the UK and the USA to develop and implement innovative electronic discovery methodologies for the Singapore market.

PRESERVATION OF ELECTRONIC EVIDENCE

> "The first step in any discovery effort is the preservation of relevant information."
>
> *Pension Committee of University of Montreal Pension Plan v Bank of America Securities*, 685 F. Supp. 2d 456 (S.D.N.Y., 2010).

Cavinder **BULL**, Senior Counsel
BA (Hons) (Oxford), MA (Oxford), LLM (Harvard)

Gerui **LIM**
BA (Hons) (Oxford)

I. INTRODUCTION

1 A litigant's duty to preserve relevant evidence for discovery is not a novel or recent development. Preservation obligations are a basic and fundamental precept of the discovery process, which would not be able to operate meaningfully if litigants were able to destroy or alter the evidence in their possession at whim. Many countries have existing jurisprudence which establishes that a party who deliberately destroys documents to put them beyond an opponent's reach may face severe sanctions from the Court.

2 While parties may be subject to an obligation to preserve relevant evidence, the application of this principle in the area of electronically stored information ("ESI") has increasingly come under the spotlight. Compared to the traditional task of preserving physical documents in hard copy, the steps to preserve ESI tend to be far less straightforward. This is largely attributable to the complex and varied nature of ESI, which can be generated in large volumes, maintained in a wide variety of formats, locations and structures, and duplicated, stored, altered or deleted in a rather haphazard manner.

3 Some of the potential challenges and difficulties which can arise when giving discovery of ESI were highlighted by the Singapore High Court in *Sanae Achar v Sci-Gen Ltd*,[1] where the Court noted that:

> The introduction of the e-Discovery PD was a response to the *increasing tendency for documents to be generated and held electronically*. In my view, its

1 [2011] 3 SLR 967.

> introduction was timely, given the *unprecedented volume of documents which are created and stored electronically today … the relative ease of duplicating such documents* (by way of illustration, the same email may be sent to multiple recipients, who may reply to one or more recipients on the email thread, copying in other recipients, or forwarding the message on to others), *the often haphazard manner in which electronic documents are stored, the different document retention policies of parties* (some may routinely delete electronic documents to maximise the use of storage capacity whereas others may retain records of all electronic documents), *the existence of metadata information*, and the fact that *it is more difficult to completely dispose of electronically stored documents than printed ones* (it is common for residual traces of an electronic document to remain on a computer's storage system, despite deletion of the same from the user's active data).[2] [emphasis added]

4 With the ever-growing use of electronic communications and documentation in all walks of life, it is important for traditional approaches to discovery to be updated where necessary, so that novel issues pertaining to the discovery of ESI can be effectively handled by litigants, legal counsel and the Courts. In Singapore, the introduction of a Practice Direction on the Discovery and Inspection of Electronically Stored Documents in 2009[3] ("the E-PD") established a useful framework for parties to carry out inspection and discovery of ESI during the litigation process. However, the question of preservation is not specifically addressed in the E-PD. At present, there remains little guidance in Singapore on how a litigant or potential litigant should seek to preserve ESI for discovery.

5 In this article, Part II will provide a general overview of the duty to preserve evidence in various jurisdictions, before considering the responsibilities of legal counsel in ESI preservation efforts, the different types of ESI which may be encountered and the scope of ESI preservation obligations. In Part III, the main steps to implement a legal hold will be identified and explained. Although a balancing exercise will be necessary in every case to determine the specific scope of a party's obligation to preserve ESI, this article will suggest that the approach towards ESI preservation issues should be structured on the principles of reasonableness, good faith and proportionality.

---

2 *Ibid*, at [12].

3 Practice Direction No. 3 of 2009 (Discovery and Inspection of Electronically Stored Documents).

II. THE DUTY TO PRESERVE EVIDENCE

6 As previously mentioned, the duty to preserve evidence applies to all forms of relevant evidence and not just ESI. It is widely accepted that preservation obligations do not depend on the actual commencement of Court proceedings, but may be triggered once a party realises that litigation may be commenced by or against it. When litigation would be "reasonably anticipated" or "contemplated" (such that the duty to preserve evidence arises) is necessarily a fact-specific inquiry.[4] In some cases, the issue of pre-litigation letters of demand may be sufficient to give notice of pending litigation and trigger evidence preservation obligations.[5]

7 Once preservation obligations are triggered, a party's usual right to manage and destroy its own documents will be curtailed to some extent, and such party should not destroy potentially relevant evidence to prevent it from surfacing in the anticipated proceedings.

1. Approach to preservation obligations in different jurisdictions

8 While the general principle that parties have a duty to preserve evidence prior to the commencement of litigation is relatively uncontroversial, the Courts in various jurisdictions have adopted differing approaches to defining a litigant's preservation obligations. This is especially when it comes to the question of whether the pre-action destruction of evidence should be treated differently from destruction that takes place after the commencement of court proceedings.

9 In many jurisdictions, the duty to preserve evidence is not found in legislation or procedural rules governing discovery (unlike the duties to give disclosure and to produce relevant documents, which are almost always expressly provided for). However, this has begun to change in recent years, and preservation obligations are starting to receive express legislative recognition in some jurisdictions as being part and parcel of the discovery process.

---

4 Where the potential litigant is an organisation, knowledge of pending or anticipated litigation which is acquired by its individual employees may be attributable to the organization as a whole. See, for example, *Toussie v County of Suffolk*, No. CV 01-6716(JS) (ARL), 2007 WL 4565160 (E.D.N.Y. Dec 21, 2007).

5 In the US, there is a practice of expressly notifying a prospective defendant that relevant evidence should be preserved for anticipated litigation.

(a) Singapore

10 In Singapore, there is no express duty to preserve evidence for pending or anticipated litigation. However, such a duty implicitly exists as part of the discovery process in litigation. This was specifically recognised by the Singapore High Court in *K Solutions Pte Ltd v National University of Singapore*[6] ("*K Solutions v NUS*") where it held that:

> While it is true that there is no specific provision in the Rules of Court prohibiting any party from destroying relevant documents in his possession, custody or power, I am of the view that it is implicit in the scheme of discovery that he should not do so especially if he knows that they are relevant to the issues in the litigation …[7]

11 In *K Solutions v NUS*, the dispute concerned an IT project where the defendant had terminated the plaintiff's services. During discovery, it gradually emerged that the plaintiff had, shortly before commencing its claim against the defendant, destroyed various categories of relevant documents, including copies of its project staff's internal email and audio recordings of project meetings. It also transpired that the plaintiff's managing director, who was the person directing the plaintiff's actions on the project, had configured his email account to delete all documents which were more than 6 months old. This deletion policy was never stopped, not even after court proceedings were afoot. As a result of the plaintiff's actions, relevant evidence was no longer available for discovery.

12 After stating that the destruction of evidence would be deliberate where the destroyer "intends to put the documents out of reach of the other party in pending or anticipated litigation",[8] the Singapore High Court held that it saw no reason in principle to distinguish between situations of pre-action and post-action destruction where it was shown that the destruction was deliberate. The Court noted that it could be more difficult to establish that the destruction was deliberate in the case of pre-action destruction. However, once the requisite intent had been established, the same consequences as for post-action deliberate destruction should follow.[9] The Court stated that "where there is both deliberate destruction and a fair

6 [2009] 4 SLR(R) 254.
7 *Ibid*, at [106].
8 *Ibid*, at [107].
9 *Ibid*, at [125].

trial is no longer possible, then a striking out would appear to be the appropriate sanction."[10]

(b) Australia

13 In Australia, the seminal case on a litigant's duty to preserve potentially relevant evidence is *British American Tobacco Australia Services Ltd v Cowell*[11] ("*British American Tobacco*"). In that case, the Victoria Court of Appeal accepted that "[i]t surely cannot be the case that the prospective defendant, learning that litigation was about to be commenced against it, could simply destroy all relevant records bearing upon the principal issue, for the purpose only of defeating the claim when brought against it."[12] However, the court also highlighted that there had to be limits to such an obligation.

14 In formulating an appropriate legal test, the Victoria Court of Appeal sought to strike a balance between a party's right to manage its own documents and the right of a litigant to obtain the other party's documents. The court decided that where pre-action destruction of evidence was involved, the question to ask was whether the conduct, proved on a civil standard of proof, had amounted to the criminal offence of attempting to pervert the course of justice or criminal contempt:

> As indicated at the outset, it seems to us that there must be some balance struck between the right of any company to manage its own documents, whether by retaining them or destroying them, and the right of the litigant to have resort to the documents of the other side. The balance can be struck, we think, if it be accepted that the destruction of documents, before the commencement of litigation, may attract a sanction (other than the drawing of adverse inferences) if that conduct amounts to an attempt to pervert the

10 *Ibid*, at [127]. The Court stressed at [126] that all the circumstances of a case would have to be considered and that a striking out could be ordered even if a fair trial was still possible. The Court also left it open as to whether striking out might be ordered in "more difficult" cases involving negligent or reckless conduct resulting in destruction: at [130].

11 [2002] VSCA 197. In allowing the appeal against the lower court's decision to strike out the defence (see *McCabe v British American Tobacco Australia Services Ltd* [2002] VSC 73 (unreported, 22 March 2002, BC200201564)), the Victoria Court of Appeal overturned the lower court's factual finding that the defendant's destruction of disadvantageous documents three years prior to the commencement of the action was pursuant to a strategy devised by its legal advisors to defeat prospective litigants.

12 *Ibid*, at [145].

> course of justice or (if open) contempt of court, meaning criminal contempt …[13]

15 In *K Solutions v NUS*,[14] the Singapore High Court noted that the test in *British American Tobacco* had been criticised by Cameron and Liberman in "Destruction of Documents Before Proceedings Commence: What is a Court To Do?"[15], by Professor Pinsler in "Destruction of Evidence Prior to the Commencement of Civil Proceedings: How is a Court to respond?"[16] and by Professor Peter A Sallmann, Crown Counsel for Victoria, in his report "Document Destruction and Civil Litigation in Victoria",[17] which was commissioned by the Victorian Attorney-General following the Court of Appeal's decision. The test in *British American Tobacco* was also doubted by Crispin J in *Russell Vance v Air Marshall Errol John McCormack in His Capacity as Chief of Air Force*,[18] who stated that it was "somewhat incongruous for a court to approach its duty to do justice between the parties to a civil case by dipping into the criminal law and asking whether conduct that may have caused irremediable prejudice to one side was tainted by illegality."[19]

(c) United Kingdom

16 In the UK, the case of *Douglas v Hello! Ltd (No. 3)*[20] ("*Douglas v Hello!*") adopted the test laid down in *British American Tobacco* in the context of an application to strike out the defence. The destruction of evidence in *Douglas v Hello!* had occurred at both the pre-action and post-commencement stages of litigation. Interestingly, the English High Court's approach was to apply two different legal tests to those two stages. In respect of pre-action destruction of evidence, the court cited *British American Tobacco* and adopted its stricter test of requiring illegal acts of attempting to pervert the course of justice or amounting to criminal contempt. In respect of destruction which took place after proceedings were commenced, the court in *Douglas v Hello!* followed the approach in the

13 *Ibid*, at [173].
14 *Supra* note 6, at [124].
15 (2003) 27 Melb U L Rev 273, at pp 282-284.
16 [2004] SJLS 20 at p 25.
17 See <http://repositories.cdlib.org/ tc/reports/AU2004>.
18 [2007] ACTSC 80.
19 *Ibid*, at [35].
20 [2003] EMLR 29.

earlier English case of *Logicrose Ltd v Southend United Football Company Ltd*[21] and held that striking out would only be ordered where the defaulting party had prejudiced the possibility of a fair trial. The English High Court in *Douglas v Hello!* did not elaborate on its reasons for distinguishing between pre-action and post-commencement destruction of evidence.

17 In the subsequent case of *Timothy Duncan Earles v Barclays Bank Plc*,[22] Simon Brown QC (sitting as an Additional High Court Judge) cited *Douglas v Hello!* and *British American Tobacco* for the proposition that "in this jurisdiction as in Australia, there is no duty to preserve documents prior to the commencement of proceedings."[23] The court also stated that "[a]fter the commencement of proceedings the situation is radically different … [i]n the case of documents not preserved after the commencement of proceedings then the defaulting party risk [sic] 'adverse inferences' being drawn for such spoliation".[24] These comments suggested that litigants were only required to take steps to preserve documents after the commencement of litigation.

18 However, the position in the UK appears to be moving in the direction of having some form of duty to preserve evidence prior to the start of proceedings. Recently, in October 2010, Practice Direction 31B[25] was introduced to address electronic discovery issues as a supplement to Part 31 of the UK Civil Procedure Rules, which governs the disclosure and inspection of documents in court proceedings. Paragraph 7 of Practice Direction 31B specifically recognises that a need to preserve discoverable evidence, including ESI, would arise as soon as litigation is contemplated. It states that:

> As soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business.[26]

21 The Times, March 5, 1988.

22 [2009] EWHC 2500.

23 *Ibid*, at [28].

24 *Ibid*, at [29]–[30].

25 United Kingdom Civil Procedure Rules, Practice Direction 31B on the Disclosure of Electronic Documents.

26 *Ibid*, at [7].

19 There are presently no reported decisions on the scope of parties' obligations under Practice Direction 31B. Given that the latter is clearly phrased in terms of a "need" to preserve evidence arising when litigation is contemplated, it remains to be seen whether the UK courts will expect more from potential litigants, in terms of taking active steps to preserve evidence at the pre-action stage of litigation.

(d) United States

20 In the US, some states recognise the tort of spoliation as an independent cause of action in common law, which may be available against a party who deliberately destroys evidence. However, the exact formulation of this tort differs across the various states. Outside of the US, other commonwealth countries have generally not adopted the tort of spoliation as part of their law.

21 Apart from considering the pre-action destruction of documents in cases where the tort of spoliation is in issue, the US courts also inquire into parties' failure to preserve evidence in the wider context of imposing sanctions, which may potentially range from striking out parts or all of the destroyer's pleadings, drawing adverse inferences, ordering the exclusion of particular evidence and the exaction of pecuniary penalties by way of costs or additional costs. This "wider context" was highlighted by the Victoria Court of Appeal in *British American Tobacco*, where the court cautioned that US cases on drawing adverse inferences from pre-action destruction were not directly relevant to the question in that case, which concerned the lower court's decision to strike out the defence.[27]

22 In 2006, amendments were made to the US Federal Rules of Civil Procedure ("the FRCP") to address ESI-related issues. In particular, Rule 37(f) provides that the availability of rule-based sanctions would be limited where ESI was "lost as a result of the routine, good faith operation of an electronic information system." This basically creates, to some extent, a safe harbour for parties where the standard of "good faith" is satisfied. The Sedona Principles note that this was the first time the duty to preserve

27 *Supra* note 11, at [165]–[168]. At [168], the Victoria Court of Appeal also stated that it was "never questioned" that adverse inferences were warranted against the defendant in that case.

evidence potentially relevant to litigation was mentioned in the FRCP.[28] Although the FRCP do not establish standards governing pre-litigation preservation as they are procedural in nature and only apply once litigation commences, the Sedona Principles observe that Rule 37(f) represents a considered policy decision intended to prevent unreasonable and unnecessary interruption of routine information systems during discovery.[29] The Sedona Principles also suggest that, in determining whether a party is sufficiently culpable for the loss of ESI, the courts will begin by examining whether the party took reasonable good faith efforts to preserve relevant electronic data.[30]

2. Who has the duty to preserve evidence?

23 Turning to the issue of who should be responsible for taking steps to preserve ESI, the answer would obviously include the parties to the pending or anticipated litigation. However, there are also some indications that the Courts may have heightened expectations towards the roles and responsibilities of legal counsel in the area of ESI preservation.

(a) External Legal Counsel

24 Traditionally, external legal counsel play the role of informing their clients of their duty to preserve potentially relevant documents for discovery. However, given that the preservation of relevant ESI is not straightforward and can raise complicated issues, it seems rather unrealistic to depend on parties to identify, analyse and handle those issues effectively by themselves. On the other hand, one may expect external legal counsel to be much better equipped to ensure that the correct approach is taken to preserving ESI.

25 In the US, the courts have already indicated, in the context of preserving ESI, that legal counsel are expected to take affirmative steps to ensure compliance by their clients. *Zubulake v UBS Warburg LLC*[31] ("*Zubulake V*") is a significant decision on this point as it sets out explicit guidelines for lawyers managing the preservation and production of their

28 *The Sedona Principles* (Second Edition, 2007) at p 28.

29 *Ibid*, at p 9.

30 *Ibid*, Comment 14b at p 71.

31 229 F.R.D. 422 (S.D.N.Y., 2004).

clients' electronic evidence. The case involved an employment discrimination dispute. After the defendant failed to give full discovery, the plaintiff applied to court to sanction the defendant for its poor conduct of the discovery process. In its judgment, the US District Court was highly critical of the failure of the defendant's counsel to safeguard certain stores of data in the defendant's possession, and also of the defendant's careless and inconsistent compliance with the litigation hold which had been issued to preserve evidence before proceedings were commenced. The court also found that the defendant had engaged in deliberate destruction of evidence favourable to the plaintiff. As a result, the defendant was ordered to pay the plaintiff's legal and other related costs, and the court issued jury instructions to draw certain adverse inferences against the defendant.

26 The court also laid down some general principles governing the preservation of evidence prior to proceedings. It held that six key duties immediately fell to counsel to be carried out, namely: (1) issuing a litigation hold; (2) making the litigation hold known to all relevant employees by communicating with them directly; (3) identifying sources of discoverable information; (4) instructing all employees to produce electronic copies of their relevant files and secure any archival media which had to be retained; (5) overseeing their client's compliance with the litigation hold; and (6) monitoring their client's efforts to retain and produce the relevant documents.[32]

27 Although the various steps outlined in *Zubulake V* may seem to be a rather onerous burden to place on counsel, it is important to stress that the court only required counsel to participate in their client's preservation efforts within the limits of reasonableness.[33] It is worth considering if a similar approach should be taken in Singapore. Requiring counsel to be actively involved would likely improve the parties' overall preservation efforts, especially where difficult issues concerning ESI are involved. This could, in turn, reduce the likelihood of downstream discovery disputes and contribute to the saving of time and costs. As such, it may be beneficial to require external legal counsel to play a more active role in managing their clients' preservation efforts from an early stage.

28 In this regard, it is the position in Singapore and other Commonwealth countries that lawyers are also officers of the Court.

32 *Ibid*, at p 432.

33 *Ibid*, at p 433.

Lawyers already owe independent duties to the Court in relation to other aspects of the discovery process, such as the preparation of their clients' lists of documents to give disclosure of relevant documents. It would be consistent for lawyers to also owe an independent duty to the Court to manage and supervise their clients' preservation of relevant evidence.

(b) In-house legal counsel

29 If external legal counsel are going to be expected to play more active roles in the preservation of ESI, one question that could arise is whether an organisation's in-house legal counsel would owe similar duties to the Court to ensure that the organisation complies with its preservation obligations, and if so, whether in-house counsel might face personal sanctions from the Court in the event that they failed to discharge such duties.

30 The US case of *Swofford v Eslinger*[34] is an interesting decision on the issue of imposing sanctions on in-house counsel. The facts of that case concerned the shooting of the plaintiff by officers of the Seminole County Sheriff's Office ("the SCSO"). The plaintiff's attorney sent two preservation letters to the SCSO, requesting that all information, physical, electronic and otherwise, relevant to the case be preserved in their original condition. Apart from a few senior employees, the SCSO's legal department failed to notify anyone of the preservation request letters, and failed to take any more steps beyond that to preserve the evidence. When the plaintiffs applied for sanctions to be imposed for inadequate discovery, the US District Court sanctioned not only the three defendants from the SCSO, but also the SCSO's general counsel (who was not a named party in the suit) for:

> … his complete failure to full his duty, both in his official capacity as General Counsel for the SCSO and as initial counsel for all Defendants in this case, to take affirmative steps to monitor compliance so that all relevant, discoverable information is identified, retained and produced.[35]

31 The sanction which the US District Court imposed against the in-house counsel was an order that the latter be jointly and severally liable (together with the three defendants in the suit) to pay the fees and costs incurred by the plaintiff as a result of the sanctionable conduct. The court based its order on *28 U.S.C. § 1927*, which permits the court to sanction

34 671 F.Supp.2d 1274 (M.D.Fla., 2009).

35 *Ibid*, at pp 1287-1288.

"[a]ny attorney or other person admitted to conduct cases in any court of the United States … who so multiplies the proceedings in any case unreasonably or vexatiously", as well as the inherent authority of the court.

32 In Singapore, Order 59, r 8(1) of the Rules of Court provides that:

> Subject to this Rule, where it appears to the Court that costs have been incurred unreasonably or improperly in any proceedings or have been wasted by failure to conduct proceedings with reasonable competence and expedition, the Court may make against any solicitor[36] whom it considers to be responsible (whether personally or through an employee or agent) an order -
>
> (a) disallowing the costs as between the solicitor and his client; and
>
> (b) directing the solicitor to repay to his client costs which the client has been ordered to pay to other parties to the proceedings; or
>
> (c) directing the solicitor personally to indemnify such other parties against costs payable by them.

33 From the wording of Order 59, r 8(1), subsections (a) and (b) would not appear to extend to costs orders being made against in-house counsel as the latter would not normally have a solicitor-client relationship with their organisation. However, subsection (c) is conceivably broad enough to be interpreted as empowering the Courts to make personal costs orders against in-house counsel who have been admitted as advocates and solicitors of the Supreme Court. There are presently no reported Singapore cases where such measures were taken, and it would probably require extraordinary circumstances to warrant such sanctions being imposed. Nevertheless, in-house counsel tasked by their organisation to oversee or manage potentially litigious matters would be well advised to take reasonable steps at an early stage to ensure that potentially relevant documents are preserved for discovery to avoid judicial criticism or sanction.

36 Under Order 1, r 4, of the Rules of Court, "solicitor" has the same meaning as in the Legal Profession Act (Cap 161, 2009 Rev Ed) s 2(1), which in turn defines the term "solicitor" to mean "an advocate and solicitor of the Supreme Court". As such, Order 59, r 8, would not appear to be limited to the lawyers who are the solicitors on record for a particular party.

3. Different types of ESI

34 There appear to be at least four main categories of ESI which may potentially need to be preserved for discovery, namely: (a) active data; (b) archival data; (c) backup data; and (d) transient data.[37]

(a) Active data

35 Active data refers to data that is purposely stored in a manner that anticipates future use and permits efficient searching and retrieval. It is typically stored on local hard drives, networked servers, distributed devices, or offline archival sources, from which information can be, and is routinely and readily accessed, without a special restoration effort. The Sedona Principles suggest that active data should be the primary source of discoverable ESI.[38]

(b) Archival data

36 Archival data refers to data that is organised and maintained for long-term storage and record-keeping purposes. Some systems allow users to retrieve archival data directly, but others may require special equipment or software, or the involvement of IT staff, in order to do so.

(c) Backup data

37 Backup data duplicates the contents of active computer systems at a specific point in time and is intended to be used as a source to recover lost data in the event of system problems or failures. Backup tapes intended for disaster recovery purposes are generally not retained for substantial periods of time as the tapes will usually be recycled and existing data on them will be periodically overwritten when new backups are made. Backup data usually requires special intervention before it is readable.

---

37 In addition to the actual contents of ESI, the accompanying metadata (*ie*, descriptive data about the name, size, characteristics, modification and usage of the ESI) may also be discoverable information in certain circumstances. Another issue which can potentially arise in discovery is when ESI has already been deleted but is still recoverable as fragments, shadows, or residual portions of the original data set.

38 *The Sedona Principles* (Second Edition, 2007), Principle 8 at p 45.

38 Some organisations do not clearly separate the concepts of backup and archival data, and may retain disaster recovery backup tapes for a relatively long time period to retain files that may need to be accessed in the future. However, the Sedona Principles recommend that the practice of using backup tapes for archival purposes should be avoided, if possible, as it is likely to result in substantially higher costs for evidence preservation and production in connection with litigation.[39]

(d) Transient data

39 Transient data may be generated by computer systems as a temporary by-product and is usually not apparent to users. It is not intended to be kept permanently and is susceptible to being overwritten in the ordinary course of business.

40 An example of a case where transient data was in issue is *Columbia Pictures v Bunnell*.[40] The defendants in that case operated a website which allowed users to download pirated works using the "BitTorrent" software technology, where users would join a peer-to-peer network to share computer files. The plaintiffs sought a court order to obtain the defendant's server log information, which was derived from information temporarily processed and stored in the Random Access Memory (RAM) of the defendants' web servers for periods which could range from a fraction of a second to hours. The server log information could only be extracted and preserved by activating certain logging or tracking functions on the defendants' server, which the defendants had not done.

41 The US court held that the server log information was important and unique information, which the defendants were required to prospectively preserve and produce in discovery. However, the court stressed that its ruling should not be read as creating a requirement for litigants in all cases to preserve and produce ESI which was temporarily stored only in RAM.[41] As for the defendants' prior failure to preserve the server log information, the court held that the imposition of sanctions was not appropriate as the defendants had acted in good faith:

39 *Ibid*, Comment 5b at p 30.

40 2007 U.S. Dist. LEXIS 46364.

41 *Ibid*, at fn 31.

> As noted above, although this court now finds that defendants have an obligation to preserve the Server Log Data in issue that is temporarily stored only in RAM, in the absence of (1) prior precedent directly on point in the discovery context; (2) a specific request by defendants to preserve Server Log Data present solely in RAM; and (3) a violation of a preservation order, this court finds that defendants' failure to retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required. Consequently, the court finds that evidentiary sanctions against defendants for spoliation of evidence are not appropriate.[42]

4. The appropriate scope of a party's duty to preserve evidence

42 In *Zubulake v UBS Warburg LLC*[43] ("*Zubulake IV*"), the court stated that "anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary."[44] However, the court also stressed that a party's obligation to preserve documents was not absolute. The following question was posed in its judgment:

> What is the scope of the duty to preserve? Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, "no". Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation.[45]

43 It is usually not practical, if not impossible, for litigants to preserve all the potentially relevant ESI in their computer systems in anticipation of future litigation. It would also be extremely onerous, as well as expensive and time-consuming, if parties had to take every conceivable step to preserve potentially relevant ESI. As such, a balance needs to be struck between a party's right to continue its routine operations and manage its ESI in the ordinary course of business, and the need for potentially relevant ESI to be preserved for anticipated litigation.

42 *Ibid*, at p 15.
43 220 F.R.D. 212 (S.D.N.Y., 2003).
44 *Ibid*, at p 217.
45 *Ibid*.

44 In the US, good faith, reasonableness and proportionality are central concepts in the Sedona Principles.[46] The latter provides suggested guidelines and recommended practices for the preservation of ESI during the pre-action stage, as well as the actual production of ESI during the litigation process.

45 In Singapore, although the E-PD does not directly address parties' pre-litigation preservation obligations, it does expressly refer to parties making reasonable efforts and acting in good faith in relation to certain issues which may arise during the discovery process. The E-PD also recognises the need to strike a reasonable balance between the potential benefits and burdens of ESI discovery. For example, it expressly lists certain factors which the Court will consider in applications for the inspection or discovery of ESI, including the volume and accessibility of documents involved, the ease and costs of giving discovery, the significance of the ESI to the issues in dispute, *etc*, before deciding whether such an application should be granted or not.

46 Given that good faith, reasonableness and proportionality in the conduct of electronic discovery already feature to some extent in the E-PD, it is proposed that these principles should form guiding principles when determining the scope of a party's obligation to preserve ESI. Thus, the duty to preserve ESI should not be absolute, but should be applied proportionately. A party should also act reasonably and in good faith, based on circumstances known at the time, when executing its preservation obligations. Where these basic tenets have been followed, it is very unlikely that a party would be exposed to sanctions for inadequate preservation efforts.

III. MAIN STEPS TO IMPLEMENT A LEGAL HOLD

47 The actual process by which litigants preserve evidence to satisfy their discovery obligations is often referred to as a 'legal hold' or a 'litigation hold'. Not surprisingly, the formulation of an appropriate preservation strategy will vary depending on the circumstances involved, and each case will have to be approached on its particular facts. However, in terms of

46 *The Sedona Principles* (Second Edition, 2007). See also the Sedona Conference, "Commentary on Proportionality in Electronic Discovery" (2010) 11 The Sedona Conference Journal 289 at pp 289-302.

general methodology, it is possible to identify four main steps to implementing a legal hold:

(a) identifying sources of ESI;

(b) deciding on an appropriate legal hold strategy;

(c) communicating and monitoring the legal hold; and

(d) engaging in good faith collaborative discussions with the other party.

1. Identifying sources of ESI

48 Once the duty to preserve evidence has been triggered, the first step should be to promptly identify potential sources of relevant ESI within a party's possession, custody and control.

49 It is significant to highlight that identifying sources of ESI may not be a straightforward task, especially if the ESI consists of non-active data. It may not be sufficient to rely on factual witnesses' perceptions of what ESI is available, as such witnesses may not fully understand or appreciate how ESI generated by them is processed, stored or deleted within their organisation. It is therefore important to consult the relevant IT or records-keeping staff in an organisation about the various types of technology used by the organisation, including hardware, software, electronic communication or recording devices, document archival or storage procedures and disaster recovery procedures.

50 On counsel's part, possessing working knowledge of general technology issues which may arise in electronic discovery will be necessary for an information gathering exercise to be conducted effectively. It is also essential that counsel should spend time learning and familiarising themselves with the organisation's particular technology infrastructure and electronic information systems. This will help to ensure that the right questions are asked at this stage, so that sources of ESI are not inadvertently overlooked.

2. Deciding on an appropriate legal hold strategy

51 After the potential sources of relevant ESI within an organisation have been identified, the next task would be to ascertain the scope of the ESI that

will be preserved. As previously mentioned, the duty to preserve evidence is not absolute as it is "unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."[47] Determining where the line should be drawn in a particular case requires an exercise of judgment, based on the consideration of various factors known at the time.

52 An approach to preservation based on principles of reasonable and proportionality would require the value of the ESI to be weighed against the burden and costs of its preservation. The factors to be considered when deciding what would be a reasonable and proportionate legal hold strategy may include:

(a) whether the ESI is unique, or whether duplicates can be obtained from a more convenient, less burdensome or less expensive source;

(b) the likely significance of the ESI to the potential claim;

(c) the possible methods or technologies available to preserve the ESI in question;

(d) the costs involved; and

(e) the potential amount involved in the anticipated litigation.

53 When designing its legal hold strategy, an organisation may generally choose any method, or any combination of methods, which would achieve the result of preserving its relevant ESI. In *Zubulake IV*, the court commented that:

> A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any documents created thereafter. *In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task is accomplished.* For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort) and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve the documents in the state they existed at that time), creates a complete set of relevant documents.

47 *The Sedona Principles* (Second Edition, 2007), Principle 5 at p 28.

> *Presumably there are a multitude of other ways to achieve the same result.*[48] [emphasis added]

54 However, it is important to bear in mind that the preservation method used for a legal hold needs to be reasonable and should not obstruct the subsequent production of documents for discovery. Thus, the preservation method should preferably preserve ESI in its native format without altering the meta-data as the latter can be separately discoverable in certain situations. Alternatively, it may be acceptable to preserve ESI in the form in which it is ordinarily maintained or at least a reasonably usable form. If a party deliberately selects a preservation method which converts existing active data into inaccessible data which is difficult to search for and retrieve, this may very well result in subsequent costs orders being made against that party.

55 On the issue of whether inaccessible backup tapes or data have to be preserved, the Sedona Principles suggest that preservation obligations generally should *not* extend to disaster recovery backup tapes, which are not intended to be used by an organisation for archival purposes. The two main justifications for this approach are, first, that the contents of backup tapes would be duplicative of existing active data, so proper preservation efforts with respect to the active data should make preservation of the backup tapes redundant; and second, that it may be burdensome and costly for a party to retain backup tapes, which it would have recycled in the ordinary course of business.[49]

56 Notwithstanding the above, there can be situations where the preservation obligation may extend to backup tapes. For example, the Sedona Principles suggest that where an organisation has determined that the *only* source of relevant ESI is one that is not reasonably accessible, the party may have to preserve that source even if it intends to subsequently dispute the production of the ESI on the basis that production would be unduly burdensome or expensive.[50]

---

48 *Supra* note 42, at p 218.

49 *The Sedona Principles* (Second Edition, 2007), Comment 5b at p 30. See also Principle 9 of *The Sedona Principles* (Second Edition, 2007) in relation to deleted, shadowed, fragmented or residual electronically stored information, and *Columbia Pictures v Bunnell* 2007 U.S. Dist. LEXIS 46364 where the US court declined to impose sanctions in respect of the defendants' prior failure to preserve relevant transient data which had to be produced in discovery (discussed at pp 141–142 above).

50 *Ibid*, Comment 8b at p 46.

57 The case of *Zubulake IV* provides an example where a party's preservation obligations extended to its backup tapes. The parties in that case were in the midst of restoring backup tapes belonging to the defendant pursuant to an earlier discovery order. In the course of the restoration effort, it was discovered that certain backup tapes were missing. The plaintiff subsequently applied for various sanctions to be imposed against the defendant. One of the issues before the US court was whether the defendant had been under a duty to preserve the missing backup tapes.

58 The court in *Zubulake IV* recognised that, as a starting point, a party generally did not have to apply a litigation hold to preserve inaccessible backup tapes, which could continue to be recycled in accordance with the party's usual schedules. However, the court held that an exception would exist if a party could identify the location of documents of 'key players' in the action on its backup tapes and that information was not otherwise available. On the facts of that case, there was evidence that some of the defendant's staff, who were among those likely to have relevant information, had deleted relevant emails from the defendant's system such that the deleted emails would have only resided on the missing backup tapes. The court concluded that the defendant had therefore been under a duty to preserve the missing backup tapes. However, as the plaintiff was unable to demonstrate that the missing documents would have supported her claims, the court declined to give instructions for an adverse inference to be drawn against the defendant.

59 *Zubulake IV* illustrates how the presence of unique and relevant ESI on a party's inaccessible backup tapes may justify the imposition of a duty to preserve the latter. An interesting question could arise in a situation where a party anticipating litigation determines that there is relevant evidence in its possession that only exists in the form of inaccessible ESI on backup tapes, but the same evidence can reasonably be expected to be in the adverse party's possession in the form of active ESI. Under such circumstances, would the first party be under an obligation to preserve its backup tapes, or would it be permissible for it to continue recycling its backup tapes in the ordinary course of business on the assumption that its adverse party will satisfy its own preservation obligations and retain the active ESI for discovery?[51] While the second approach seems *prima facie*

51 In *K Solutions v NUS*, *supra* note 6, the defendant had provided email accounts ("the NUS email accounts') to the plaintiff's staff for the duration of the project, which it

reasonable, it may still be necessary to take into account factors such as the cost of preserving the backup tapes, the potential significance of the evidence to the litigation and whether there are any known facts which suggest that the other party might destroy the evidence in its possession, in order to assess whether the first approach may be warranted in the circumstances.

60 While the obligation to preserve inaccessible ESI is unlikely to arise in most situations, parties should give careful consideration as to whether there are any special reasons which call for a different approach in their case.

3. Communicating and monitoring the legal hold strategy

61 The third main step in implementing a legal hold strategy is to effectively communicate its requirements to the organisation's relevant staff. In many cases, issuing a written notice may be an appropriate way of executing the legal hold. The instructions in a legal hold notice should be reasonably clear, understandable and capable of being followed. The staff should also be informed of the potential consequences of non-compliance with their preservation obligations.

62 Depending on the circumstances, alternative methods of putting a legal hold in place may also be preferred. For example, if a staff member within the organisation is the subject of the litigation and there are reasons to believe that he or she may seek to destroy relevant ESI, it may be appropriate to take steps to collect the ESI which that staff member has access to before a legal hold notice is issued. Alternatively, it may be possible

---

engaged the plaintiff to work on. Shortly before the project was terminated, the plaintiff's project staff made copies of the emails in their respective NUS email accounts and gave the email copies to the plaintiff, before deleting most of the emails in their NUS email accounts. However, those email copies were later found to have been destroyed and suppressed by the plaintiff. At the hearing of the plaintiff's appeal against the first instance decision to strike out its case, the plaintiff tried to argue that the lost emails could nevertheless be obtained from the storage capabilities of the defendant's email system. This argument was only raised shortly before the hearing and was disputed by the defendant. The Court questioned the merits of the plaintiff's suggestion and held (at [142]) that it was too late for the plaintiff to raise this possibility to prevent its case from being struck out. The Court did not comment on whether, notwithstanding the email copies that ought to have been in the plaintiff's possession, the defendant would also have been required to preserve any duplicate ESI which might be in an inaccessible format.

to limit that staff member to read-only access rights depending on the system used by the organisation. What is important is that every case should be evaluated on its own facts. The communication and execution of the legal hold strategy should be tailored to address the needs of a particular situation.

63 After the initial communication of a legal hold to the relevant staff in the organisation, a party should still take reasonable steps to monitor its preservation efforts and ensure that the legal hold is complied with. Good practices can include sending periodic reminders to the staff involved, obtaining confirmations of compliance and conducting regular assessments to see if the scope of the legal hold needs to be changed for any reasons, *eg*. new allegations may have surfaced or there could be developments in the litigation. The negligent or otherwise ineffective execution of a litigation hold may lead to sanctions being imposed against the defaulting party.

64 It may also be advisable for an organisation to document the process by which its legal hold is implemented. The Sedona Conference Commentary on Legal Holds[52] suggests that the information to be documented may include the date and by whom the legal hold was triggered, possibly the triggering event, the scope of the legal hold, any subsequent changes in scope, notices and reminders sent, compliance confirmations, the collection protocol, when and who information was collected from, notes of any interviews conducted to ascertain additional information sources, and a master list of people and systems involved in the preservation efforts.

65 Where a legal hold process is documented, the documentation produced could arguably fall within the scope of solicitor-client or litigation privilege. If so, the other party may not be able to compel disclosure. Nevertheless, having such documentation in hand may assist in a party's subsequent discovery efforts, especially in long and protracted litigations involving substantial amounts of ESI from numerous sources. Documenting the legal hold process may also provide a party with the option of disclosing the information to the Court[53] in the event that it subsequently faces allegations that it fell short in its preservation efforts.

52 The Sedona Conference, "Commentary on Legal Holds: The Trigger and The Process" (2010) 11 The Sedona Conference Journal 2010 265 at p 285.

53 The disclosing party should take care to ensure that such disclosure would not inadvertently amount to a general waiver of privileged material.

Proper documentation of the steps which were taken by the party may help to demonstrate that a party had conducted its preservations efforts with reasonable diligence and in good faith.

4. Good faith collaborative discussions with the other party

66 At some stage, or at least shortly after litigation has commenced, it may be viable to engage the other party in good faith discussions with a view to identifying and agreeing on the scope of ESI to be preserved. Such an approach is endorsed in the Sedona Principles, which observe that:

> Early discussion of issues relating to the preservation and production of electronically stored information may help reduce misunderstandings, disputes and unnecessary motions, including post-production sanction motions involving the failure to preserve relevant information … parties should pay particular attention to achieving a balance between competing needs to preserve relevant evidence and to continue critical routine operations in order to reach agreement on 'reasonable preservation steps'.[54]

67 The Sedona Principles also list some of the preservation issues which parties should seek to resolve early in an action, namely: (i) the identification of data sources which will be subject to preservation and discovery; (ii) the relevant time period; (iii) the identities of particular individuals likely to have relevant electronically stored information; (iv) the form or forms of preservation and production; (v) the types of metadata to be preserved and produced; (vi) the identification of any sources of information that are not reasonably accessible because of undue burden or cost, such as backup media and legacy data; (vii) use of search terms and other methods of reducing the volume of electronically stored information to be preserved or produced; and (viii) issues related to assertions of privilege and inadvertent production of privileged documents.

68 There are clear advantages to following a structured approach where preservation issues are dealt with at an early stage of proceedings, as opposed to being swept under the carpet until problems with missing documents surface during the production stage of discovery. By that time, relevant ESI could be lost and it may be far too late for a party to remedy the shortcomings in its legal hold. Further, if parties are able to discuss and resolve early on in their dispute that certain sources of ESI are not

54 *The Sedona Principles* (Second Edition, 2007), Comment 3a at p 21.

reasonably accessible and do not have to be preserved, this may help to avoid situations where parties incur unnecessary costs to maintain protective legal holds due to fears of discovery disputes later on.

69 In Singapore, there are currently no guidelines on how parties in litigation should approach ESI preservation issues. However, given that the E-PD already encourages parties to collaborate in good faith and decide on a mutually agreeable electronic protocol in relation to aspects of the disclosure and production stages of discovery,[55] extending this approach to include preservation issues such as those described in the Sedona Principles would support and tie in with the existing framework under the E-PD.

IV. CONCLUSION

70 While the traditional preservation of physical evidence may have been a fairly straightforward matter, developments in technology have led to additional complications which look set to increase with time. The difficulties in determining the scope of preservation obligations should not go unaddressed, particularly since parties may face harsh sanctions if they fail to meet the preservation standards required of them.

71 There is thus a growing need to formulate express guidelines in relation to parties' duty to preserve ESI before the commencement of litigation, as well as the role which legal counsel are expected to play in such endeavours. It is worth noting that the US and, more recently, the UK, have both taken some steps to update and supplement their procedural rules. It is respectfully suggested that measures should also be initiated in Singapore to keep pace with international developments in this area. The introduction of express guidelines would aid certainty, facilitate and complement the existing discovery framework under the E-PD, and help participants in the litigation process to address the increasing use of electronic communications and documentation in modern life.

---

55 E-PD, *supra* note 3 at [43B].

PERSPECTIVES ON PRESERVING ELECTRONIC EVIDENCE WHEN LITIGATION IS CONTEMPLATED OR HAS COMMENCED

Francis **XAVIER**, Senior Counsel
LLB (National University of Singapore)

Harpreet **SINGH** Nehal, Senior Counsel
LLB (National University of Singapore), LLM (Harvard)

Bob **YAP**
BEc (Accounting) (Monash University, Australia)

TAN Swee Wan*
BSc (National University of Singapore)

I. INTRODUCTION – THE DUTY TO PRESERVE AND THE LITIGATION HOLD

1 Once a party reasonably anticipates litigation, it behooves the party to preserve electronic evidence by way of a "litigation hold" or an analogous process. As the court noted in *Zubulake v UBS Warburg LLC*[1] ("*Zubulake IV*"):

> The scope of a party's preservation obligation can be described as follows: *Once a party reasonably anticipates litigation, it must suspend its routine document retention / destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.* As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold.[2] [emphasis added]

2 It is important to appreciate that the general obligation of solicitors with respect to discovery imposes on solicitors a positive duty to implement

---

* The views expressed in the paper do not necessarily represent the collective view of all the panellists on the issues discussed.

1 *Zubulake v UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y., 2003).

2 *Ibid*, at p 218.

the litigation hold. This was recognised by Megarry J who observed in *Rockwell Machine Tool Co Ltd v EP Barrus (Concessionaires) Ltd*[3] that:

> It seems to me necessary for solicitors to take positive steps to ensure that their clients appreciate at an early stage of the litigation, promptly after writ issued, not only the duty of discovery and its width [b]ut also the importance of not destroying documents which might by possibility have to be disclosed. This burden extends, in my judgment, to taking steps to ensure that in any corporate organisation knowledge of this burden is passed on to any who may be affected by it.[4]

3 Solicitors will also have to work closely with in-house counsel in respect of litigation holds. It cannot be gainsaid that adverse consequences of non-compliance with e-discovery obligations, including deliberate destruction or spoliation of electronic evidence, will have adverse consequences on litigants, leading ultimately to the possibility of judgment being entered against the relevant party. In this connection, it was observed in *Zubulake v UBS Warburg LLC*[5] ("*Zubulake V*") that:

> The spoliation of evidence germane "to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction." A party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.[6]

4 The duty extends to *potentially* relevant documents. A party that excludes a category of the documents from the litigation hold on the basis that that category of documents does not (at that stage of the litigation) map directly to an expressly demarcated issue would thus appear to fall short of the duty of preservation. It is necessary to go further by extending the litigation hold to all documents which are potentially relevant to the dispute between the parties.

5 Thus, while discussing the duties in maintaining a litigation hold, the court in *Zubulake V* considered that litigators have an affirmative duty to

3 [1968] 1 WLR 693.

4 *Ibid*, at p 694; see also *Koh Teck Hee v Leow Swee Lim* [1991] 2 SLR(R) 328.

5 229 F.R.D. 422 (S.D.N.Y., 2004).

6 *Ibid*, at p 430.

ensure that relevant documents are preserved by (i) placing a litigation hold on them; (ii) communicating to the client the need to preserve the documents; and (iii) arranging to safeguard any relevant archived media.[7] Thus, counsel has the duty to advise clients on the obligation to preserve potentially discoverable documents:

> In sum, counsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. In particular, once the duty to preserve attaches, counsel must identify sources of discoverable information. This will usually entail speaking directly with the key players in the litigation, as well as the client's information technology personnel. In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media (e.g., backup tapes) that the party has a duty to preserve. Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril.[8]

6 One significant issue is when a party to anticipated litigation comes under a duty to preserve the potentially relevant documents. This is particularly important, given that a familiar facet of in-house data management system is the deletion of information. Thus, it was held in *Kronisch v United States*[9] that spoliation (*ie*, deliberate instances of deleting material data) can occur where a company does not preserve evidence, which it knows may be relevant to future litigation. The duty to preserve electronic evidence does not arise only after litigation commences. Rather, it attaches once a party has notice that the evidence is relevant to litigation.[10] Such notice usually arises when suit has been filed, thus giving the relevant party express notice, and sometimes, in circumstances where such party should have known that the evidence may be relevant to future litigation.[11]

7 *Ibid*, at p 432.
8 *Ibid*, at p 439.
9 150 F.3d 112 (2d Cir. 1998).
10 *Ibid*, at p 126.
11 *Ibid*, at p 126.

7 There does not appear to be any explicit reference to "litigation holds" or any similar concept in the Practice Direction on the Discovery and Inspection of Electronically Stored Documents[12] ("the E-PD"). However, it is clear that the principles outlined above flow directly from the general obligations of a solicitor with respect to traditional discovery under the common law. Further, the litigation hold is an important safeguard in ensuring that evidence is not compromised for proceedings which a party may either commence or defend. It is noteworthy that the Singapore courts have taken a robust approach to instances of spoliation.[13] While the test appears to focus on whether there has been a deliberate intent to destroy evidence,[14] it is clear that, in appropriate cases, a failure to implement a proper litigation hold places a party at risk of the court inferring an intent to destroy evidence.

II. LITIGATION HOLD AND THE CHALLENGES POSED BY ELECTRONIC DOCUMENTS

8 Data has become a torrent flowing into every area of the global economy. Digital data is now everywhere – in every sector, economy, organisation and user of digital technology. As much as 92 percent of information produced each year is stored in digital format. Businesses are, today, far more prolific in generating digital data than paper documents.

9 One reason for the growing volume of stored e-mail is the precipitous decline in the cost of digital storage, thanks to commoditisation and lower-priced, high capacity drives making it to the market. For example, one gigabyte of disk space was about USD40,000 in the eighties and the same disk space costs less than a dollar today.

10 Any litigation hold needs to deal with a large – and rising – volume of unstructured digital data, particularly in e-mail format. However, volume is not the only challenge for e-discovery. As much as 70 percent of e-mails and corporate documents are duplicates. Extraneous and repetitive data escalate costs at every stage of any discovery process. Since the essence of discovery is the sharing of documents, issues concerning volume and redundancy, as

12 Practice Direction No. 3 of 2009 (Discovery and Inspection of Electronically Stored Documents).

13 See, for example, *K Solutions Pte Ltd v National University of Singapore* [2009] 4 SLR(R) 254.

14 *Ibid*, at [110] and [125].

well as file size (gigabytes) and difficulty of transmission, become particularly acute when companies face multi-production matters or multi-jurisdictional litigation, both of which require coordinating discovery amongst widely dispersed legal support teams. For example, law firms need to compare the costs and staffing requirements associated with the printing, packing, and trucking of documents to Web-based file sharing.

11 All e-discovery approaches have two major components: (1) document review and (2) various mechanical processes needed to prepare the documents for review and to implement "production". Since document review is performed by an attorney or paralegal, and is highly labor-intensive, this aspect of e-discovery is extremely costly. While mechanical (non-review) processes are less expensive, highly inefficient methods can drive up costs. Any approach that emphasises mechanical processes (the more computerised the better) and contains billable hours by attorneys will tend to prevail.

III. WHAT OUGHT TO BE PRESERVED?

12 A key step in understanding the extent of a litigation hold is an identification of the potential sources of storage of electronic evidence. There are a number of different devices and/or storage media in which one may encounter digital evidence that could contain relevant information. While personal computers and servers are probably the most common sources encountered, other sources of potentially relevant electronic evidence include access control or verification systems, *eg*, firewalls or routers, Personal Digital Assistants (PDA), *eg*, the Blackberry, Palm and PocketPC, digital voice mail systems tied to a PBX phone set-up, mobile phones, portable music players and digital cameras.

13 Furthermore, there are a number of different storage mediums which may be used. While lawyers are probably most familiar with the hard disk, there are many other storage mediums that are available and being frequently utilised in today's world, *eg*, backup tapes, USB drives, floppy disks, CDs, DVDs, and memory cards.

14 Similarly, electronic evidence can themselves take diverse forms. Today's computer environment allow for the storage of virtually any sort of document, transaction, or record. Common types include, but are not limited to, (a) electronic correspondence, *eg*, e-mails (including Web-based

e-mails through services such as Hotmail, Yahoo!, Gmail, and others), text messages, instant messages, financial records; (b) organisational information, *eg*, address books, calendars, diaries; (c) office documents, *eg*, spreadsheets, documents, project plans, and CAD diagrams; (d) chat logs; (e) internet history and internet cache files; (f) temporary files, auto recovery files, and deleted files; (g) unallocated space; and (h) virtual memory.

15 The sheer volume of electronic documents can often mean that preservation of evidence will be a difficult task. In recommending the scope of the obligation to preserve electronically stored information, Principle 5 of the Sedona Principles requires reasonable effort to be exerted in good faith to retain information that may be relevant to pending or threatened litigation. However, it is recognised that it would be unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information. As the court noted in *Zubulake V*:[15]

> To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit." Although this sounds burdensome, it need not be. Counsel does not have to review these documents, only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive documents. When the opposing party propounds its document requests, the parties could negotiate a list of search terms to be used in identifying responsive documents, and counsel would only be obliged to review documents that came up as "hits" on the second, more restrictive search…In short, it is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. *Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched. This is not to say that counsel will necessarily succeed in locating all such sources, or that the later discovery of new sources is evidence of a lack of effort. But counsel and client must take some reasonable steps to see that sources of relevant information are located.* [emphasis added]

The balance is a fine one. While entities are not expected to preserve every single email or electronic document when litigation arises (since this would cripple entities involved in litigation), the right of such entities to continue to manage their electronic databases in its ordinary course of business, even

15 *Supra* note 5, at p 432.

if some data is overwritten as part of routine procedure, must be balanced against the need to ensure preservation of relevant data. A reasonable balance must thus be struck between (i) the duty to preserve potentially relevant electronic evidence and (ii) the organisation's need, in good faith, to continue operations and allow regular document management policies to continue.

16 It is difficult to state with precision the fine balance that has to be struck between these competing considerations. In *Monaid Technologies Inc. v Samsung Electronics Co. Ltd.*[16], it was considered that a litigant is not under a duty to keep or retain every document in its possession, but is under a duty to preserve what it knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation. In *Concord Boat Corp v Brunswick Corp*[17], the court held that all relevant e-mails subsequent to the filing of complaint must be preserved, but not all e-mails prior to commencement of litigation. As stated by the court, "to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail".[18] The Court found that this would cripple most large corporations.

17 The Sedona Principles drew an analogy between the duty of preserving electronic evidence and the duty to preserve physical evidence: once litigation is reasonably contemplated, an organisation need not immediately preserve the contents of the office wastebaskets/recycling facilities. These can be disposed of as part of routine procedure. However, organisations are certainly prohibited from deliberately disposing of these contents in order to destroy documents.[19]

18 Similarly, an organisation need not halt or freeze its regular electronic procedures.[20] For example, a word processing program saves backup copies of documents and routinely overwrites them. Requiring all backup copies to be preserved would mean that the program would have to be shut down and that backup copies would have to be made at regular intervals. This

16 348 F.Supp.2d 332 (D.N.J., 2004) at p 336.

17 1997 WL 33352759.

18 *Ibid*, at p 4.

19 *The Sedona Principles* (Second Edition, 2007), Comment 5(a), at p 28, and Comment 5(g), at p 34.

20 *Ibid*, Comment 5(g), at p 34.

would be prohibitively expensive and would also interfere with the running of the organisation.

19 A difficult question arises as to what happens when electronic evidence is located on an inaccessible source. The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible[21] sets out the following considerations, amongst others:[22]

> (a) The duty to preserve applies to any and all relevant documents, tangible things, or electronic information in the possession, custody, or control of a party no matter where located, even when the electronic information is located on an inaccessible source.
>
> (b) Knowledge or belief that litigation has begun or is imminent triggers preservation obligations and requires that reasonable steps be undertaken to maintain relevant and discoverable information pending discovery.
>
> (c) Parties should not exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve.

20 However, the Sedona Principles suggest that, absent a demonstration of special need and relevance, a responding party should not be required to preserve, review or produce deleted, shadowed, fragmented or residual electronically stored information. A party must show good cause to obtain such information, *eg*, that production would be ordered only if relevant in obtaining overwritten drafts/backup copies.

IV. TECHNICAL CHALLENGES ASSOCIATED WITH PRESERVATION

21 The importance of ensuring that data is adequately preserved entails that due care should be taken in the process of data extraction. Various considerations need to be taken into account to avoid the inadvertent

21 The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible (July 2008).

22 *Ibid*, at p 4.

alteration or destruction of electronic evidence. Key amongst these considerations are listed and discussed in this Part.

1. Environmental Issues

22 Operationally, the nature of the IT environment is a primary consideration in determining the proper mechanisms for implementing a proper and effective litigation hold. Further, it would be appropriate to identify, at the outset, the privacy issues that may impact on what data can be examined, collected and/or transported out of the jurisdiction, particularly in the context of a cross-jurisdictional dispute.

23 It would also be advisable, at the outset, to recognise any legal or professional privilege or other privilege-related issues that may affect the acquisition process. In this connection, identifying the authority to which the electronic evidence may be subject (*eg*, by authorisation of the systems owner, by consent, under legislative directive, under the order of a court, *etc*) would generally be crucial, as it could potentially have a significant impact on the scope of preservation.

2. Safe shutdown

24 In instances where a computer system is operating, it may be necessary for it to be shut down prior to data acquisition. The most appropriate method of safely shutting down a computer is very much dependent upon its operating system and the processes active at the time. It is therefore necessary for there to be a proper understanding of the specific technology environment to prevent damage to the data contained within the computer system.

3. Destructive programs

25 Security software and other applications that are designed to wipe data on any attempted unauthorised access.

4. Remote access

26 Networks and the Internet present a remote danger to electronic evidence stored on a computer system. Physical isolation may not be

enough to prevent the loss of electronic evidence if remote connectivity is enabled.

5. Magnetic radiation

27 Electronic evidence stored on magnetic media, such as a floppy disk or hard drive, is susceptible to alteration or damage from external magnetic radiation.

6. Mishandling

28 Electronic evidence that resides on a storage device that relies on mechanical action is susceptible to damage resulting from mishandling.

7. Heat

29 While modern storage devices are designed to withstand significant levels of heat, there may come a point at which the electronic circuits associated with the storage device will begin to fail, leading to the loss of information stored in the device.

8. Power fluctuations

30 Given that electronic storage devices rely on electricity to operate, it comes as no surprise to learn that significant fluctuations in power supply can result in significant damage to the storage device as a whole.

V. ISOLATION OF POTENTIALLY RELEVANT DOCUMENTS – THE IMPORTANCE OF PLANNING

31 Planning is one of the most important aspects of any process of obtaining electronically stored information protected via a litigation hold. The overriding objective of utilising forensic technology is to leverage on the use of tools and experience to identify and acquire all electronic evidence that may be relevant to the investigation and litigation. Planning will assist in meeting this objective. At the same time, it limits, as far as possible, the incurrence of unnecessary costs.

32 It is clear that, in order for any process of planning to be effective, the individuals responsible for the planning must have a basic understanding of the possibilities and limitations of the various forensic technology approaches so that appropriate consideration can be given to them as the investigation progresses.

33 The planning stage should include the appointment and/or identification of a coordinator who would be responsible for the overall management of the digital evidence recovery process, resource allocation/delegation and risk management. The individuals who would be involved in the digital evidence recovery process (*eg*, client IT personnel and/or forensic technology professionals) ought to be identified at an early stage.

34 In planning the recovery of electronically stored evidence, close attention must be given to the subsequent security and integrity of the evidence. A key, but often overlooked, issue is the advisability of ensuring that all subsequent movement of evidence is clearly traceable. There should also be a clear separation between the individuals involved in the collection process, and the client personnel whose activities are potentially relevant to the matter in hand.

35 A pre-search briefing session should be held for all data-gathering operations. This briefing session should include details of the following matters:

(a) The background to the case and any allegations made. Simply delineating scopes to various individuals, without providing them with an effective working understanding of the issues in the case, may lead to inefficiencies and duplication of tasks. It also increases the risk of potential sources of relevant data being overlooked.

(b) The key custodians and/or individuals actually involved or suspected to be involved in the subject matter of the litigation ought to be identified at the outset.

(c) The solicitors and/or external consultants will require a fairly detailed understanding of the nature of the business (in order to gain an understanding of the records that may be available) and the size of the business (this may indicate the volume of electronic evidence that may be seized/reviewed).

(d) All individuals involved in the process ought to be made aware of the environmental issues which could potentially impact the collection process. In this regard, detailed consideration ought to be given to the data infrastructure of the organisation under scrutiny. It should be noted that a broad level of understanding is unlikely to be of much utility – what is required is a detailed appreciation of the way various parts of the infrastructure interact. Further, all individuals involved in the process ought to be made fully aware of the legislative, regulatory, legal and commercial aspects of any search and document retrieval.

(e) A working timetable for the exercise ought to be carefully thought out and put in place at the start of the exercise. All steps decided upon ought to be carefully and transparently documented, not least because it may subsequently become necessary to justify the approach taken before a court or tribunal.

VI. PROFESSIONAL E-DISCOVERY / FORENSIC CONSULTANTS

36 A law firm may have little incentive to upgrade its e-discovery approach if it is already successfully billing for traditional services. Corporate counsel may be unaware of potential cost savings in the discovery phase of litigation, or it may have limited ability to engineer these savings through its law firm. Needless to say, what "works" in the short term – potentially "overcharging" clients – may not work in the long term since both vendors and buyers will need to stay competitive.

37 In this regard, modern e-discovery is a "buy," not "build," proposition. Few organisations can afford the investment required to build an efficient e-discovery infrastructure. However, the economics of the document analytics approach to e-discovery means that the outsourcing of the entire document management process may be desirable.

38 With outsourcing, the law firm gets out of the document management business, *eg*, photocopying, coding, imaging, rastering, boxing, shipping, *etc*, thus enabling it to reduce or reallocate support staff. With the review phase highly streamlined, lawyers can spend more time on higher-value strategic issues of the case, thereby offering better services to

their clients. Modernised e-discovery therefore offers the potential for both higher profit margins for law firms and reduced bills for corporate counsel.

39 Indeed, the question may be posed as to whether there is an ethical duty to retain an expert. Lauren Katz[23] suggests that there may be a duty to retain an appropriate e-discovery consultant in order to fulfill ethical duties of competence and diligence. It ought to be clear that a lawyer with inadequate technical knowledge cannot act with reasonable diligence in e-discovery. A useful example is the case of *Infinite Energy, Inc. v Thai Heng Chang*[24] where the plaintiff had applied for sanctions against defendant for failing to disclose a deactivated Yahoo! e-mail account. Defendant's counsel said that he believed it was impossible to retrieve deleted emails from a deactivated account, but did not offer evidence for this beyond his own assumption. The Court found that a lawyer violates his duty of diligence if he assumes that a certain technology does not exist.[25] Judges have expressed that they require expert assistance to make decisions that are complex and beyond their scope of expertise. Accordingly, an attorney who does not have a strong understanding of technical issues will need expert assistance in arguing complex technical issues.[26] Questioning an opposing party's production of documents and defending the reasonableness of one's own production may also require expert knowledge. Courts have held that where expert input is not used in support of the challenge/defence, the challenge/defence may be insufficient since the Court would have no factual basis to make the determination.[27] These concerns may arise in the local context as well, under the Legal Profession Act (Cap 161, 2009 Rev Ed) and the attendant secondary legislation promulgated thereunder.[28]

23 Lauren Katz, "A Balancing Act: Ethical Dilemmas in Retaining E-Discovery Consultants" (2009) 22 Geo. J. Legal Ethics 929 at p 935.

24 2008 WL 4098329.

25 *Supra* note 21, at p 938.

26 *Supra* note 21, at pp 938–939.

27 *Supra* note 21, at pp 938–939.

28 See, in particular, rule 12 of the Legal Profession (Professional Conduct) Rules (2000 Rev Ed) which provides: "An advocate and solicitor shall use all reasonably available legal means consistent with the agreement to which he is retained to advance his clients' interest."

VII. CONCLUSION

40 The obligations associated with the preservation of potentially relevant electronic evidence present various challenges to clients and lawyers. The proliferation of electronic data, the potential width of the obligations in the context of the discovery process, and the tension between the ends of justice and the means required to achieve those ends, all come together to create a complex web of considerations informing the process of preservation. For the solicitor, intertwined with these considerations is the difficulty of transitioning from the traditional "paper" perception of discovery obligations to an understanding of the complex effects that those obligations have in the context of the information age. An awareness of the potential issues that may arise as well as a specific understanding of clients' information systems is critical. While a sophisticated technical understanding of the complexities associated with the storage and retrieval of electronic documents may (at least at the present time) be beyond the realm of reasonable expectation, it is clear that it is no longer sufficient for the client or the practitioner to plead ignorance. Familiarity with the issues engaged is both expected and required.

41 In this context, the general trend observed in the major common law jurisdictions is that the courts are more than ready to tackle head on the difficulties associated with preservation of electronic evidence. This is to be welcomed. Justice requires that relevant and material documents ought to be placed before the body charged with the ascertainment of the truth. Further, the current trends underlying the developments in the rules governing the process of preservation represent the right balance between the competing principles informing those rules remains to be seen. In the meantime, the increasing levels of familiarity of both the courts and of practitioners provide a fascinating and fertile ground for development of the law on discovery.

INFORMATION GOVERNANCE – PITFALLS AND BEST PRACTICES

Kelvin KOW
LLB (Cambridge), LLM (Columbia)

I. INTRODUCTION

1 While the emphasis elsewhere in this conference had been on the problems and issues which arise when an electronic discovery ("e-discovery") order is served on a company, this panel sought to address how those problems could be avoided by corporate counsel in the first place, *viz*, by setting up effective information governance systems. The discussion was broken up into three components, each led by a different panel speaker.

2 The first speaker, Mr Wong Taur-Jiun (Head of Legal, Rabobank Singapore) shared his experiences in leading his department's transition from paper to electronic records (see Part II *infra*). The second speaker, Mr Tay Yu-Jin (Counsel, Shearman & Sterling LLP) gave us an overview on the challenges which in-house counsel might face, and also outlined some best practices to be considered for adoption (see Part III *infra*). The third speaker, Mr Richard Kershaw (Asia Managing Director, Catalyst Repository Systems) provided a computer forensic expert's perspective on the information governance issues which corporate counsel must come to terms with (see Part IV *infra*). The panel discussion was chaired by Mr Chua Lee Ming (General Counsel, Government of Singapore Investment Corporation).

II. TRANSITIONING FROM PAPER TO ELECTRONIC RECORDS

3 The transition from paper to electronic records has widespread implications for a company's information governance. A brief case study on the transition made by Rabobank Singapore ("Rabobank"; also referred to, where appropriate in the context, as "the bank") may provide some guidance for corporate counsel and administrators contemplating such a transition.

4 The transition to electronic records was a pilot project for Rabobank and limited to its legal department ("Rabobank Legal"). From the outset, it should be noted that the transition was possibly more manageable for Rabobank Legal as compared to a large local bank. The reason for this is that Rabobank, being a foreign bank in Singapore which provides only wholesale banking services, had a smaller scale and scope of business operations as compared to larger local banks which may provide retail banking services as well. Notwithstanding, some lessons may be gleaned from Rabobank Legal's experiences.

5 It should also be noted that the impetus for Rabobank Legal's transition from paper records to electronic records arose, not from any grand legal thesis, but rather, from the 2008 financial crisis which created cost pressures for businesses across the board. One clear avenue for reducing costs was to cut down on office rental space and out of that was borne a real commercial need to reduce organisational archival and storage space. It would not be surprising that similar cost pressures may convince other businesses to make a similar transition.

6 This part of the discussion will be addressed in three sub-parts, namely:

(a) Feasibility study;

(b) Implementation; and

(c) Future challenges.

1. Feasibility study

7 In Rabobank's experience, a feasibility study was commissioned to explore how the transition from paper to electronic records could be implemented. This was itself done in three phases.

(a) First phase: survey of the regulatory environment

8 Rabobank, being a bank, is highly regulated in Singapore. A survey of the regulatory environment in Singapore was accordingly required as part of the first phase of the feasibility study. Rabobank Legal's first consideration was the Monetary Authority of Singapore's ("MAS'") Guidelines ("the MAS Guidelines"), which established that Rabobank Legal was allowed to

convert its paper records into electronic ones. The MAS Guidelines read, in relevant part, as follows:

> **Guidelines on Risk Management Practices - Internal Controls (February 2006)**
>
> 3.4.2 An institution should also establish the minimum retention period for taped telephone conversations and documents, taking into account the relevant laws, rules and regulations. ***Financial transaction documents may be retained*** *as originals, copies, on microfilm* ***or in electronic form****, taking into account whether such forms are admissible in court or in compliance with regulatory requirements.* Such records should be properly kept and stored in a manner that is reasonably practicable to retrieve.
>
> …
>
> **MAS Notice 626 (prevention of money laundering)**
>
> 10.3 ***A bank may retain documents*** as originals or copies, in paper ***or electronic form****,* or on microfilm, provided that they are admissible as evidence in Singapore.
>
> [emphasis added in italics and bold italics]

9 Rabobank Legal also reviewed a number of other relevant local legislative provisions. Two legislative acts were of particular significance, *viz*, the Evidence Act (Cap 97, 1997 Rev Ed) ("Evidence Act") and the Electronic Transactions Act (Cap 88, 1999 Rev Ed) ("ETA").[1] Section 35 of the Evidence Act governs the admissibility of electronic records and computer output. Section 6 of the ETA establishes the legal recognition of electronic records, while s 9 of the same Act sets the conditions for the lawful retention of electronic records.

10 Following its review of the relevant legislation, Rabobank Legal came to a determination on how it could keep its electronic records lawfully. This informed the document retention methods and policies which were put in place later.

(b) Second phase: studying the information technology systems

11 The second phase of the feasibility study involved studying the bank's information technology ("IT") systems. Rabobank Legal had to determine whether the bank's IT resources and capabilities were able to support the transition to a system of electronic record keeping. It also had to consider

1 It should be noted that the ETA has been repealed as of 1 July 2010 and re-enacted as the Electronic Transactions Act 2010 (No 16 of 2010).

the costs of the available data storage technology and the amount of storage capacity required. Finally, even when it was determined that the bank could afford the hardware and software required for the transition, there was still a need to ensure that technical support was available to tackle any problems the IT system encountered.

(c) Third phase: drafting policies and obtaining approvals

12 The final phase of Rabobank Legal's feasibility study involved drafting workable document retention policies and obtaining the necessary approvals from senior management.

2. Implementation

13 When it was determined from the above-mentioned feasibility study that the transition to electronic records was feasible and the necessary approvals were given, Rabobank Legal moved to implement its transition. This was carried out over a relatively short period of about six months.

14 Today, Rabobank Legal functions significantly differently *vis-à-vis* the time when it relied on paper records. Emails and draft documents are no longer printed. The department has moved to a functional mailbox which allows the entire department to access a single mailbox at the same time. Emails are no longer stored on individual employees' computers, but rather, are stored centrally. In addition, the department has adopted the "Enterprise Vault"[2] system which provides for the automatic archival of documents. The "Enterprise Vault" system also has the advantage of reducing mailbox space required through the use of electronic tags. Emails which are more than seven years old are removed from the system and stored on compact discs.

2 Enterprise Vault is a product of Symantec. According to Symantec, Enterprise Vault provides integrated content archiving capabilities, enabling users to store, manage and discover unstructured information across the organisation. For more information, see <http://www.symantec.com/enterprise-vault>.

15 The original hard copy transaction documents are kept in physical vaults. However, they are also processed as softcopy documents in the Portable Document Format ("PDF")[3] and posted onto "SharePoint",[4] an enterprise collaboration software. These files are tracked using a document management system that was developed in-house.

3. Future challenges

16 Despite the smooth transition in the Rabobank case study, there are further challenges that may emerge in the near future.

17 First, Rabobank's electronic record-keeping system is not implemented bank wide. As a large international organisation, the bank faces problems arising from the inconsistent use of IT. For example, different parts of Rabobank worldwide use different versions of the Microsoft Windows operating system. Issues of compatibility may arise and standardisation efforts may have to be made.

18 Second, the storage of electronic data inevitably engenders further issues. One straightforward issue is the necessity to acquire more storage capacity regularly as the electronic records kept by the bank increase. A more difficult issue would be the potential of system-level data corruption, which could prove to be a nightmare scenario. Backup and contingency plans must be made to prepare for such possibilities.

19 Finally, there is the challenge of the retrieval of relevant material, *viz*, whether the bank is able to find out what it really needs. This issue may, however, be addressed with improvements in search technology.

3 The Portable Document Format is a file format produced by Adobe Systems. It is a global standard for capturing and reviewing information from various computer applications. For more information, see <http://www.adobe.com/products/acrobat/adobepdf.html>.

4 SharePoint is a product of Microsoft. According to Microsoft, SharePoint allows people to set up web sites to share information with others, manage documents from start to finish, and publish reports to help in decision making. For more information, see <http://sharepoint.microsoft.com/en-us/product/capabilities/Pages/default.aspx>.

III. MANAGING ELECTRONIC DATA AND E-DISCOVERY IN LITIGATION / ARBITRATION

20 To save space and costs, we use technology to create and digitise information. We think that such information is easy to delete, but the truth is that complete deletion is almost impossible. Information is being created all the time, and the advent of the technological age has exponentially increased the rate of creation of information. The challenge for us (and, in particular, information managers) is to manage all this information.

21 There is a tension which information managers must deal with. On the one hand, we have to keep some of the information we create. There might be document retention regulations which we have to comply with, or perhaps, certain information is saved in general anticipation of litigation and arbitration proceedings. On the other hand, we are obliged to disclose the documents we retain when ordered to produce them. This might be pursuant to, *inter alia*, a court order for discovery,[5] a government investigation, *etc*. The difficult balance which every corporation needs to strike is exactly how much information to retain so that its interests are advanced overall.

22 The obligation to preserve documents has long existed in common law jurisdictions, even back when records were predominantly (or even solely) paper records. We may be less familiar, however, with the technology and the processes with which we capture, organise and disclose information in compliance with a discovery order or a regulatory requirement. Against the sea change engendered by the electronic data explosion, the corporate counsel's traditional role in an organisation is beginning to evolve. Corporate counsel cannot work in a vacuum; instead, it has become critical for corporate counsel to link up and sync in with other key technology officers in the company such as the Chief Information Officer, the Chief Information Security Officer and/or the Chief Technology Officer.

5 In the Singapore context, see, for example, Order 24 of the Rules of Court (Cap 322, R 5, 2006 Rev Ed). Generally, a party to a litigation has an obligation to disclose to the opposing party all documents which are, or have been, in his possession, custody or power that are relevant to the issues in dispute, subject to the requirement that discovery must be "necessary either for disposing fairly of the cause or matter or for saving costs".

23 Litigation in common law countries is seeing an exponential increase in the material that may have to be disclosed for the purposes of discovery. This creates onerous obligations for companies. As in other areas of corporate decision-making, it is wise to be prepared for the worst. As such, it is probably safe for corporate counsel to assume that at some point, the company will need to disclose documents in some form of investigation. Even if the company is a peripheral party to a dispute, it might well be subject to information preservation obligations which require the company to issue a "litigation hold" (also known as a "legal hold").

24 Corporate counsel should be familiar with the concept of a litigation hold. When a company "reasonably anticipates" litigation or arbitration proceedings, it should issue a "litigation hold" notice to its employees to preserve relevant documents. This may involve the suspension of the usual disposing or processing of paper and/or electronic records. Although external counsel, as officers of the court, bear responsibility to issue such litigation holds, corporate counsel should be aware that they often also have legal obligations to issue litigation holds. In the United States of America ("the USA"), these obligations have arisen in the context of investigations and regulatory compliance. Other jurisdictions are expected to follow the USA approach, if they have not already done so. It should also be noted that sanctions for non-compliance can apply to companies as well as to specific individuals.

25 As for document retention policies, there is unfortunately no "one size fits all" answer. What kind of document retention policy an organisation adopts depends on its business. Investment bankers are known for destroying everything except the "bible" of execution documents, but that approach might not be suitable for other organisations. In any case, the virtues of a robust document destruction policy must be highlighted. Such a policy will dramatically reduce the risk exposure in terms of what a company can be ordered to produce. However, corporate counsel should note that document destruction policies should not be frequently tweaked, as fickle document destruction policies would usually raise alarm bells.

26 With regard to retained documents, email and other forms of electronic messaging pose particular dangers. It is not unusual for a case to turn on a few compromising emails which no one expected to see the light of day. As such, it is critical to remind employees that they should never assume that good business relations with another company will persist or

that the emails which they send externally or internally will forever remain private. Indeed, increased caution is counselled especially in view of the proliferation of instant electronic messaging services such as BlackBerry Messenger[6] and WhatsApp Messenger,[7] as well as social media networks like LinkedIn[8] and Facebook.[9] The problems raised by electronic messages will only become more complex.

IV. FOUR CRITICAL ASSESSMENTS TO BE MADE FOR MANAGING E-DISCOVERY

27 It is no surprise that the objectives of external lawyers and consultants differ from those of their clients' in-house counsel. One of the overriding concerns of corporate counsel is cost. To get the best return on a limited corporate budget, in-house counsel should do their best to understand the technology and options available to their organisations for their information governance functions, including pre-existing technology and processes. This will help them to arrive at optimal solutions for their organizations.

28 Corporate counsel might already be familiar with the Electronic Discovery Reference Model ("EDRM"). The EDRM was created to develop resources and best practices for e-discovery consumers and providers.[10] The stages of the EDRM may be visually represented as follows:[11]

---

6 BlackBerry Messenger is a mobile messaging application for users of BlackBerry mobile phones. This messenger allows users to exchange text messages without going through the traditional Short Message Service ("SMS") network. See <http://www.blackberry.com>.

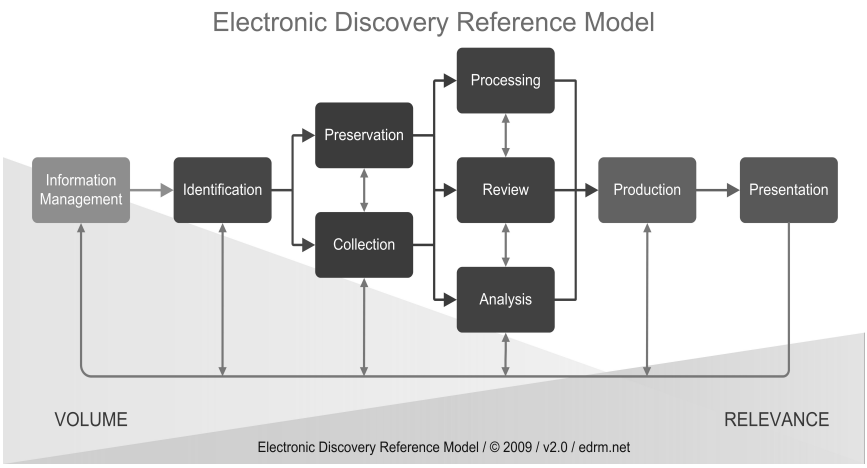
7 WhatsApp Messenger is a cross-platform mobile messaging application which allows users to exchange text messages without going through the traditional SMS network. See <http://www.whatsapp.com>.

8 LinkedIn is a large professional network which allows users to exchange knowledge, ideas, and opportunities with a broader network of professionals. See <http://www.linkedin.com>.

9 Facebook is a social networking site that allows users to create personal profiles, add other users as "friends", exchange messages, join common interest groups, *etc*. See <http://www.facebook.com>.

10 For more information on EDRM, see generally <http://www.edrm.net>.

11 The EDRM website provides detailed explanations of the various stages. See <http://www.edrm.net/resources/edrm-stages-explained>. Copyright to the diagram belongs to EDRM (edrm.net).



29 The EDRM is a wonderful theoretical model but it may be difficult to draw practical guidance from it. It is suggested that corporate counsel treat the EDRM in a similar way to an International Organisation for Standardisation ("ISO") standard[12] or a compliance standard like the Control Objectives for Information and related Technology ("COBIT").[13] It can be a helpful starting point for corporate counsel to map the high-level information related activities going on within their organization to these theoretical categories. Used in this way, the EDRM would help corporate counsel to understand what information governance capabilities their organisations already have which can support the need for data in the litigation process. From there, corporate counsel can go on to consider which parts of their company's e-discovery management process must be established or augmented, and whether the same should be done by setting up the capabilities in-house or outsourcing the functions externally.

30 There are currently no established standards for the implementation of e-discovery management, but corporate counsel are recommended to undertake the following four sets of assessments, each of which will be elaborated upon *in seriatim*:

12 The ISO is the world's largest developer and publisher of International Standards. It is an international network of standards that enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society. See <http://www.iso.org>.

13 The COBIT is a set of best practices for information technology, created by the Information Systems Audit and Control Association. See <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>.

(a) Assessing existing enterprise infrastructure;

(b) Assessing additional technology that is available;

(c) Assessing the human resources available within the company; and

(d) Assessing what kind of external help is required.

1. Assessing existing enterprise infrastructure

31 It is not unusual for corporate counsel to go to great lengths to learn where the information is stored within their organisations when their companies contemplate the prospect of litigation. This is so that they can establish their organisational "litigation readiness maps". However, this effort is often expended needlessly as oftentimes some other party in the organisation already has the necessary knowledge regarding the company's information network. This might be the Chief Information Officer, the Chief Information Security Officer and/or the Chief Technology Officer. In the course of their work, corporate officers performing compliance or information security functions invariably have to identify the company's different types of information assets, as well as document where they are in both physical and logical formats. That is a fantastic starting point for assessing both the location of information assets and the nature of existing enterprise infrastructure.

2. Assessing additional technology that is available

32 Following the first stage, corporate counsel should have a good understanding of their company's information assets and the enterprise infrastructure on which they reside. Before moving on, one should be reminded that, ultimately, the point of enterprise infrastructure is to conduct business and not to prepare for litigation. Accordingly, one should not get carried away with changing the enterprise infrastructure for the dominant purpose of pre-empting or preparing for litigation.

33 Having said that, the first step in the second stage of assessments is to look at the existing enterprise infrastructure and the features which are already available. One may then consider how the company can leverage on its infrastructure's existing capabilities to assist the legal department with little additional investment and policy mapping.

34 The second step is the introduction and implementation of an enterprise content management system. It is important to realise that a content management system (such as "Enterprise Vault" used by Rabobank, as discussed above) is *not* an e-discovery system. The two kinds of systems, *viz*, a content management system *contra* an e-discovery system, reach different objectives. An enterprise content management system sets up a centralised repository which reduces the documents and storage used for electronic record keeping. However, the material contained in that content management system might not be ready for the e-discovery process.

35 Therefore, there is also a need to explore e-discovery specific technology for the analysis, review and production of documents. Again, there are different options available. The simple solution is to buy hardware and software off the shelf and install them in-house. There are now also dedicated appliances which can be put onto the corporate network. This allows initial discovery processes to be conducted behind the company's firewall. The installation of these appliances is therefore the preferred option for organisations with special requirements for, *inter alia*, intellectual property security. However, these require additional investment in software licensing, the hardware to run such software, and the training for and salaries of employees to run such a system. In-house systems are also more limited in functionality and are of course also limited by the amount of hardware that the organisation can afford. Finally, there are cloud solutions for organisations which decline to invest in e-discovery technology within their own enterprise infrastructure or have greater requirements for performance and scale.

36 Corporate counsel should be aware of the following points when it comes to assessing e-discovery tools.

> (a) First, e-discovery technology is generally created in the USA. This means that the technology generally works optimally when handling the English language, but may experience difficulties handling multibyte Asian language character sets like Chinese, Japanese and Korean (popularly known as "CJK"). Furthermore, the technical support may only be available during working hours in the USA. In Asia, where documents in languages other than English may be discoverable, it is important to encourage service providers to develop e-discovery tools which can handle other languages as well.

(b) Second, note that any e-discovery tool of choice should have analytics capabilities as this will help to reduce costs. With that said, it is good sense to be wary of "feature creatures" *ie*, vendors selling e-discovery tools by listing features and implying that these will solve all e-discovery problems. No currently existing e-discovery tool is a panacea for e-discovery issues. Any tool will require effort to implement and e-discovery technology providers should provide a consultative approach to solve the unique problems faced by different companies.

3. Assessing the human resources available within the company

37 Today's corporations need data for varied purposes. We are increasingly seeing dedicated groups being created to pool information together for different purposes. "Incident Response" groups, *viz*, groups dedicated to addressing and managing the aftermath of a security breach or attack, started out primarily to deal with virus outbreaks. This then expanded to data needed for internal investigation. Now we see "Litigation Management" Groups, and recently, we have seen the rise of "Internal Request for Data" Groups. Regarding the latter, they are neither only an e-discovery response function, nor purely the old style "incident response". Rather, their objective is to understand where the information is located within an organisation and find it for a whole range of reasons, such as a virus response, an internal or regulatory investigation response, a litigation response, compliance requirements, audit testing and so on. These often require very different skill sets – someone assessing and containing a malware outbreak requires a different skill set from someone conducting a forensic examination.

38 It is important to understand what technical skill sets the company will need to form those teams. As before, corporate counsel should look first at what resources they already have in-house. Where there are gaps to be filled, one may consider whether those skill sets should be recruited and brought in-house, and also consider how those skill sets can be maximised through, *inter alia*, double-hatting.

4. Assessing what kind of external help is required

39 When engaging external service providers, it is important to do due diligence on them – whether they are software vendors, consultants or external counsel. When looking at external support, especially on cross-border matters, external counsel need to understand, for instance, (a) the difference between common law and civil law jurisdictions; and (b) whether the legal issues of privilege and confidentiality arise.

40 External counsel should also be queried on their understanding of technology. Their ability to interface with a company's IT department or vendor is critical to a successful working partnership. Further, one should be aware of language issues that arise for companies with a regional or global reach. These may surface in a variety of contexts, from communications with the company's IT administrator based in China to the technical display of a particular language in any given review.

41 Finally, there are also a variety of data protection regimes which must be dealt with. It is crucial that external counsel do not mistake privacy laws for data protection laws as the two are different. Anecdotally, there has been an instance in which legal counsel from the USA misunderstood Japan's data protection laws for privacy laws. They proceeded to build a very expensive review process on that basis which unfortunately turned out to be irrelevant.

42 In summary, when any kind of information response team is activated, it must first consider the purpose of its endeavour. The requirements for data collection differ depending on whether the information is required for an investigation, for litigation or for arbitration. The response team should include: general counsel who understand what data will be relevant to a given matter, a business leader who understands where the company sees that data from a day-to-day perspective, an IT administrator who understands where that data really is, and finally, an in-house or external forensics consultant who can help determine how to preserve that data.

V. CONCLUSION

43 It cannot be gainsaid that information governance for today's corporate organisations is a complex and difficult task. There is a continual need for corporate counsel to learn from each other's experiences, to be kept

abreast of legal developments by litigation/arbitration practitioners and to be aware of the fresh perspectives offered by the rapidly developing field of computer forensics. The panellists hope that the discussions had been helpful in giving corporate counsel some brief guidance on their roles as the governors of corporate information.

SOME INTERNATIONAL DEVELOPMENTS IN ELECTRONIC EVIDENCE

Stephen **MASON**[*]
BA (Hons) (History and Educational Philosophy), MA, LLM, PGCE (FE)

I. INTRODUCTION

1 This article considers two topics that are directly related to digital evidence, encrypted data and cloud computing, and one topic, obtaining evidence from other jurisdictions, that affects all forms of evidence, but has become more significant because of the volume and geographical spread of digital data that invariably accompanies even the simplest of civil litigation or criminal prosecution work.[1] Some remarks are offered in relation to the chaotic nature of the changes to legal information as a result of the development of digital communications, such as how lawyers and judges obtain access to information, books and articles, and whether the plethora of data, much of which is flimsy in content, needs to be the topic of guidance from professional bodies.

II. OBTAINING EVIDENCE FROM OTHER JURISDICTIONS

2 There are wide variations between what happens in practice and how judges in different jurisdictions deal with obtaining evidence from other jurisdictions. In discussing this topic, consideration will mainly focus on the response by judges and organisations in the United States of America, which illustrates the nature of some of the problems that might be necessary to address by means of an international convention or treaty.

---

* Stephen Mason (stephenmason@stephenmason.eu) is a barrister. He is the author of *Electronic Signatures in Law* (Cambridge University Press, 3rd Ed, 2012) and general editor of *Electronic Evidence* (LexisNexis Butterworths, 2nd Ed, 2010) and *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

1 This article was developed from a presentation given by the author at the International Conference on Electronic Litigation, 11–12 August 2011, (Supreme Court of Singapore and the Singapore Academy of Law) that also included a short discussion of digital wills, including case law from Canada, South Africa, Norway and the United States of America. These cases are dealt with in full in Stephen Mason, *Electronic Signatures in Law* (Cambridge University Press, 3rd Ed, 2012), Ch 6.

3 In criminal matters, attempts are made to acquire evidence and obtain the cooperation of potential witnesses by agreement, to such an extent that the Crown Prosecution Service in the UK has a liaison officer in Washington expressly to facilitate the exchange of evidence and witnesses. The Global Prosecutors E-Crime Network was partly set up to develop a coordinated approach for dealing with electronic crime.[2] More formal provisions include multilateral conventions (such as the 1959 European Convention on Mutual Assistance in Criminal Matters, and the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union of 29th May 2000, which supplements the 1959 convention), bilateral treaties between States (such as the 1994 Treaty Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters), other arrangements such as the Harare Scheme (currently being updated), that is relevant to Commonwealth countries and which is a voluntary Scheme Relating to Mutual Assistance in Criminal Matters, and memoranda of understandings. However, it is not always the case that an organisation is willing to cooperate with the prosecuting authorities, as in the prosecution of *Yahoo!* in Belgium for refusing to provide e-mail correspondence to the Belgian investigating authorities in a case involving credit card fraud.[3]

4 In civil matters, it is probably correct to infer that evidence and witness statements are generally obtained for inclusion in civil proceedings by agreement. However, the main international mechanism for the obtaining and taking of evidence is the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, which entered into force on 7 October 1972. Unfortunately, the obtaining of evidence by means of a Letter of Request can be time consuming.[4] In addition, the Convention is

2 See <http://www.iap-association.org>.

3 For the decision in the Court of First Instance in Dendermonde, see Corr. Dendermonde 2 maart 2009, onuitg.; for the appeal to the Court of Appeal in Ghent, third chamber, sitting in criminal matters, see Gent 30 juni 2010, onuitg.; and for the decision before the Court of Cassation of Belgium, see Cass. 18 januari 2011, nr. P.10.1347.N – all of these judgments are translated into English and published in (2011) Digital Evidence and Electronic Signature Law Review 8.

4 A practical response to this issue was ordered by Magistrate Judge Margolis in *Valois of America, Inc. v. Risdon Corporation*, 183 F.R.D. 344 (D. Conn. 1997), in that the parties were ordered to confer to determine which documents were to be released, failing which they were to apply to the court again.

not necessarily considered to be mandatory by every signatory, as expressed by the United States Supreme Court in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*,[5] echoing the comments of Keenan, DJ in *Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Company*,[6] in which he observed, at 28, that the United States did not intend to abandon the practice of extraterritorial discovery when agreeing to comply with the Hague Convention, and indicated that the Hague procedures were neither exclusive or mandatory.[7] In the European Union, Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters[8] applies to all the Member States of the EU with the exception of Denmark,[9] which has not participated in the Regulation, and is therefore not bound by it nor subject to its application. The Regulation provides for direct contact between the courts in the Member States. There is a standardised request form that is included in the annex to the Regulation.

1. 'Blocking' legislation

5 This part of the article will provide a brief sketch in the context of the United States[10] regarding 'blocking' legislation (that is, legislation that either prevents evidence from being sent abroad, or that makes it an offence to send evidence abroad), and the approach taken by judges in the United States to the obtaining of evidence from abroad for legal proceedings in the United States.

5 482 U.S. 522 (1987).

6 105 F.R.D. 16 (S.D.N.Y 1984).

7 Opinion is divided as to whether the Convention is mandatory or not mandatory, on which see Hague Conference on Private International Law, *The Mandatory/Non-Mandatory Character of the Evidence Convention Le Caractere obligatoire ou non Obligatore de la Convention Preuves*, (Preliminary Document No 10 of December 2008) (this document considered previous reports on this matter, and provides references to a number of academic articles).

8 OJ L174, 27.6.2001, pp 1–24.

9 *Ibid*, at [22] of the Preamble.

10 For a detailed treatment, see Gary B. Born and Peter B. Rutledge, *International Civil Litigation in United States Courts* (Aspen Publishers, 4th Ed, 2006).

(a) The failure to comply with an order to disclose does not prevent a trial from taking place

6 The Supreme Court has held that judges in the United States may order the production of documents that are governed by foreign laws that make it an offence to send evidence abroad, even if the law has a valid purpose, although the dismissal of a complaint with prejudice is not justified for failure to comply with the order for disclosure.[11] In *Société Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*,[12] the Swiss holding company sought to repatriate assets (valued in 1958 at US$100m) seized by the Alien Property Custodian during World War II. The trial judge issued an order for the production of documents that had not been released by the petitioner, but a certain amount of the evidence could not be revealed because to do so would have constituted a breach of article 273 of the Swiss Penal Code prohibiting economic espionage, and article 47 of the Swiss Bank Law, relating to the secrecy of banking records. The District Court of Columbia dismissed the complaint with prejudice, a decision that was affirmed by the Court of Appeals for the District of Columbia Circuit.[13] The Supreme Court granted certiorari. In the Supreme Court, Harlan J, who delivered the opinion of the court, considered the policies underlying the Trading with the Enemy Act and the policies made explicit by Congress when the Act was amended in 1941, together with the provisions of the Fifth Amendment. In this instance, the Supreme Court determined that dismissal of the complaint with prejudice by the lower court was not justified, the judgment of the Court of Appeals was reversed, and the matter remanded to the District Court for further proceedings. In essence, the Supreme Court accepted that the petitioner had cooperated as much as it could to produce evidence under the requirement to disclose. However, because it had the burden of proof of showing it was not the enemy within the meaning of the Act, its failure to adduce relevant evidence at trial enabled the trial judge to draw justified inferences that were not favourable to the petitioner. Thus the petitioner

11 In *Lynondell-Citgo Refining, LP, v. Petroleos de Venezuela, S.A.*, 2005 WL 1026461 (S.D.N.Y.), Motley J upheld an adverse inference instruction because the defendant consistently failed to produce relevant corporate minutes – one of the reasons given was that to do was would be in violation of Venezuelan law, although the report does not set out the details of the law that it was claimed would be violated.

12 357 U.S. 197 (1958).

13 243 F.2d 254 (D.C Cir. 1957).

was not forced to produce the evidence, but had to face the consequences at trial of not adducing sufficient evidence to meet the burden of proof.

(b) The speculative nature of the penalties is no reason for failing to provide the evidence

7 In the United States Court of Appeals for the Second Circuit, Kaufman CJ gave the judgment for his brother judges in the case of *United States of America v. First National City Bank*,[14] in which First National City Bank of New York (Citibank) was served with a subpoena in connection with a federal Grand Jury investigation of alleged violations of the antitrust laws by a number of its customers. A number of documents were required to be produced that were located in the bank's offices in New York City and Frankfurt, Germany, relating to any transaction in the name of (or for the benefit of) its customers C. F. Boehringer & Soehme, G.m.b.H., a German corporation, and Boehringer Mannheim Corporation, a New York corporation. Citibank produced materials that were located in New York, but refused to produce or divulge any documents located in Frankfurt. The bank did not even inquire or determine whether any relevant papers were overseas, and William T. Loveland, the vice-president responsible for the decision to defy the subpoena, appeared before the members of the Grand Jury and asserted that the bank's action was justified because compliance would subject Citibank to civil liability and economic loss in Germany. The court heard expert evidence on two occasions, and it became clear that:

(a) Bank secrecy was not part of the statutory law of Germany;

(b) It was in the nature of a privilege that could be waived by the customer but not the bank;

(c) A violation of bank secrecy could subject the bank to liability in contract or tort but not to criminal sanctions or their equivalent;

(d) It was a simple matter for a bank customer to obtain an *ex parte* restraining order enjoining a bank from disclosing privileged material;

(e) A violation of such an injunction would be punished under a general provision of the criminal law governing violations of court orders;

14 396 F.2d 897 (2d Cir. 1968).

(f) Citibank would have a number of valid defenses in the event Boehringer ever initiated legal action; and

(g) In criminal proceeding in Germany, bank secrecy does not provide a basis for refusing to obey a court order to provide evidence.

8 Pollack J concluded that Citibank had failed to provide a sufficient reason for failing to comply with the subpoena.[15] Kaufman CJ indicated, at 900:

> … that it was manifest that Citibank would not be subject to criminal sanctions or their equivalent under German law, that it had not acted in good faith, and that there was only a "remote and speculative" possibility that it would not have a valid defense if it were sued for civil damages. Accordingly, he adjudged the bank and Loveland to be in civil contempt and fined the bank $2,000 per day for its failure to act; he sentenced Loveland to 60 days' imprisonment. For the reasons stated below, we conclude that Judge Pollack's order was justified and affirm.

9 In his judgment, Kaufman CJ illustrated that this was not a case where there was a risk of the imposition of criminal penalties, but '… a possible prospective civil liability flowing from an implied contractual obligation between Citibank and its customers that, we are informed, is considered implicit in the bank's license to do business in Germany' (at 901). In evaluating the contention by Citibank that it should be excused because of the suggested conflict between German and United States requirements, it was determined that Citibank had failed to justify its position of disobedience. It was necessary to "balance the national interests of the United States and Germany and to give appropriate weight to the hardship, if any, Citibank will suffer" (at 902).

10 The alleged hardships the Citibank claimed it would be subjected to if it complied with the subpoena comprised two grounds: that C. F. Boehringer & Soehme, G.m.b.H. would enforce economic reprisals against Citibank, and it would lose foreign business that in turn would harm it and the economic interests of the United States, and second, Citibank indicated that it would be subjected to civil liability in legal action by C. F. Boehringer & Soehme, G.m.b.H. Both arguments, weak as they were, were

15 Francis, MJ held that the reasons put forward to justify withholding the discovery of documents of foreign patent prosecution documents on the basis of attorney-client privilege were not acceptable as being inadequate in *In Re Rivastigmine Patent Litigation*, 237 F.R.D. 69 (S.D.N.Y. 2006).

rejected. The first, on the basis that the protection of the foreign economic interests of the United States must be left to the appropriate departments of the government. The second, that the court agreed with Pollack J that the risk of civil damages was slight and speculative. In addition, it was noted that Citibank had failed to produce or segregate documents or records which reflected the bank's own work product, and the expert testimony indicated that disclosure of such material would not violate any policy of bank secrecy. Since the Grand Jury was shortly to be dismissed, the court directed that the mandate be stayed for a period of seven days from the date of the filing of the opinion to permit Citibank, if it decided to, to apply to the Supreme Court for a further stay or other relief.

(c) Actions involving subsidiaries of companies incorporated in the United States

11 Judges are generally not persuaded to allow United States corporations to conduct business through wholly owned foreign companies to avoid the payment of taxes in the United States, as indicated in the case of *United States of America v. Vetco Inc.*[16] In this instance, the Court of Appeals for the Ninth Circuit affirmed an award against Vetco for failing to produce documents requested by Internal Revenue Service, even though doing so would, Vetco argued, violate article 273 of the Swiss Penal Code that referred to making business secrets available to a foreign governmental agency, amongst other organisations. Expert evidence demonstrated that it would be a defence for a Swiss company to produce documents pursuant to an order of a United States Court enforcing a summons issued by the Internal Revenue Service.

(d) Comity

12 Although the provisions of blocking legislation may be prayed in aid to prevent disclosure, nevertheless wider issues relating to comity between

16 691 F.2d 1281 (9 Cir. 1981); conversely, a non-party with a subsidiary corporate entity located in the United States can be ordered to disclose documents from another jurisdiction, for which see *Dietrich v. Bauer*, 2000 WL 1171132 (S.D.N.Y.), where the test lies in control, not the location; the party relying on the foreign law has the burden of establishing that the foreign law prevents the production of the evidence, for which see *Columbia Pictures, Inc., v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007), 69 Fed.R.Serv.3d 173.

nation states are also highly relevant, as illustrated in the case of *Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Company*,[17] where the plaintiffs refused to provide certain documents that were either considered to be covered by executive privilege or covered by the provisions of article 1 of French Law No 80-538, prohibiting a French party for disclosing any document if such a disclosure would infringe upon the sovereignty, security or essential economic interests of France, on pain of a criminal penalty of up to six months imprisonment and a fine of up to 120,000 Francs (article 3). Keenan DJ indicated that the claim of executive privilege was not sufficiently made out, partly because there was insufficient evidence to determine whether the documents to be disclosed were similar to state secrets, and partly because the asserted claim of confidentiality was only addressed to the release of information to a foreign public authority. In respect of the claim under the statute, the learned judge considered two questions: whether the court had the power to order the production of documents in France, taking into account the provisions of articles 11 and 21 of the Hague Convention which permits a party to refuse to give evidence, and if the court found the provisions of the Convention to be discretionary, whether considerations of comity compelled the court to exercise judicial restraint and not order production.

13 In reaching his decision, Keenan DJ carefully considered the purpose of the Convention and the issue of comity and judicial restraint, referring, at 26–32, to the Restatement (Second) of Foreign Relations Law of the United States (1965). The learned judge concluded that there was little evidence to demonstrate that the French statute had been or would be enforced, and as a result there was no real threat of prosecution; that the plaintiffs had a choice, that they could withdraw their complaint or produce the documents that were requested, or face the risk of prosecution under French law. Respecting comity, while Keenan DJ indicated he was sensitive to the need for comity and to respect the law of foreign states, he also made pertinent comments, at 32, in respect of the purpose of discovery:

> Plaintiffs come into this Court seeking the protection of United States laws that enable injured persons to recover for breach of contract. Plaintiffs cannot avail themselves of these benefits, yet neglect their accompanying responsibility to disclose all relevant facts to their adversary. … This is particularly true in view of plaintiffs' connection with the French government and the questionable motives behind passage of the French

17 105 F.R.D. 16 (S.D.N.Y 1984).

> statute upon which plaintiffs rely. To permit plaintiffs to evade their discovery responsibilities in this case would unfairly disadvantage the defendant and make a mockery of our judicial system.

14 The plaintiffs were ordered to produce the relevant documents, and the court reserved judgment on the nature of the sanctions that would be imposed for failure to comply with the order.[18] Requests by a foreign party to a case for a protective order to limit discovery in the United States to procedures provided for in the Hague Convention also tend not to be accepted, as in *Adidas (Canada) Limited v. SS Seatrain Bennington*,[19] where Leval DJ considered that the Convention was prepared in part because civil law countries considered the taking of evidence to be a judicial function, thus attempts by litigants to obtain discovery within their territory to be a usurpation of their sovereignty. The applicant's interpretation that nothing should take place that infringed the sovereignty of a signatory was dismissed on the basis that it would give an extraordinary and unfair advantage to a litigant from France in the United States. Considering the attempt to pray in aid the French blocking Law No 80-538 of 16 July 1980, the learned judge indicated, at 3, the absurdity of the French position:

> It is inconceivable that Law No. 80-538 is to be taken at face value as a blanket criminal prohibition against exporting evidence for use in foreign tribunals. For if it were, French nationals doing business abroad would be at the mercy of their business counterparts: they would be unable to redress breaches and frauds committed against them by suit in foreign courts since they would be barred from supporting their claims with their documents.

(e) Objections on the grounds of privacy laws

15 In *Reino de Espana v. American Bureau of Shipping*,[20] in dealing with a request by the American Bureau of Shipping to compel the Spanish to disclose records (e-mails in particular) in litigation concerning one of the largest oil spills in history, Ellis, MJ roundly rejected claims by the Spanish

18 *Bodner v. Paribas*, 202 F.R.D. 370 (E.D.N.Y. 2000) in which United States Magistrate Judge Go traversed relevant case law, indicating that the blocking laws referred to were not relevant, that one of the laws referred to "was intended to prevent recurrence of past bigotry and anti-Semitic and racists acts that are the very events that plaintiffs here seek to investigate" (at p 376), and that the defendants did not face a realistic risk of prosecution; the party seeking the application failed to show good cause, having the burden of persuasion.

19 1984 WL 423 (S.D.N.Y.), 1984 A.M.C. 2629.

20 2006 WL 3208579 (S.D.N.Y.).

that to search e-mail accounts would violate privacy laws. Unfortunately, the report does not indicate the precise law or article that Spain prayed in aid in its argument.

(f) Whether there is a realistic risk of prosecution

16 In considering laws that threatened prosecution, Leval DJ indicated the rationale of the French in particular in *Adidas (Canada) Limited v. SS Seatrain Bennington*,[21] which was behind the various attempts by the French to prevent evidence from being sent to other jurisdictions (at 3 and in footnote number 4 at 4):

> The legislative history of the statute [Law No. 80-538] gives strong indications that it was never expected or intended to be enforced against French subjects[22] but was intended rather to provide them with tactical weapons and bargaining chips in foreign courts.
>
> Footnote 4:
>
> A report to the French National Assembly recommended the law's adoption on the ground that it would offer French nationals "a legal excuse for refusing to supply the information and documents demanded of them [and] a judicial weapon which will at least make it possible for them to gain time. The conflict thus created will block matters for a time and will make it possible to raise the conflict to a governmental level." With respect to the potential penalties, the report noted that 'it is necessary not to misunderstand the actual scope of these penalties … [since] … these penalties are applied only on the improbable assumption that the companies would refuse to take the protective provisions offered to them. In all other cases, these potential fines will assure foreign judges of the judicial basis for the legal excuse which companies will not fail to make use of." See Report No. 1814, Nat'l Assembly Comm. On Production and Exchanges (Deputy Mayoud), 1979-1980, 2d Sess. (June 19, 1980) at 61, 63-4, Joint Appendix of Seatrain and Navi Fonds at Exhibit 5.

21 1984 WL 423 (S.D.N.Y.), 1984 A.M.C. 2629.

22 This is an interesting use of the word "subject". A person is a subject when a monarch is head of state, but not in a republic. The French re-entered the modern age with the assumption of the Third Republic in 1870.

17 For the sake of completeness, the French law is set out in full:[23]

Loi n°68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères [on the disclosure of documents and information of an economic, commercial, industrial, financial or technical to individuals or legal entities]

Article 1

Modifié par (modified by) Loi 80-538 1980-07-16 art. 2 by JORF du 17 juillet 1980 p1799

Sous réserve des traités ou accords internationaux, il est interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin.

[Subject to international treaties or agreements, it is unlawful for any person of French nationality or habitual residence on French territory and any officer, representative, agent or employee of a corporation having its seat or establishment to communicate writing, orally or in any other form, in any place whatsoever, to provide foreign public authorities with documents or information of an economic, commercial, industrial, financial and technical communication if it is likely to affect the sovereignty, security, essential economic interests of France or of public order, as specified by the administrative authority as required.]

Article 1 bis

Créé par (created by) Loi 80-538 1980-07-16 art. 2 by JORF du 17 juillet 1980 p 1799

Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.

[Subject to any treaties or international agreements and laws and regulations, no person shall request, seek or disclose, in writing, orally or in any other

23 Unofficial translation. The law is available on the legifrance web site at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068321&dateTexte=20110716>.

form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the establishment of evidence to any foreign judicial or administrative proceedings or in connection with them.]

Article 2

Modifié par (modified by) Loi 80-538 1980-07-16 art. 2 by JORF du 17 juillet 1980 p 1799

Les personnes visées aux articles 1er et 1er bis sont tenues d'informer sans délai le ministre compétent lorsqu'elles se trouvent saisies de toute demande concernant de telles communications.

[The persons referred to in articles 1 and 1 bis are obliged to immediately inform the competent minister when they are seized of any application concerning such communications.]

Article 3

Modifié par (modified by) Ordonnance n°2000-916 du 19 septembre 2000, art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

Sans préjudice des peines plus lourdes prévues par la loi, toute infraction aux dispositions des articles 1er et 1er bis de la présente loi sera punie d'un emprisonnement de six mois et d'une amende de 18000 euros ou de l'une de ces deux peines seulement.

[Notwithstanding the greater penalties provided by law, any violation of the provisions of articles 1 and 1 bis of this law shall be punished by imprisonment of six months and a fine of 18,000 euros or by one of these two penalties.]

18 The general tenor of the decisions by judges in the United States indicate that where there is an objection to the obtaining of evidence from France, and the objection is made by one of the parties, it is more likely that disclosure will be ordered, especially when the objections tend to be argued in terms of vague principle.[24] This view was taken by Pitman, MJ in *In re Vivendi Universal S.A. Securities Litigation*,[25] in which the Lazard Group LL, who were not a party to the litigation, requested the court to issue a protective order requiring the discovery to take place under the Convention. This application was rejected, partly because there was no evidence to demonstrate that a prosecution was likely in France, and partly because Lazard was a registered corporation in Delaware with its principal executive offices in New York city.

24 See the decisions of Matsumoto, DJ in *Strauss v. Credit Lyonnais, S.A.*, 242 F.R.D. 199 (E.D.N.Y. 2007) and *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429 (E.D.N.Y. 2008).

25 2006 WL 3378115 (S.D.N.Y.).

19 A change took place in 2007, when a lawyer qualified at the French bar was prosecuted for breach of article 1 bis of Loi n°68-678 du 26 juillet 1968. This prosecution illustrated that the French authorities were prepared to take legal action against an individual. In this instance, Christopher X ignored the Convention procedures and requested the relevant information without consent. The lawyer was prosecuted, and his appeal to the *Cour de cassation, chambre criminelle* (Court of Cassation, Criminal Division)[26] was not successful. The court upheld the conviction and the fine of €10,000.[27]

20 In summary, when considering matters relating to foreign discovery, judges in the United States refer to the Restatement (Third) of Foreign Relations Law of the United States, in particular § 442(1)(c), which provides:

> In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

21 This brief foray into a complex area of law illustrates some of the problems that judges in the United States have to deal with, such as flimsy arguments to prevent a foreign party (or non-party) from delivering up evidence in proceedings. It is inevitable in the digital age that increasing amounts of evidence will have to cross borders both ways, and arguably, nation states ought to reconsider the international rules relating to the disclosure of evidence across jurisdictions.

---

26 *In re Advocate Christopher X*, Cour de cassation chambre criminelle du 12 décembre 2007 n°07-83228; a translation into English is available in the (2010) 7 Digital Evidence and Electronic Signature Law Review 130–133.

27 For a discussion of the position vis-à-vis the United States and France, together with a discussion of the case law, see Dr Pierre Grosdidier, "The French Blocking Statute, the Hague Evidence Convention, and the Case Law: Lessons for French Parties Responding to American Discovery", at <http://www.haynesboone.com/french_blocking_statute/>.

III. ENCRYPTED DATA

1. United States of America

22 It was only a matter of time before the courts had to deal with encrypted data and the failure to obtain the password to decrypt the data. One of the first cases in which this problem was raised was the case of *In re Grand Jury Subpoena to Sebastien Boucher*.[28] The facts were that on 17 December 2006, Boucher and his father entered the United States from Canada at Derby Line, Vermont. Customs and Border Protection Officer Chris Pike found a laptop computer in the vehicle they were travelling in. He opened the computer and switched it on without entering a password. He searched the various files in the computer, and discovered approximately 40,000 images, some of which appeared to be pornographic, based on the names of the files. Boucher was asked if any of the files contained abusive images of children, to which he responded that he was not certain. Officer Pike continued to search the files, and noticed some files with names that suggested child pornography. He then requested the help of Special Agent Mark Curtis, who determined that a number of files contained abusive images of children. Boucher was then given rights under *Miranda*, and told the Special Agent that he downloaded pornographic files, and indicated that he did not intentionally download child pornography and deleted any such images when he came across them. Boucher was given access to the laptop and navigated to Z drive, obtaining access by inserting a password. The Special Agent did not see Boucher do this. Boucher was subsequently arrested and his laptop was seized. After obtaining a search warrant, the government discovered that the Z drive was encrypted. The investigating authorities could not open the Z drive. A grand jury subpoena was issued for Boucher, directing him (at 2) to:

> … provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

23 Boucher moved to quash the subpoena because, he alleged, that it violated his right not to incriminate himself under the provisions of the Fifth Amendment. Whether the privilege against self incrimination applied

28 2007 WL 4246473 (D.Vt.).

in this instance depended on whether the subpoena sought testimonial communication. Both parties agreed that the contents of the laptop computer were not covered by the Fifth Amendment, because they were voluntarily prepared and not testimonial in nature. Niedermeier, MJ, commented, at 3, that:

> Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, 'Do you know the password to the laptop?' If Boucher does know the password, he would be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court.

24 The learned judge concluded that the provisions of the Fifth Amendment prevented the government from compelling Boucher from providing the password on the basis that it would compel him to display the contents of his mind to incriminate himself.

25 The government appealed this decision.[29] Chief District Court Judge William K. Sessions, III, of the District of Vermont, overruled the initial ruling and sustained the government's appeal. The government argued on appeal that it did not seek the password for the encrypted hard drive, but required Boucher to produce the contents of the encrypted hard drive in a format they could be viewed by the grand jury. The government was aware of the existence and location of the information during the border examination, which meant the information was not testimonial, as noted by the learned judge at 3:

> Boucher accessed the Z drive of his laptop at the ICE agent's request. The ICE agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography. The Government thus knows of the existence and location of the Z drive and its files. Again providing access to the unencrypted Z drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information.

26 In this instance, Boucher had already cooperated and potentially incriminated himself by admitting ownership of the laptop, and provided law enforcement officers with partial access to it prior to his arrest.[30]

---

29 *In re Grand Jury Subpoena to Sebastien Boucher*, 2009 WL 424718 (D.Vt.).

30 The Boucher case was not cited in an identical argument before Borman, DJ in *United States of America v. Kirschner*, 2010 WL 1257355 (E.D.Mich.), who decided that the

2. Canada

27 In Canada, the reverse occurred in the case of *R v. Beauchamp*,[31] in which the defence sought an order to require the Crown to disclose a copy of encrypted files, located on a hard drive, that had been seized by the police. The Crown has not been able to de-encrypt the files, and as a result had no knowledge of the data that was encrypted. It was agreed that the encrypted information was both potentially inculpatory and potentially exculpatory for the accused parties. The Crown submitted that the encrypted information was beyond its control, although it was, arguably in its possession, but not in a format that it was able to view. The learned judge concluded that the Crown was in partial possession and control of the hard drives, but it had no knowledge of the information in the encrypted files. R Smith J analysed the position thus, at 40:

> The seizure by the police of the hard drives containing encrypted information is similar to the seizure of a locked safe which the police cannot open, containing documents which include both inculpatory and exculpatory evidence. The police or Crown would clearly be in possession or control of the safe, but if they did not have the key or combination and were unable to break the safe open, then they would not have knowledge of the contents of the safe. In this case, the Crown's control of the contents of the safe, which are known to one accused but not to the Crown, is not complete, as the Crown needs the key or combination, or in this case the password, in order to access the documents in the safe. The unique feature of this case is that the accused Cattral has the key or password, which is necessary to complete the possession or control of the information in the safe.

28 The application for disclosure of a copy of the encrypted files in the hard drives was refused, although the learned judge indicated that the applicants may, at their option, obtain disclosure of the contents if they provide the password or key to the Crown and the Crown would then review the material.

---

subpoena requiring the defendant to give up the password must be quashed, on the basis that the request would incriminate him. For more discussion and reference to other article, see David Colarusso, "Heads in the Clouds, A Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-incrimination" (2011) 17 Boston University School of Law Journal of Science and Technology Law 69.

31 2008 CANLII 27481 (ON SC).

3. England & Wales

29 A similar problem had occurred in England & Wales in the case of *R v S (F) and A (S)*,[32] where the police issued a section 49 notice under the Regulation of Investigatory Powers Act 2000 (it is a criminal offence to knowingly refuse or fail to make the disclosure required by a notice issued under s 49), requiring the defendant to provide the password to encrypted data. The relevant issue is that data that is encrypted might contain incriminating information, but it is not certain that it will contain incriminating information. Sir Anthony May said, at 20:

> …the key to the computer equipment is no different to the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral. In the present cases the prosecution is in possession of the drawer: it cannot however gain access to the contents. The lock cannot be broken or picked, and the drawer itself cannot be damaged without destroying the contents.

30 The Court of Appeal determined that the purpose of the statute is to regulate the use of encrypted material, and to impose limitations on the circumstances in which it may be used, subject to a proportionality test and judicial oversight, and that neither the process, nor any subsequent trial could be considered to be unfair.[33]

4. Obtaining the password

31 One way of understanding what might be included in encrypted files is to interpret information against known data, as in the United States case of *United States of America v. Hersh a.k.a. Mario*.[34] In his summary of the facts, Circuit Judge Marcus pointed out that a search of Hersh's residence uncovered evidence of computer images of juvenile males engaged in sexual activities. A number of files were encrypted, and the judge described, in footnote 4, how these were handled by the investigators:

---

32 [2008] WLR (D) 313, [2008] EWCA Crim 2177.

33 This case is discussed in more detail in Stephen Mason, *Electronic Evidence* (LexisNexis Butterworths, 2nd Ed, 2010) 10.228–10.250.

34 United States Court of Appeals for the Eleventh Circuit No 00-14592 July 17, 2002 before Anderson and Marcus, Circuit Judges, and Middlebrooks, District Judge available in electronic format at <http://laws.lp.findlaw.com/11th/0014592opn.html>.

> Several computer files containing child pornography were found in Hersh's residence: (1) three recovered computer files with viewable images found on the C-drive of Hersh's computer, and (2) encrypted files found on a high-capacity Zip disk. The images on the Zip disk had been encrypted by software known as F-Secure, which was found on Hersh's computer. When agents could not break the encryption code, they obtained a partial source code from the manufacturer that allowed them to interpret information on the file print outs. The Zip disk contained 1,090 computer files, each identified in the directory by a unique file name, such as "sfuckmo2," "naked31," "boydoggy," "dvsex01, dvsex02, dvsex03," etc., that was consistent with names of child pornography files. The list of encrypted files was compared with a government database of child pornography. Agents compared the 1,090 files on Hersh's Zip disk with the database and matched 120 file names. Twenty- two of those had the same number of pre-encryption computer bytes as the pre-encrypted version of the files on Hersh's Zip disk.

32 In this instance, although the files could not be decrypted, nevertheless there was a sufficient link between the names of the files and evidence of child pornography known to the police.

33 One other mechanism could be used: to apply for a search warrant and install key logging software on the computer, so as to obtain the password when the computer was used, as in the case of *United States v. Scarfo*.[35]

IV. CLOUD COMPUTING

34 The word 'cloud', in cloud computing, is a fairly accurate description of the ephemeral nature of the structure by which the services are offered.[36] Just as a cloud might appear and disappear rapidly, and the forces of air, heat and water vapour will change the internal dynamic of the cloud, so too the services offered over the internet by providers of software can be equally transitory. Cloud computing is best described by reference to a set of

35 180 F.Supp.2d 572 (D.N.J. 2001).

36 A paper entitled "Introduction to cloud computing architecture" (June 2009) by Sun Microsystems provides a useful technical introduction, available at <http://www.sun.com/featured-articles/CloudComputing.pdf>; also useful is Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (December 2009), available at <https://cloudsecurityalliance.org/guidance/>.

characteristics, rather than by offering a definition.[37] In any event, cloud computing affects lawyers and how they deal with the obtaining of evidence in both civil and criminal proceedings, especially in relation to e-mail.

35 For instance, in civil proceedings in the United States of America where data is stored in a cloud computing service, courts have ordered that such data be disclosed if it is relevant to the proceedings, for which see *National Economic Research Associates, Inc., v Evans*,[38] where e-mail communications exchanged between an employee and his lawyer sent over a laptop computer owned by the business via the employee's personal web based e-mail account and protected by a password were the subject of privilege, and *Romano v Steelcase, Inc.*,[39] where, in an action for injuries sustained as a result of a motoring accident, the defendant obtained an order to obtain relevant personal information uploaded by the claimant on the social networking web sites Facebook and MySpace to counter the claim by the claimant that she had had suffered permanent injuries.

36 Whilst evidence from the cloud can be obtained, nevertheless a significant problem can occur in respect of attorney-client privilege. For instance, the lawyer representing the employer in employee litigation must take great care not to handle e-mail correspondence that attracts privilege between the employee and their lawyer, as in *Stengart v. Loving Care Agency, Inc.*,[40] where Marina Stengart communicated with her lawyer by way of a web based e-mail account by means of a computer owned by her employer. Her employer requested a forensic expert to recover all the files stored on the laptop computer, including e-mails, which had been saved on the hard drive. The lawyer for Loving Care reviewed all the data on the computer, including the e-mails between Ms Stengart and her lawyer. The lawyer for Loving Care maintained that the company had the right to review the

37 One technical definition of cloud computing has been offered by Peter Mell and Tim Grance of the National Institute of Standards and Technology, Information Technology Laboratory: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." Version 15 (10-7-09), available at <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>.

38 2006 WL 2440008.

39 907 N.Y.S.2d 650 (N.Y Sup. Ct. 2010).

40 201 N.J. 300 (2010), 990 A.2d 650.

e-mails in the light of the use of electronic communications policy, which read, in the relevant part:

> The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.
>
> …
>
> E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.
>
> The principal purpose of electronic mail (*e-mail*) is for company business communications. Occasional personal use is permitted …'

37 The trial court ruled that, in the light of the employer's policy, the employee had waived the attorney-client privilege by sending the e-mails on the company computer. The Appellate Division reversed this and found that the employer's counsel had violated the provisions of Rule of Professional Conduct 4.4(b), which requires that a lawyer who has "reasonable cause to believe that [a] document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender." The Supreme Court of New Jersey concurred with the Appellate Division.

38 The Supreme Court considered the central issue was whether Stengart had a reasonable expectation of privacy in her e-mails with her attorney sent and received by way of her company laptop computer. The court identified two factors bearing upon this issue: the scope of the policy and the importance of attorney-client privilege. Rabner CJ, who delivered the opinion of the court, concluded that the policy was ambiguous because it did not address personal accounts; failed to warn employees that the contents of such e-mails were stored on a hard drive and could be forensically retrieved and read by Loving Care, and acknowledged that personal use of e-mail was permitted. Regarding the attorney-client privilege, it was clear that e-mail messages are covered by the privilege, in the same way as any other form of communication.[41]

41 The case of *Lenz v. Universal Music Corp.*, 2010 WL 4789099 (N.D. Cal.) illustrates the importance of instructing clients not to discuss their legal matters on Facebook, blogs, or other social media. In this case Fogel DC upheld a decision to compel

39 It is important to be aware of the terms and conditions of each e-mail provider used by clients and lawyers. Some lawyers across the world use free e-mail serves such as Gmail and Yahoo!, yet are not necessarily aware of the terms of use of such services. For instance, Yahoo! has recently altered its terms of use in the UK, although the change is not easy to notice. The change of use is reflected in the frequently asked questions, the first question which reads as follows:[42]

> 1. What are "relevant ads" as they relate to Yahoo! Mail?
>
> To make our ads more relevant and useful for you, we make educated guesses about your interests based on your activity on Yahoo!'s sites and services, as well as provide ads that are contextually relevant to the page they are being served with. When you use the new Yahoo! Mail our automated systems *scan and analyse all incoming and outgoing communications content sent and received from your account (such as Mail and Messenger content including instant messages and SMS messages) to detect, among other things, certain words and phrases (we call them "keywords") within these communications*. This might result in ads being shown to you in Mail for products and services that are related to those keywords. In addition, these keywords may contribute to the interest categories we assign to your browser for interest-based ads that we show throughout the Yahoo! Ad Network. No additional ads are shown to you, just more relevant ads.
>
> [emphasis added]

40 Also of relevance is the answer to question 2:

> 2. How does Yahoo! Mail message analysis work?
>
> While many features in the Yahoo! Mail are new, the underlying technology that supports them is the same as the automated systems that already scan and analyse your inbox for spam, viruses, malware, and phishing scams. This technology looks for patterns, keywords, and files in Mail, Messenger, and other communications content. In order to bring you the newest Yahoo! Mail, Yahoo!'s automated systems will *scan and analyze all incoming and outgoing email, IM, and other communications content sent and received from your account* in order to personalize your experience. This will result in both product enhancements as well as more relevant advertising in addition to a safer, less cluttered Mail experience.
>
> [emphasis added]

---

production of attorney-client communications because Stephanie Lenz had discussed the communications in e-mails, in instant chats with family and friends, in blog postings and with the media.

42 See <http://info.yahoo.com/privacy/uk/yahoo/mail/ymailfaq/details.html>.

41 Although the system indicates that such scanning of content will only involve automated systems, nevertheless it is not clear whether communications between client and lawyer can be considered to be privileged if the content is being screened in this way. This issue is raised as a preliminary point that will probably need further consideration, but lawyers and judges can expect to have to deal with such issues in the near future.

V. CONCLUDING REMARKS

42 There is no doubt that there has been an increase in the volume of journals, books and other materials for lawyers in the digital age. Generally, lawyers and judges are aware that much of what can be found for free on the internet, for instance, cannot be taken at face value, even when it is written by lawyers. At issue for the legal profession are a series of interrelated areas of interest that should concern all lawyers and judicial training establishments, covering education; knowledge; experience of other jurisdictions; access to information; legal textbooks and journals. To put electronic evidence (and electronic signatures) into context, it is one subject that is considered 'niche' by the vast majority of lawyers and judges, yet affects every aspect of law – every area of law. Lawyers and judges now correspond daily (if not minute by minute) by e-mail and SMS: each time they use digital technology they use their electronic signature and create digital evidence. It is identical for their clients: people in businesses, governments and individuals use computers, PDAs, smart telephones and a range of other devices, all of which create and store digital data. To suggest that either topic (electronic evidence and electronic signatures) are 'niche' areas for the specialist, illustrates the ignorance of the judge or lawyer that responds in such a way.

43 Unfortunately, neither electronic evidence nor electronic signatures are part of the professional curriculum of any course that leads to the qualification of being a lawyer. It cannot be right that lawyers qualifying in 2011 know nothing about electronic evidence and electronic signatures, yet are expected to advise and represent clients – the vast majority of which will have a problem that includes either one or both of these areas of law. It is negligent to fail to ensure would-be lawyers are properly qualified for the work they will be required to do once they are qualified.

44 Digital evidence and electronic signatures are with us, but pitifully few lawyers are prepared.

ELECTRONIC EVIDENCE IN SINGAPORE: OUT WITH THE OLD, IN WITH THE NEW

> The use of personal computers at home and in the office is now common place, as is the linking of such computers to form vast networks that allow information to be entered, stored, altered and retrieved by a host of users in a global environment. Developments in document imaging technologies have also enabled users to keep images of their paper documents in electronic media, thereby allowing them to save storage costs as the paper originals could then be destroyed. The law has therefore to be updated to facilitate the wider use of these new technologies. Such a law, of course, has to strike a balance between guaranteeing the reliability of evidence produced by such technologies and ensuring that the admissibility of such evidence is not hampered by complicated conditions and procedures.
>
> *Singapore Parliamentary Debates, Official Report* (18 January 1996) vol 65 at col 450–451 (Prof S. Jayakumar, Minister for Law).

YEONG Zee Kin
LLB (National University of Singapore),
LLM (Computer & Communications Law) (Lond)

Paul **CHAN**[*]
LLB (National University of Singapore)

I. INTRODUCTION

1 Such was the justification provided in Parliament by the then Singapore Minister for Law, Prof S. Jayakumar, for the introduction of the recently repealed Section 35 of the Evidence Act (Cap 97, 1997 Rev Ed) ("Section 35" and "Evidence Act", respectively) in 1996. Unfortunately, not unlike the fate of some of the technology it was meant to facilitate, Section 35 was soon felt to be wanting, inadequate and out of date with

* The authors express their deepest appreciation to Stephen Mason for his comments to an earlier draft of this article. Some of the ideas in this article springboard from discussions of the panel on "Electronic Evidence in Singapore – Law and Practice" chaired by Lok Vi Ming, SC with members: Stephen Mason, Yeong Zee Kin, Christopher Ong and Bryan Tan.

modern requirements and realities. That Section 35 did not strike the appropriate balance between reliability and ease of admissibility that the Minister spoke of was a common sentiment. Indeed, dissatisfaction with Section 35 grew so strong that barely seven years after its enactment, the Attorney-General's Chambers ("AGC") commissioned the Singapore Academy of Law ("SAL") to undertake a thorough review of the provision. Despite this, Section 35 confounded its critics, retaining its role in our statute books as the gateway by which electronic evidence is admitted in court for a further 8 years. It is only recently that Section 35 was repealed by the Evidence (Amendment) Act 2012.[1]

2 This paper reviews two related perennial issues: first, what is the appropriate balance to be struck between reliability of electronic evidence and ease of admission; and second, how, legislatively, this balance is best achieved. It will be suggested that the resilience of Section 35 may be partially explained by the fact that it does indeed strike the correct balance for certain types of electronic evidence. However, it will also be propounded that the effect of Section 35 was far too wide.

3 To these ends, this paper will begin with a brief overview of the import of Section 35 in light of the case law that has developed. Section III will then examine the possible objections to Section 35. This may usefully be done by discussing the review undertaken by SAL as well as the motivations underlying the reforms actually undertaken in the UK. This paper concludes with a look at the new presumptions that were introduced with the repeal of Section 35.

II. SECTION 35 OF THE EVIDENCE ACT: IN RETROSPECT

4 The proliferation of electronic communication, documentation and storage has proven to be mostly a boon to commerce. However, where the law of evidence is concerned, electronic data is met with suspicion. This may be partly due to the inability of most people, including legislators and judges, to completely comprehend the inner workings of a computer and partly due to the perceived unreliability and transient nature of technology. As a result, the law in many jurisdictions singles out electronic evidence and

1 Act No 4 of 2012; passed on 14 February 2012 and received Presidential assent on 20 March 2012, it is currently awaiting commencement notification.

subjects it to a regime not applicable to conventional forms of evidence. So it is in Singapore.

5 The admissibility of evidence in Singapore is governed by the Evidence Act. This includes electronic evidence which, until the recent amendments,[2] was termed "computer output" in the Evidence Act.[3] Under s 3(1) of the Evidence Act, the phrase "computer output" enjoyed the following definition:

> "computer output" or "output" means a statement or representation (whether in audio, visual, graphical, multi-media, printed, pictorial, written or any other form) –
>
> (a) produced by a computer; or
>
> (b) accurately translated from a statement or representation so produced;

6 As one may immediately appreciate, this is a fairly expansive definition that would include almost any kind of end product emanating from a computer. This broad understanding of electronic evidence is accentuated by the definition accorded to the term "computer" in the same section:

> "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —
>
> (a) an automated typewriter or typesetter;
>
> (b) a portable hand held calculator;
>
> (c) a device similar to those referred to in paragraphs (a) and (b) which is non-programmable or which does not contain any data storage facility;
>
> (d) such other device as the Minister may by notification prescribe;

7 That "computer output" may take many difference forms – audio, visual, graphical, multimedia, printed, pictorial or written – is confirmed by case law. The courts have understood the phrase to include records of text

2 The definitions of "computer" and "computer output" or "output" have been deleted by the Evidence (Amendment) Act 2012.

3 In this paper, the terms "electronic evidence" and "computer output" are used interchangeably.

messages exchanged through a short messaging service,[4] emails,[5] business registration records,[6] printouts from the customs authorities' immigration status database,[7] banking records,[8] business accounts,[9] video recordings,[10] drug analysis reports produced by mass spectrometers and gas chromatographs,[11] medical scans,[12] electronic signatures,[13] information on a hard disk,[14] server logs,[15] spreadsheets, call tracing records[16] and reports/logs from rig computers.[17] These decisions demonstrate that "computer output" is not limited to documents produced by a computer as would be understood by a layperson. Rather, any device that contains a processing unit, regardless of its level of sophistication, will be considered to be a "computer" (save for the exceptions specific in the definition) and any product emanating therefrom will be considered "computer output".

8 A special regime was established under Section 35 for the admission of computer output as evidence:

> 35.—(1) Unless otherwise provided in any other written law, where computer output is tendered in evidence for any purpose whatsoever, such output shall be admissible if it is relevant or otherwise admissible according to the other provisions of this Act, and it is –

4 *Ler Wee Teang Anthony v Public Prosecutor* [2002] 1 SLR(R) 770; *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2005] 1 SLR (R) 502.

5 *Malcomson Nicholas Hugh Bertram & Anor v Naresh Kumar Mehta* [2001] 3 SLR(R) 379; *Lim Seong Khee v Public Prosecutor* [2001] 1 SLR(R) 631.

6 *Aw Kew Lim & Ors v Public Prosecutor* [1987] 2 MLJ 601.

7 *Roy S Selvarajah v Public Prosecutor* [1998] 3 SLR(R) 119.

8 *Industrial & Commercial Bank Ltd v Banco Ambrosiano Veneto Spa* [2003] 1 SLR(R) 221.

9 *Lim Mong Hong v Public Prosecutor* [2003] 3 SLR(R) 88.

10 *Heng Aik Ren Thomas v Public Prosecutor* [1998] 3 SLR(R) 142; *Public Prosecutor v Chee Soon Juan* [2008] SGDC 131.

11 *Public Prosecutor v Ang Soon Huat* [1991] 1 MLJ 1.

12 *Dr Khoo James & Anor v Gunapathy D/O Muniandy* [2002] 1 SLR(R) 1024.

13 *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] 2 SLR(R) 651.

14 *Megastar Entertainment Pte Ltd v Odex Pte Ltd* [2005] 3 SLR(R) 91.

15 *Odex Pte Ltd v Pacific Internet Ltd* [2008] 3 SLR(R) 18.

16 *Annis bin Abdullah v Public Prosecutor* [2004] 2 SLR(R) 93; *Kamrul Hasan Abdul Quddus v Public Prosecutor* [2011] SGCA 52.

17 *Jet Holding Ltd and others v Cooper Cameron (Singapore) Pte Ltd and another* [2005] 4 SLR(R) 417; *Jet Holding Ltd and others v Cooper Cameron (Singapore) Pte Ltd and another and other appeals* [2006] 3 SLR(R) 769.

> (a) expressly agreed between the parties to the proceedings at any time that neither its authenticity nor the accuracy of its contents are disputed;
>
> (b) produced in an approved process; or
>
> (c) shown by the party tendering such output that –
>
> (i) there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt or suspect the truth or reliability of the output; and
>
> (ii) there is reasonable ground to believe that at all material times the computer was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the accuracy of the output was not affected by such circumstances.

9 In order to foreshadow arguments to be made later, two preliminary points must immediately be highlighted. First, the Section 35 regime was applicable "where computer output is tendered in evidence for any purpose whatsoever".[18] This phrase was intended to obliterate the distinction made by pre-1996 jurisprudence between admitting computer output as real evidence and a document containing hearsay. Under that distinction, developed at common law and applied in Singapore under the pre-1996 version of Section 35, computer output admitted as real evidence need not satisfy the requirements of the pre-1996 wording of Section 35.[19] On the other hand, computer output admitted as a document containing hearsay would be subjected to the requirements of the pre-1996 wording of Section 35.[20] However, the post-1996 wording of Section 35 enlarged the scope of the electronic evidence regime by making it applicable to all computer output tendered in evidence, regardless of the purpose for which it was tendered.[21]

10 Secondly, it is clear from the wording of Section 35 – "if it is relevant or otherwise permissible according to the other provisions of this Act" – that the special regime was intended to be an additional evidential hurdle on top of the other requirements of the Evidence Act imposed on other kinds of evidence. The law of evidence generally admits all evidence that is

18 Section 35, Evidence Act.

19 *Public Prosecutor v Ang Soon Huat* [1991] 1 MLJ 1.

20 *Aw Kew Lim & Ors v Public Prosecutor* [1987] 2 MLJ 601.

21 *Lim Mong Hong v Public Prosecutor, supra* note 9, at [38].

deemed relevant.[22] That is the first criterion of admissibility. However, relevance is a necessary but insufficient criterion. Evidence tendered must also not infringe any of the rules that may exclude a piece of evidence from admission. Such exclusionary rules are many but may typically be classified into the following four categories: hearsay, opinion, character of the witness and conduct of the witness on other occasions. To these exclusionary rules there exist limited exceptions. Insofar as electronic evidence is concerned, Section 35 added an additional requirement for admissibility on top of all the other generally applicable requirements. Put plainly, before computer output may be admitted as evidence, it must:

(a) be relevant;

(b) not infringe any of the exclusionary rules of evidence or, if it does so infringe, must fall within one of the exceptions to the exclusionary rules; and

(c) satisfy the requirements of Section 35.

11 What then was this additional requirement imposed upon all electronic evidence? It was that electronic evidence must be received in evidence under one of three alternative modes of admissibility: by way of an express agreement between the parties to the proceedings, by way of computer output produced via an approved process and by proof of the proper accuracy of the computer printout. If the party wishing to adduce computer output as evidence failed to satisfy any of these three modes of admissibility, the computer output would be ruled inadmissible even though it was otherwise admissible by some other rule of evidence.[23]

1. Admission by agreement

12 Under the express agreement mode, computer output was admissible if the parties to the proceedings agree, at any time, not to dispute both the authenticity and accuracy of the contents of the computer output. Section 35 did not stipulate the form in which this agreement is to be made. In practice, it was tacitly accepted that an oral agreement would suffice. One may go so far as to say that acquiescence – or the failure to raise any form of objections – would be sufficient as *implied* oral agreement. This

22 For a definition of the term "relevance", see s 3(2), Evidence Act.

23 *Lim Mong Hong v Public Prosecutor*, *supra* note 9, at [35].

was the practice in the vast majority of cases where electronic evidence was adduced, admitted and relied upon at trial without the spectre of Section 35 dimming the doorway to the courtroom. How such an agreement would qualify as an express agreement – as required under Section 35 – is unclear but this issue has never been litigated.

13 The provision also did not mention if the agreement must be specific to the computer output in question or whether a blanket agreement would be sufficient.[24] Similarly, it was not clear whether the agreement had to be for identified computer output to be adduced for a specific trial or whether a broad agreement made prior to any contemplated legal proceedings would also suffice.

14 Hence, there arose another practice where – typically in standard form agreements – an express agreement to admit electronic evidence was included. The standard form agreement between parties would contain provisions that had the effect of expressing an agreement between parties that any electronic evidence that was produced within the contractual relationship would be admissible in the event of any legal proceedings arising out of that contractual relationship. Sometimes, such contractual provisions were drafted in the negative: that parties to the agreement would not raise any objections to admissibility of the electronic evidence solely on the basis that the evidence sought to be adduced in the legal proceedings were electronic in nature.

15 In order to protect accused persons in criminal proceedings, Section 35 also provided that the agreement is only effective if the accused is legally represented. In addition, an agreement that is obtained "by means of fraud, duress, mistake or misrepresentation" is vitiated and ineffective to admit the computer output.

2. Admission of computer output from an approved process

16 The "approved process" mode of admissibility was intended to facilitate the admissibility of electronic images of physical documents and records. An approved process was a process which has been approved by a

24 Section 35 is also silent as to whether in multi-party proceedings, an agreement is required to be obtained between every party to the proceedings or only as between the parties whose interests would be affected by the computer output. On this issue, see Seng D, "Computer Output as Evidence", [1997] SJLS 130 at p 147.

certifying authority pursuant to the Evidence (Computer Output) Regulations 1996.[25] Pursuant to this Regulation, an approved process may only be sought with respect to an "image system", being a computer system that is capable of capturing, storing and retrieving images or generating image system output. To tender the computer output of an imaged document, this output must be supported by proof that the output is obtained from an approved process and that it accurately reproduces the contents of the original document. In this regard, two certificates must be produced. One is to be signed by a person holding a responsible position in relation to the operation and management of the certifying authority to certify that the imaging system has been approved.[26] The other is to be signed by a person holding a responsible position in relation to the operation or management of the approved process to certify that the computer output is obtained from the approved process.[27]

17 There was doubt as to whether this scheme gained traction. There were anecdotal accounts that this scheme was adopted by banks for the imaging of cheques put through the clearing system. Further doubt as to the acceptance of this scheme is cast when one considers that the Evidence (Computer Output) Regulations for the appointment of certifying authorities that are necessary to approve the process was last notified in 2001. Three organisations were appointed as certifying authorities and the last of their appointments had expired by 2004.[28] The fact that none of the previously appointed certifying authorities were able or willing to renew their appointments suggests that the approved process was a scheme that eventually fell into disuse.

3. Admission by certification

18 Finally, the last mode of admissibility for electronic evidence is the admissibility by proof of proper operation and accuracy. Two conditions must be satisfied. First, it must be shown that there is no reasonable ground for believing that the output is inaccurate because of the improper use of

25 Evidence (Computer Output) Regulations 1996 (1997 Rev Ed).

26 Section 35(3), Evidence Act.

27 Section 35(4), Evidence Act.

28 The appointments of M/s KPMG Consulting Pte Ltd expired on 16th May 2002; M/s Ernst & Young expired on 24th September 2003; and M/s PricewaterhouseCoopers expired on 20th March 2004.

the computer and that no reason exists to doubt or suspect the truth or reliability of the output. Secondly, it must be demonstrated that there is reasonable ground to believe that at all material times, the computer was operating properly. Compliance with both conditions may be shown by way of a certificate or certificates (as may be necessary). Such a certificate must be signed by a person holding a responsible position in relation to the operation and management of the relevant computer system. It is not necessary to call an expert or even the "systems operator" or the "information systems manager"; rather, someone who is familiar enough with the computer to attest to its working condition will suffice.[29] In *R v Shephard*,[30] which was a decision on the UK provision on which Section 35 was modelled, the witness who gave evidence was the store detective. As the computer involved was of the simplest kind printing limited basic information, she had the requisite familiarity.[31]

19 For practical purposes, so long as the person is familiar with how the computer is typically used and how it is supposed to operate under normal circumstances, such person would be sufficient in most cases. On the occasions where the technical workings of the computer system becomes relevant, then a technical manager – usually the manager of the IT department or, if the computer system is more complex, a representative of the company that provided the software and/or computing equipment – may be called.

20 It is this mode of proving computer output that was the most frequent overt use of Section 35; but even so, these were rare instances. As a matter of observation, it cannot be gainsaid that the issue of admissibility of computer output is usually only considered at the threshold of the courtroom.[32] By this time, the prospect of an express oral agreement on admissibility would be dim and the only other practical mode of admission would be by written certification.

21 The case of *Ng Koo Kay Benedict and another v Zim Integrated Shipping Services Ltd*[33] must be recognised for its interpretation of

29 *Lim Mong Hong v Public Prosecutor*, *supra* note 9.

30 [1993] 1 All ER 225.

31 Yeong Zee Kin, "Computer Misuse, Forensics and Evidence on the Internet" (2000) 5(5) Communications Law 153, at p 163.

32 Formal notice of objections may be given either after the exchange of lists of documents or after the exchange of affidavits of evidence-in-chief.

33 [2010] 2 SLR 860.

s 35(1)(c) to allow admission of computer output by oral certification. Before this case was decided, practitioners had always read the requirement for a written certificate under s 35(6) to be the only mode of certification recognised by the Evidence Act. Lai Siu Chiu J took an interpretation of s 35(1)(c) that permitted certification by oral evidence led from a witness who was familiar with the operations of the computer that produced the output sought to be admitted into evidence. In hindsight, this was probably a natural extension of how certification under Section 35 had been handled prior to the decision. No form was ever prescribed for the certification under s 35(6), and the form of such certification had always followed either the format of a conditioned statement (for criminal cases) or an affidavit (for civil cases). With this in mind, it is only natural that the matters that the deponent can aver to in an affidavit must be equally admissible if he were to give oral testimony in the witness stand.

22 Be that as it may, this case continued the slow erosion of the necessity for Section 35. It may be posited that the case set the tone that admissibility of computer output no longer required the formality of a written certificate. So long as an appropriate witness is called to provide some positive evidence of the operations of the computer that generated the output sought to be admitted into evidence, that it was working properly and properly used on the occasion in question, and that there was no reason to doubt the truth or reliability of the output, this would be sufficient to admit the computer output under s 35(1)(c). With this decision, the manner of adducing electronic evidence was beginning to look at lot more similar to the manner of adducing other forms of business records.

III. OBJECTIONS AND SUGGESTIONS FOR REFORM

23 Since the passage of the 1996 amendments to the Evidence Act, rapid advancements in information technology have been made. Accessibility to the internet became ubiquitous. Palmtops and personal digital assistants became affordable and, therefore, widely popularly after 1999. Thereafter, personal cell phones came along with internet accessibility allowing people to surf the internet almost anywhere, anytime. The commercialisation of the internet has also led to an exponential increase in electronic trading and retailing. Similarly, social media platforms are now enjoying immense popularity. Such epochal changes have posed challenges to the legal landscape as a whole. More than most, the law of evidence has felt the

pressure resulting from the changes. To examine if the Evidence Act post-1996 amendments could adequately deal with the technological advances that have been made, the Law Reform & Revision Division of the AGC requested the Technology Law Development Group ("TLDG") of the Singapore Academy of Law to review Section 35 (and its accompanying provision, s 36 of the Evidence Act) and to recommend possible changes. To this end, two documents were eventually published: a consultation paper and a final report.

24 In the consultation paper, a number of objections against Section 35 were raised. First, it was suggested that Section 35 did not comply with the principle of non-discrimination against electronic evidence, or the equivalence principle. By requiring electronic evidence to be subjected to a regime to which non-electronic evidence was not, adducing electronic evidence in court was made more difficult.

25 Secondly, the view that Section 35 was overly onerous was also put forward. Admission by express agreement is, it was contended, rarely used for the simple reason that parties who have seen fit to settle their disagreements by way of litigation are unlikely to consent to the admission of electronic evidence which may be detrimental to their case. This problem is particularly acute for criminal matters. The second method of admission – via an approved process – is feasible only for large organisations, usually governmental ones, and does not apply to run of the mill cases. This leaves only the third method which is, in the TLDG's view, not easy to apply as it is often difficult to identify and find the right persons to make the prescribed legal declarations.

26 Finally, it was propounded that in an age of improved reproduction techniques and technology, coupled with avenues of discovery and pre-trial assessments of documents, the "best evidence" rule appears increasingly anachronistic in relation to electronic evidence. The force of that rule has severely diminished because of the ability of electronic evidence to make perfect duplicates of original documents. As a result, there should be no objections to a court relying upon electronic documents without stringent requirements of authentication.

27 Consequently, four options to reform Section 35 were proposed by the TLDG and were, thereafter, put forward for public consultation. The first option, drawing on the principle that electronic evidence should be treated no differently from other types of evidence, was to adopt a non

computer-specific approach. Under this approach, the conventional rules of evidence will apply to determine if a piece of electronic evidence should be admitted. The rules on hearsay, best evidence and authentication will determine the admissibility of a document, if contested. However, the common law distinction between real evidence and documentary evidence will apply (see [10] above). The TLDG opined that no legal difficulties exist in the application of the rules of hearsay and of real evidence to electronic evidence. Such an approach best preserves the discretion of the court to deal with electronic evidence as the justice of the case demands. In situations where the source of the electronic evidence is reliable or trustworthy, the court may be receptive to admitting electronic evidence with little need for supplementary evidence. However, if an electronic document was only produced for the purposes of legal proceedings or is otherwise questionable, the court may require clear and strict proof evidencing authentication.

28 The next option suggested was also a non computer-specific one but which also contemplated the inclusion of presumptions to facilitate the admissibility of electronic evidence. The force for the inclusion of the presumptions is the recognition that some types of electronic evidence are inherently more reliable than others. Accordingly, rules should be enacted to facilitate their admission. Such a presumption already exists at common law in relation to mechanical instruments where, under the maxim *praesemuntur omnia rite esse acta*, the law presumes that mechanical instruments were in order when they were used. It was suggested that such an approach will combine the advantage of having a technology neutral approach while facilitating easy admission of electronic evidence in most cases. This will engender the certainty and predictability necessary to conduct business activities.

29 The penultimate approach, described as option three, is one that provides a mechanism for the easy admissibility of business records in general. Such business records will, of course, include electronic business records. Business records are already admissible pursuant to s 32(b) of the Evidence Act as an exception to the hearsay rule, *ie*, business records are admissible even if they contain hearsay information. What the approach propounds is an admissibility provision that will collapse the hearsay rule, the authentication rule and the best evidence rule into one general provision that provides for the admissibility of business records. The *raison d'être* for this approach is, of course, a nod to the business community. It is already an acknowledged presumption in the Evidence Act that records kept in the

ordinary course of business are inherently reliable. The proposed provision merely takes this presumption to its logical conclusion and, in so doing, allows for an admission mechanism that will facilitate the inclusion of electronic business records which is becoming more prevalent and unavoidable.

30 The last method considered was a tweaking of the current approach of admissibility for electronic evidence. The changes that may be taken on board includes making Section 35 inclusive and descriptive and not exclusive and prescriptive in nature. Pursuant to this suggestion, while parties may continue to use any of the three modes of admissibility, they are free to utilise the inherently flexible common law approach to authentication. Other more specific, and less drastic, changes include amending s 35(1) of the Evidence Act to only require proof that (i) the output is accurate and reliable; and that (ii) at all material times the computer that produced the output was operating properly or, if not, the accuracy and reliability of the output was not compromised, and allowing such proof to be furnished by way of an affidavit by any qualified person in relation to the computer output to be tendered. The court should retain a discretion to decide if the maker of the affidavit is such a qualified person. These are but some examples of how Section 35 may be revised or amended. Whatever the specific changes may be, the broad theme of this approach is to acknowledge the reliability, integrity and authenticity issues that plague electronic evidence by retaining the existing framework. However, the balance between reliability and ease of admissibility needs to be recalibrated in favour of the latter.

31 After the consultation paper was published and two months of public consultation undertaken, the TLDG published a final report which captured the responses to the suggestions for reform. Put simply, five of the respondents to the public consultation were in favour of option two. One respondent was, in substance, in favour of an approach that mirrored option four, one respondent was against both option two and four while the last respondent proposed a new methodology. It is not useful to delve into the details of the responses, primarily because many of the responses that propose novel suggestions lacked sufficient particularity to enable a proper evaluation of the feasibility of such suggestions. It was, however, worth noting that none of the respondents supported maintaining Section 35 as it was. Some felt that the current Section 35 merely leads to a certificate-supporting route (because admission via the express agreement

and approved process modes were infrequently used) which is not ideal.[34] Others felt that a fundamental rethinking of the distrust of electronic evidence needs to be considered.[35]

32 A similar review had been undertaken in England with respect to s 69 of the Police and Criminal Evidence Act, 1984 ("PACE")[36] on which our Section 35 was modelled. Section 69 of the PACE was repealed without replacement pursuant to the recommendation of the Law Commission for the following reasons:

> (a) section 69 of the PACE fails to address the major cause of inaccuracy in computer evidence: human error;
>
> (b) advances in technology make it impossible to comply with s 69 of the PACE as it is increasingly impracticable to certify the proper workings of all the intricacies of the computer operation;
>
> (c) a *recipient* of a computer-produced document, who wishes to tender it in evidence, may well be in no position to satisfy the court about the operation of the computer; and
>
> (d) it is illogical that s 69 of the PACE applies where the document is tendered in evidence, but not where it is used by an expert at arriving at his or her conclusions, nor where a witness uses it to refresh his or her memory. If it is safe to admit evidence which relies on and

34 Daniel Seng and Sriram Chakravarthi, "Computer Output as Evidence: Final Report", (Singapore Academy of Law, 2004), Annex 2, at p 36.

35 *Ibid*, at p 65.

36 69 Evidence from computer records

> (1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown—
>
> (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
>
> (b) that at all material times 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 ; and
>
> (c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.
>
> (2) Provision may be made by rules of court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section such information concerning the statement as may be required by the rules shall be provided in such form and at such time as may be so required.

> incorporates the output from the computer; it is hard to see why that output should not itself be admissible.[37]

33 The Law Commission had reasoned that the major cause of inaccuracy in electronic evidence is human error, not the reliability of the computer itself. Insofar as the reliability of the computer operations is concerned, it was sufficient that the common law maxim of *praesemuntur omnia rite esse acta* would apply.

IV. A VALEDICTION TO SECTION 35

34 Before turning to the new provisions introduced by the Evidence (Amendment) Act 2012, it is perhaps appropriate to reassess our experience with Section 35 in order to articulate the lessons that have been learnt. It cannot be gainsaid that there has been much discontent from practitioners about Section 35 and they have tried very hard to ignore its existence. Given the preponderance of computer output that is admitted as electronic evidence, it is amazing that Section 35 has been used so sparingly, even reluctantly, in our courtrooms.

35 Both the review undertaken by the TLDG as well as the English Law Commission hinted at the problem: for some – or indeed most – types of electronic evidence, special provisions for admissibility is unnecessary simply because such evidence poses no more danger to reliability than other types of evidence. Yet what both groups failed to identify is the fact that while a special admissibility regime is unnecessary for most types of evidence, there still exists a minority category of electronic evidence for which the concerns sought to be addressed by Section 35 are valid. The findings of both groups, therefore, generally suffered from the same flaw Section 35 does: it treats all electronic evidence alike. Fortunately, practitioners took a somewhat contrary approach. In the vast majority of cases, computer output had been treated like any other documentary evidence. It is adduced through its maker or through one of the hearsay exceptions, more likely than not the business records exception. It is on rare occasions that a Section 35 certificate is produced by the party seeking to admit the computer output as evidence. Perhaps this is the first and foremost lesson that ought to be borne in mind.

---

37 United Kingdom, The Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Report 2450, 1997) at [13.7] to [13.10].

1. Authenticity

36 Generally, evidence law makes a distinction between the concepts of "authenticity" and "accuracy" in the admission of documentary evidence. Authenticity has to do with provenance. Under the Evidence Act, this concept is embodied in s 9:[38]

> **Facts necessary to explain or introduce relevant facts**
>
> **9.** Facts necessary to explain or introduce a fact in issue or relevant fact, or which support or rebut an inference suggested by a fact in issue or relevant fact, or which establish the identity of any thing or person whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened or which show the relation of parties by whom any such fact was transacted, are relevant in so far as they are necessary for that purpose.

In order to demonstrate the authenticity of documentary evidence for the purposes of admissibility, one must not only establish the nexus between the document and a relevant fact but also that the document presented in court is, indeed, the document in question. Authenticity, therefore, involves examining the origination of the document, its time of origination, its purpose and its occurrence in order to ascertain the relevance of a particular document.

37 Where authenticity is concerned, this is not an issue that is particular to electronic evidence or computer output. There was therefore no need to enact a particular set of provisions targeted only at electronic evidence to address any concerns regarding authenticity. In fact, the Evidence Act already has a set of extensive provisions that deal with authentication.[39]

2. Accuracy

38 The requirement of accuracy, however, is targeted at ensuring that the information reflected on the document, even if authentic, is accurate and, therefore, worthy of some degree of consideration. There are two ways in which information on a document may not be accurate. The first has to do with the trustworthiness of the information. The law of evidence generally excludes information that is hearsay or an opinion from being considered unless such information falls within specified exceptions. The other concerns the integrity of the information. Where ordinary handwritten or

38 See also illustration (a) of s 9, Evidence Act.

39 See ss 69–92, Evidence Act.

typewritten documents are concerned, this may involve issues of tampering or forgery.

(a) Trustworthiness

39 Likewise, the issues concerning the accuracy of the contents of computer output, insofar as they relate to hearsay and opinion, are no different from those assailing other documentary evidence. Case law has demonstrated that even if a piece of electronic evidence satisfies the requirements of Section 35, the requirements of the rule against hearsay must still be complied with. Such was the import of the decision in *Jet Holding Ltd and others v Cooper Cameron (Singapore) Pte Ltd and another and other appeals*.[40] In that case, the plaintiffs successfully sued the defendant for a negligent breach of duty but failed to prove most of their losses. This was because the bulk of the plaintiffs' documents which allegedly proved the quantum of their loss were not admitted into evidence. Some of these documents were computer output which the trial judge felt contained hearsay content. On appeal, the plaintiffs argued that since the computer output complied with Section 35, the computer output should be accepted into evidence. The Court of Appeal disagreed. It was held that compliance with Section 35 did not mean that the content of the output should be accepted *per se*. It must still be shown that the content did not offend the rule against hearsay. The rule against hearsay is therefore an independent consideration and Section 35 does not, and should not, address that point. The same can be said of opinion evidence that is contained within an electronic document.

(b) Integrity

With electronic documents, the integrity of the information contained within may be impinged in three ways. One, like tampering or forgery of traditional handwritten documents, an electronic document may be surreptitiously edited or overwritten by someone else after the original author had entered the intended information ("the tampering problem"). Second, the user of the computer may, in the first place, enter incorrect information, whether due to an unfamiliarity with the computer or other reasons, causing the computer to also, accordingly, display inaccurate

40 [2006] 3 SLR(R) 769.

information ("the data entry problem"). Third, there is the possibility of errors in the hardware or software program resulting in inaccurate output ("the reliability problem"). It is submitted that Section 35 was intended to address this last category; the prior two categories are (again) not unique to electronic evidence and have been or may be comprehensively dealt with in the other parts of the Evidence Act or through common law.

40 Insofar as the tampering problem is concerned, this problem is akin to forgery and is, therefore, not new to law. Usually, this problem is addressed by having the original author of the document testify as to whether the information on the computer output accurately reflects the information he had entered into the computer. It is up to the party asserting that the document is not what it is appears to be to persuade the judge, whether by other extrinsic objective evidence or by witnesses' testimony, that the document had been edited or changed. This procedure may generally be used even with information contained on an electronic medium.

41 The data entry problem is also not unique, even if it may be due to the computer user being unfamiliar with the computer program or device. This problem is no different from the writer of a handwritten document penning down inaccurate information. Like the tampering problem, the accuracy of the contents of the document, in this regard, is usually tested at trial by the adduction and cross-examination of relevant witnesses and there is no reason why such should not be the same where wrong information is entered into a computer. After all, the workability of the computer is not itself impinged. Should there be any doubts about the accuracy of information contained in electronic evidence through inaccurate authorship, the weight accorded to such documents may accordingly be diminished.

42 The real difficulty with electronic evidence is the reliability problem where the computers may properly be said to be the author of the output. Whether the computer has properly performed its function is something that is not within the immediate knowledge of the computer user. That the computer may not have done so is something that cannot be ruled out easily. For this category, we may identify the computer, rather than a human being, as the originator or the author of the electronic evidence. Under this category, we would include the following.

43 *Output that has been produced by a computer by automation and without human supervision*. For example, a traffic camera may be

programmed to work every time it detects a vehicle exceeding a certain speed limit. In such an instance, the court does not have reference to a human originator to ascertain if the evidence provided in court is accurate. There is no traffic police officer, armed with a radar speed gun, stationed with the camera to testify that a car was indeed exceeding a certain speed when its picture was taken. Even though the programming must initially have been done by a human being, there is no actual supervision of the computer when the software kicks into action. For this reason, the computer may be deemed the originator of the output that eventuates.

44 *Output that has been produced by a computer which was used to analyse certain original information to reach a conclusion*. A calculator, for instance, is supposed to use information provided to it in a pre-programmed manner to achieve a desired result. Machines that are used to analyse blood, breath or urine to test for alcohol or drugs are other examples of such computers. They use the test samples, whether blood, breath or urine, apply a certain formula and produce a result or conclusion. Again, a human originator must first program the computer and, perhaps, provide the initial information. Nevertheless, once programmed, there is no supervision as to how the computer carries out the mathematical or scientific function to arrive at the conclusion.

45 Because the computer may be properly deemed the author of the output in such cases, the court must at least be satisfied that the computer was properly designed and programmed and that there is no reason to suspect that the computer has deviated from the manner in which it was originally programmed to work. For this reason, if parties cannot reach an agreement not to dispute the authenticity of the contents of the output, a Section 35 certificate would have had to be produced to dispel any nagging suspicion that the information contained on a specific document may be inaccurate because any perceived inherent fragility of computers. Section 35 therefore provided the perfect balance between the need to ensure that the information contained is accurate yet, at the same time, making the process practical. Furthermore, all that is required is to call a witness who is familiar with the computer in the sense that the witness can attest to the fact that the computer is working properly. An expert is not necessary.[41] As a result, the accuracy of a specific piece of information may be tested without too much hassle.

41 *Lim Mong Hong v Public Prosecutor, supra* note 9.

3. Foremost lesson

46 Apart from computer output that are in truth "authored" by a computer, the majority of electronic evidence do not face evidential problems that are unique to computer output (*ie*, the reliability problem). Even if they may face other evidential issues, these issues (*ie*, authenticity and trustworthiness, the tampering problem and data entry problem), as explained earlier, may be resolved by resort to general evidence law. As such, there was no need for such evidence to satisfy the requirements of Section 35. That they were subjected to the requirements of Section 35, it is submitted, is the reason why there is much dissatisfaction with Section 35 from the bar.

47 Hence, Section 35 was not necessary for the preponderance of computer output that were sought to be admitted as electronic evidence. Had they been exempted from Section 35, the law would have expedited their admission in court without particularly compromising the reliability and accuracy of the evidence. Be that as it may, as water tends to find its natural course, so too did practitioners find ways to admit computer output evidence in our courtrooms without the formalities of Section 35 unless absolutely necessary. What this highlights is the fact that the formalities of Section 35 were unnecessary for the majority of computer output that were sought to be admitted as electronic evidence.

V. THE EVIDENCE (AMENDMENT) ACT 2012: BETTER LATE THAN NEVER

48 At the Second Reading of the Evidence (Amendment) Bill 2012, the Minister for Law (Mr K Shanmugam) articulated the reason for the repeal of Section 35 and the introduction of presumptions in its place:

> The current framework for the admission of computer output evidence is found in sections 35 and 36. They were introduced in 1996. Computer technology was then in its infancy. A cautious approach was therefore taken. Currently, short of agreement between parties, computer output can be admitted only if: (i) it is produced in an approved process; or (ii) it is shown to be produced by a properly operating computer which was properly used.
>
> This is a somewhat cumbersome process not consonant with modern realities. With the benefit of experience, we can say now that computer output evidence should not be treated differently from other evidence. Sections 35 and 36 are therefore repealed. In addition, there will be presumptions facilitating the admission of electronic records. For example,

> where a device is one that, if properly used, accurately communicates an electronic record, it will be presumed that an electronic record communicated by that device was accurately communicated. Sounds a little circular, but it does make sense. Further, documents in the form of electronic records will be treated as primary evidence.[42]

49 A perusal of the Parliamentary Report of this Second Reading of the Bill leads to an interesting observation: there was no debate on the repeal of Section 35. Perhaps its time had really passed. The only Member of Parliament who spoke at any length on the repeal of Section 35 (apart from the Minister for Law who was moving the Bill) was Non-Constituency Member of Parliament Mrs Lina Chiam:

> I support this Bill which modernises the law in treating documents created electronically as primary documents. I can only wish that this Amendment Bill was put before us earlier, since the relevant reports from the Singapore Academy of Law were published back in the year 2004.[43]

50 As Section 35 went quietly into the night, the Evidence (Amendment) Act 2012 introduced a slew of amendments to the Evidence Act which essentially placed computer output evidence on the same footing as other documentary evidence.

1. Computer output as primary evidence

51 To give effect to Parliament's intent to treat electronic evidence as primary evidence, a new Explanation 3 was introduced to the definition of "primary evidence" in s 64:

> **Primary evidence**
>
> **64.** Primary evidence means the document itself produced for the inspection of the court.
>
> …
>
> *Explanation* 3.—Notwithstanding Explanation 2, if a copy of a document in the form of an electronic record is shown to reflect that document accurately, then the copy is primary evidence.
>
> *Illustrations*
>
> (a) An electronic record, which has been manifestly or consistently acted on, relied upon, or used as the information recorded or stored on the computer system (the document), is primary evidence of that document.

42 *Singapore Parliamentary Debates, Official Report* (14 February 2012) vol 88 at col 45.

43 *Ibid*, at col 50.

> (b) If the electronic record has not been manifestly or consistently acted on, relied upon, or used as a record of the information in the document, the electronic record may be a copy of the document and treated as secondary evidence of that document.

52 Hence, accurate copies of electronic records "which [have] been manifestly or consistently acted on, relied upon, or used as the information recorded or stored on the computer system (the document)" will henceforth be considered primary evidence of that electronic document. This approach focuses on parties' *past* treatment of an electronic record in determining whether it is primary evidence. If a copy of an electronic record has in the past been treated by parties as accurate, then it is primary evidence. The nature of the information (*ie*, the purpose for which the information was generated) is irrelevant.

53 Section 10 of the Electronic Transactions Act (ETA) adopts a different approach to determining when an electronic record is an original:

> **Provision of originals**
>
> **10.**—(1) Where a rule of law requires any document … to be provided or retained in its original form … that requirement is satisfied by providing or retaining the document … in the form of an electronic record if the following conditions are satisfied:
>
> (a) there exists a reliable assurance as to the integrity of the information contained in the electronic record from the time the document … was first made in its final form, whether as a document in writing or as an electronic record;
>
> (b) where the document … is to be provided to a person, the electronic record that is provided to the person is capable of being displayed to the person;
>
> …
>
> (2) For the purposes of subsection (1)(a) —
>
> (a) the criterion for assessing integrity shall be whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display; and
>
> (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

54 For an electronic record to be considered a digital original under the ETA, there must exist "a reliable assurance as to the integrity of the

information contained in the electronic record".[44] The integrity of the electronic record depends on whether the information contained in the electronic record "has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display".[45] There must be reliable assurance of such integrity; and "the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances".[46] Under this approach, the *purpose of creation* is the key determinant of the level of security that is required before an electronic document qualifies as a "digital original". Hence, if the information that is created has a high level of significance, *eg*, e-mail instructions from a private banking customer to his private banker to enter certain high-value transactions, the level of security has to be higher before the electronic record is considered to be an original (*eg*, use of encryption or digital signatures).

55 The practical difficulties that are presented by these two contrasting approaches may be illustrated in the following manner. A private wealth customer of a bank gives oral instructions over the telephone to his private banker to enter into certain transactions. The bank has an audio record of the conversation which is stored in its internal systems with a high level of security. The customer has made a simple audio record using an electronic voice recorder, and stores a copy of the conversation on his home personal computer. A dispute arises over the instructions given by the customer. Both audio records are produced and parties treat each of them as accurate records of the telephone conversation when the disputed instructions were given. For the purpose of discovery and inspection, and eventually at trial, the law requires that the best evidence be tendered. This means that an original, if available, has to be tendered as primary evidence of the document. If not available, a copy may be tendered as secondary evidence. Hence, are both originals? Can both be tendered as primary evidence?

56 Under the ETA "purpose of creation" approach, given the nature and significance of the conversation, the bank's audio record stored in its secure system may qualify as a "digital original". The customer's audio record will, in all likelihood, not qualify as an original under s 10 of the ETA. The

44 Section 10(1)(a), ETA.
45 Section 10(2)(a), ETA.
46 Section 10(2)(b), ETA.

customer will therefore not be able to produce his audio record – whether for discovery and inspection or at the eventual trial – as an original record of the telephone conversation. The bank, on the other hand, will be able to produce its audio record as an original record.

57 Under the "past treatment" approach in Explanation 3 to s 64 of the Evidence Act, the result is different. Since parties had previously treated both audio records as originals, both the bank's audio record and the customer's audio record will be treated as primary evidence. Each party may disclose its audio record as "originals" for discovery and inspection, and produce it at trial for the court's inspection as such.

58 The present authors prefer the "past treatment" approach as it only clothes an electronic document with the status of primary evidence after parties have "manifestly or consistently acted on, relied upon or used" the electronic document as an accurate copy. It reinforces past conduct and does not prescribe different standards depending on the purpose for which the electronic document was created. Be that as it may, the "purpose of creation" approach under s 10 of the ETA can accommodate consideration of "all relevant circumstances" in determining the relevant standard of reliability.[47] It is submitted that there is therefore sufficient latitude for parties' past treatment to be taken into account as a relevant circumstance. Therefore, where parties had previously treated an electronic document as accurate, this may be sufficient to qualify it as an original under the "purpose of creation" approach as well. Given practitioners' past pragmatism with Section 35, one may confidently expect that such a harmonious interpretation of s 64 of the Evidence Act and s 10 of the ETA will be adopted in due course.

2. Proof of authenticity

59 Section 9 Evidence Act is amended by the introduction of a new illustration (g):

> (g) *A* seeks to adduce evidence against *B* in the form of an electronic record. The method and manner in which the electronic record was (properly or improperly) generated, communicated, received or stored (by *A* or *B*), the reliability of the devices and the circumstances in which the devices were (properly or improperly) used or operated to generate, communicate, receive

47 *Ibid.*

> or store the electronic record, may be relevant facts (if the contents are relevant) as authenticating the electronic record and therefore as explaining or introducing the electronic record, or identifying it as the relevant electronic record to support a finding that the record is, or is not, what its proponent *A* claims.

60 This amendment is in effect a legislative endorsement of the pragmatic approach taken in *Ng Koo Kay Benedict and another v Zim Integrated Shipping Services Ltd*,[48] *viz*, oral testimony is sufficient and written certification is not mandatory. The difference is that under the former Section 35, the onus is on the party adducing electronic evidence to prove authenticity and accuracy, but more specifically, the matters set out in s 35(1)(c). The effect of this illustration is that while the evidential burden remains on the party seeking to adduce electronic evidence, the facts that are relevant will depend very much on the pleaded case and the issues in dispute. In other words, electronic evidence will be adduced and proved like any other type of documentary evidence.

3. Presumptions of authenticity

61 Since the decision in *Jet Holding Ltd and others v Cooper Cameron (Singapore) Pte Ltd and another and other appeals*,[49] it was clear that the accuracy of electronic evidence had to be proved either through direct evidence (*ie*, through its maker) or via one of the hearsay exceptions. The Evidence (Amendment) Act 2012 introduced a set of presumptions to facilitate the admission of electronic evidence.

(a) Electronic records that are produced ordinarily by a device is presumed to have been produced by it

62 The first presumption appears to be an attempt at restating the common law maxim *praesemuntur omnia rite esse acta*: the law presumes that mechanical instruments were in order when they were used. This presumption is intended to apply to mechanical instruments that, more often than not, operate properly.[50] The law has thus caught up with culture, as modern society operates on the assumption that computers are

48 *Supra* note 33.

49 *Supra* note 40.

50 See Colin Tapper, *Cross & Tapper on Evidence* (11th Ed) at p 40.

working properly most of the time. This obviates the necessity for especial proof of reliability:

> **Presumptions in relation to electronic records**
>
> **116A.**—(1) Unless evidence sufficient to raise doubt about the presumption is adduced, where a device or process is one that, or is of a kind that, if properly used, ordinarily produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record.
>
> *Illustration*
>
> *A* seeks to adduce evidence in the form of an electronic record or document produced by an electronic device or process. *A* proves that the electronic device or process in question is one that, or is of a kind that, if properly used, ordinarily produces that electronic record or document. This is a relevant fact for the court to presume that in producing the electronic record or document on the occasion in question, the electronic device or process produced the electronic record or document which *A* seeks to adduce.

63 This presumption can be relied upon in cases where the computer is the "author" of the electronic evidence. The primary facts that need to be proved are (a) the ordinary behaviour of the computer and (b) that it was properly used on the occasion that the electronic evidence was produced or communicated. To prove the former, it will be necessary to demonstrate that the computing device, when working properly and used properly, produces a certain type or types of output. To prove the latter, evidence has to be led to show that on the occasion in question the computing device was used properly. Once these primary facts are proved, it is submitted that there is one further step necessary. It must be shown that the electronic evidence in question is of the same type of output that the computing device ordinarily produces. The statutory presumption can then be invoked to presume that the electronic evidence was produced by that computing device. It is implicit that the computing device in question was working properly on the occasion in question. Otherwise, the electronic evidence in question would not be properly formed. To put it in another way, the ordinary behaviour of a computing device is to produce a properly formed output, and not an incomplete or poorly formed one (*ie*, gibberish).

64 It may be noted that the presumption draws a distinction between electronic evidence that is ordinarily produced by the electronic device and electronic evidence that is accurately communicated. The presumption of accuracy only applies to communication devices, *eg*, telecommunications

and network equipment. Hence, a fax machine will be presumed to have transmitted the document accurately; similarly, network equipment and transmission devices. This distinction makes sense as communication devices essentially take an input and transmit it such that the output at the destination is exactly the same as the input. It performs no further processing on the input to transform it, for that is not the purpose of communication devices. Their purpose is accurate transmission. Again, it is implicit that the communication device was working properly in order for the transmission to be accurate.

65 For devices that produce an electronic record, the presumption only works to authenticate (*ie*, prove that the electronic record was produced by that device) but does nothing for the accuracy of production. Going back to the earlier illustrations involving traffic cameras, calculators, and blood, breath and urine analysers, the statutory presumption does not go so far as to presume that the computer output is accurate. The presumption merely helps to prove provenance, *viz*, that the computer output was produced by said device. In order to prove accuracy or reliability, the party adducing the electronic evidence will need to discharge its evidential burden by calling an appropriate witness to give evidence in the nature of the new Illustration (g) of s 9 of the Evidence Act.[51]

66 The effect of these two provisions is that where no issue is raised on the accuracy on an electronic record "authored" by a computer, the presumption alone is sufficient to presume that the electronic record was produced by it in the ordinary course and is thus admissible. The only primary facts that are necessary are proof of its ordinary behaviour and that there was proper usage of the computer in question on the occasion in question. Once this hurdle is crossed, the presumption kicks in. It is only on occasions where the accuracy of the electronic record is challenged that the party seeking to admit the electronic record into evidence will have to adduce positive proof of reliability. This may be fulfilled by calling the requisite witnesses familiar with the workings of the computer to provide testimony – factual or expert – to satisfy the court on reliability. If the computer was used as a tool by a human author to produce the electronic record – *eg*, a letter typed using a word processing software progam – the author may be called as a factual witness. If the computer was the "author" of the electronic record – *eg*, end-of-day trading statements that are

51 See above at [59] and [60].

automatically generated – then expert witnesses may have to be called to give testimony to the workings of the computer in order to assure the court of its reliability.

(b) Presumptions that dispense with proof of production

67 The next set of presumptions essentially makes it easier to adduce electronic evidence that is obtained from some other party. In the scheme of litigation, there are essentially friendly parties, adversaries and neutral parties. Where electronic evidence has been produced by a friendly party (*eg*, an employee or associate), the evidential burden lies on the party that seeks to adduce it. There will usually be no difficulties in calling the maker or adducing the evidence through one of the hearsay exceptions.

68 Where electronic evidence has been obtained from your adversary (including his associates), then it becomes a little more difficult to prove authenticity. The relevant maker will usually turn hostile as a witness and the party seeking to rely on it will usually not have knowledge of the full facts in relation to its provenance. The latter – *ie*, insufficient knowledge to prove provenance – will often be true for documents obtained from a neutral third party. Hence, the set of assumptions assumes that since the electronic evidence is either from a neutral party or an adversary, it is safe to presume authenticity.

69 With respect to third-party electronic evidence, the primary facts that need to be proved in order to rely on the presumption is that the electronic evidence was generated by a neutral third party in the usual and ordinary course of business and not under the control of the party seeking to adduce it. These twin requirements ensure impartiality:

> (2) Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the electronic record.
>
> *Illustration*
>
> *A* seeks to adduce evidence against *B* in the form of an electronic record. The fact that the electronic record was generated, recorded or stored in the usual and ordinary course of business by *C*, a neutral third party, is a relevant fact for the court to presume that the electronic record is authentic.

70 Central to this presumption is neutrality or the inability to control. To have "control" is to have the ability "to exercise authoritative or dominating influence"; *ie*, to direct the actions of another.[52] "Control" must therefore involve a significant measure of influence over the actions of the party that is generating, recording or storing the electronic evidence, *eg*, a controlling interest in a subsidiary or related company. Mere contractual obligation or "power" – to use the parlance of discovery, *ie*, possession, power and custody – is insufficient. In discovery applications, it is not uncommon for a party to the proceedings to be ordered to produce documents within its power to obtain, *eg*, historical account statements from his banker or daily statements of transactions in a foreign exchange or equity trading account. Such statements ought to benefit from this presumption. Needless to say, where a third party is compelled to provide discovery, *eg*, third party discovery against an Internet Service Provider (ISP) for the production of Internet Protocol (IP) addresses and internet usage logs, the electronic records produced will benefit from this presumption.

71 If the intention is for this presumption to obviate the need to call a representative from the neutral third party to the witness stand, the presumption does not go far enough. In order to establish that the electronic records are produced "in the usual and ordinary course of business", it will be necessary to call a witness from the neutral third party to provide some evidence of how the records were ordinarily produced. While this may be necessary when we are dealing with technical records like IP addresses and server logs, this may be a little inconvenient when we are dealing with more common records like bank account or trading statements. Here, unless we are able to benefit from one of the hearsay exceptions,[53] we may still be required to trouble the neutral third party to send a representative as a formal witness.

72 Before considering the next presumption, it needs be commented that for criminal proceedings, the investigation officer and an accomplice are both considered to be parties to the proceedings. The former ought to be considered an adversary while the latter may either be a friendly party or an

52 See <http://www.tfd.com/control>.

53 For example, s 171, Evidence Act provides: "…a copy of any entry in a banker's book shall in all legal proceedings be received as prima facie evidence of such entry and of the matters, transactions and accounts therein recorded."

adversary, if he has turned to be a Prosecution witness against the accused person.

73 With respect to electronic evidence obtained from your adversary, the phrase that is employed in this presumption is "party who is adverse in interest". It is wider than the adverse party in the immediate litigation and encompasses the adversary's associates so long as the associates' interests are adverse to your client's, *eg*, companies in the adversary's group of companies:

> (3) Unless evidence to the contrary is adduced, where an electronic record was generated, recorded or stored by a party who is adverse in interest to the party seeking to adduce the evidence, the court shall presume that the electronic record is authentic in relation to the authentication issues arising from the generation, recording or storage of that electronic record.
>
> *Illustration*
>
> *A* seeks to adduce evidence against *B* in the form of an electronic record. The fact that the electronic record was generated, recorded or stored by *B*, who opposes the relevance of the evidence, is a relevant fact for the court to presume that the electronic record is authentic.

74 One key difference between the adverse party presumption and the neutral party presumption is that for the former there is no need to prove the "the usual and ordinary course of business" as a primary fact before the presumption can be invoked. For the adverse party presumption, any electronic record produced by the adverse party can be admitted under this presumption. Hence, when a customer sues his bank or ISP, any statement or log that he has obtained from his adversary will be admissible upon proof that it was produced by his adversary.

75 A final comment may be made with respect to this set of presumptions. They operate on records that are "generated, recorded or stored" by either a neutral or adverse party. Generation and recording involve active steps taken to produce the electronic records. By contrast, storage is passive in the sense that the electronic records are not produced by the neutral or adverse party, merely in their custody. Where the electronic records are merely retrieved from storage, the evidential burden of proof does not end with the reliance on these presumptions. One must take steps to prove authorship or have the evidence admitted under one of the hearsay exceptions. This is best illustrated by the example where a party's documents are stored on an online storage service, *eg*, Dropbox. Documents retrieved from it will benefit from the neutral party

presumption since it was obtained from a party whose usual and ordinary course of business is to store documents provided to it on its online platform for future retrieval, and it cannot be said to be under the control of its customer (*ie*, the party to the proceedings). However, the party seeking to adduce any of the documents retrieved from Dropbox into evidence must go further to consider the nature of the documents. If a word processor document, then the author has to be called. If a word processor document produced by an adverse party, then the adverse party may be invoked. If a copy of a bank account or trading statement, then the neutral party presumption may (again) be invoked in respect of that document.

(c) Approved process

76 Before leaving the presumptions, it ought to be noted that the new s 116A retains provisions for an approved process and the Minister is empowered to make regulations for such imaging systems. The only presumption that deals with both authentication and accuracy is the present one in relation to electronic evidence reproduced from an approved process:

> (6) Where an electronic record was recorded or stored from a document produced pursuant to an approved process, the court shall presume, unless evidence to the contrary is adduced, that the electronic record accurately reproduces that document.

77 The approved process presumption is a fairly narrow and specific one. It works only for documents "recorded or stored through the use of an imaging system". Further, the entire imaging and reproduction process has to be certified in accordance to regulations pronounced by the Minister. Once these primary facts are proved, it is presumed that the electronic document is an accurate reproduction of the image of the original document.

78 Although the previous approved process method under Section 35 had probably fallen into disuse, there must be sufficiently large investments into existing systems that rely on the approved process method of proving electronic evidence to justify retaining the approved process as a presumption. It remains to be seen if the approved process will find its second wind. With the present policy shift to provide for a set of presumptions to ease the proof of electronic records, it is unlikely that there will be any rush towards a more elaborate and thorough procedure that requires scrutiny of the process of digitising documents and regular process

audits. In other words, perhaps this presumption is retained to ensure "backward compatibility" and to preserve past investments.

VI. CONCLUSION

79 Section 35 was enacted during a time when the general population was still beginning to come to terms with advance technology. Accordingly, the form it took reflected an inherent suspicion of the unfamiliar and complex. Unfortunately, such inherent tendencies often augment the problem that actually exists. Where Section 35 was concerned, the scope it covered far surpassed that which was necessary. For this reason, it was widely unpopular amongst practitioners during its brief lifetime.

80 It must, therefore, come as a relief to many that Section 35 may now be consigned as an aberration in history of evidence law. With the repeal of Section 35, it may be fairly said that it will no longer be more difficult to adduce electronic evidence in court when compared to traditional forms of evidence. In fact, with presumptions created to facilitate proof of authenticity of certain kinds of electronic evidence, one may even go further to say that electronic evidence now in fact enjoys some advantage in certain areas. In hindsight, such developments have an import far beyond evidence law. It simply reflects the fact that the technology age has truly and finally come of age.

PRESENTATION OF COMPUTER FORENSIC EVIDENCE

LIANG Hanting
LLB (National University of Singapore)

Rakesh **KIRPALANI**
LLB (National University of Singapore)

TAN Sze Yao*
BA Law (Cantab), LLM (Columbia University)

I. INTRODUCTION

1 Evidence is a cornerstone in litigation. When a matter is brought to Court, allegations of wrongful acts and claims for loss and damage must be substantiated with the necessary evidence. Such evidence usually goes towards exhibiting the *elements* of the alleged causes of action, as well as the *actual* loss and damage suffered.

2 In civil matters, whether a plaintiff is able to prove his case normally turns on the contemporaneous documentary evidence placed before the Court. Parties rely heavily on the disclosure of all the necessary documents to place the sequence of events leading to the allegations in context.

3 Once upon a time, paper represented the state of the art on which all documentary evidence was recorded. Parties wrote letters to one another, a process which sometimes took weeks, especially where the recipient was overseas and the letter was couriered by ship. Contracts and agreements were executed only in person and original copies were provided to the parties.

4 When the facsimile came along, the time taken for correspondence to reach the recipient was greatly reduced, and the speed of transmission was

* The authors express their deepest appreciation to Darren Cerasi and Lau Kok Keng for their valuable comments and contributions to this article. Some of the ideas in this article springboard from the panel "Presentation of Computer Forensic Evidence" chaired by Senior Assistant Registrar Yeong Zee Kin, with members Ms Indranee Rajah, SC, Lau Kok Keng, Lem Chin Kok, Ramesh Moosa and Darren Cerasi.

therefore greatly increased. Nevertheless, the fact remained that most contemporaneous documents existed in paper form.

5 Even today, to a large extent, paper continues to be the preferred medium through which evidence is presented to the Court. When a matter goes before the Court, courtrooms are often inundated with paper bundles and arch files, with the parties patiently taking the time to each search for the relevant document in question at the appropriate time. Care is exercised in ensuring that everyone – in particular the judge – is on the correct page before any evidence is gone through in detail.

6 In recent years, however, the state of the art has changed tremendously, and paper can no longer be said to be the obvious choice for maintaining records.

7 With the advent of electronic mail, the internet, the hard disk, flash drives, smart phones, social media and cloud storage, amongst others, there is a growing preference for individuals and organisations to maintain their records in electronic form. This paradigm shift has been in no small part facilitated by the ease of access, convenience and increased efficiency provided by such technologically advanced storage mediums.

8 Accordingly, when matters are litigated, these electronic records form the basis of the electronic evidence that comes to be presented before the Court.

9 Where there is general resistance by parties to deal with the evidence in electronic form because they may be unfamiliar with how to handle or present such evidence to the Court, the temptation to convert the electronic evidence into paper form is strong. In most instances, this retrograde process, quite apart from being inefficient and costly, is also likely to result in the best evidence in the matter not being placed before the Court.

10 Dealing with evidence in electronic form has multiple advantages, such as the ability to use keyword searches and to refer to metadata. Unlike hard copy documents, it is also not as easy to misplace or destroy electronic evidence. Importantly, there is a possibility that electronic evidence which has been deleted (whether maliciously or otherwise, for instance via inadvertent file corruption) can be recovered through modern computer forensic techniques.

11 To avail themselves of these advantages, parties would be well-advised to deal with the evidence in their native electronic form where possible, so

as to ensure the speedy and efficient administration of justice, and to vouchsafe that the best evidence is placed before the Court for consideration.

12 In respect of parties unfamiliar with electronic evidence, guidelines on how best to present such computer forensic evidence to the Court – from the point of appointing the computer forensic expert, whose role has become extremely important, to the preparation of the computer forensic expert's report for the Court's consideration – would be instructive. It is important that parties and their computer forensic expert understand that they must communicate technical matters clearly to the Court. The forensic expert report needs to be simple enough for the parties and the Court not to get lost in technical jargon, but probative enough to establish each litigant's case.

II. SELECTION AND BRIEFING OF EXPERTS

1. Choosing the right experts

13 The importance of choosing the right computer forensic expert cannot be overstated. The computer forensic expert will greatly influence the quality and quantity of the computer forensic evidence gathered, assist in communicating the evidence to the bench, and lend credibility to bolster a legal case.

14 Compared to choosing experts in other fields, selecting the right computer forensic expert is a slightly different endeavour. This is because, at present, there are no internationally-recognised accreditation or qualification systems to quickly identify suitable computer forensic experts.

15 Although there have been efforts made by various countries to establish professional regulatory bodies to initiate and regulate a register of competent forensic practitioners, such as the short-lived Council for the Registration of Forensic Practitioners in the United Kingdom,[1] there is still some way to go before standardisation on any manner of global scale.

1 Stephen Mason and Andrew Sheldon, *Proof: The Investigation, Collection and Examination of Digital Evidence* (LexisNexis Butterworths, 2nd Ed, 2010) at p 53.

16 Nevertheless, a good starting point would be to identify which computer forensic tools an expert has been trained in, as there is a strong industry emphasis on the same. The computer forensics industry recognises certain tools as industry standards that can accomplish the necessary forensic tasks required of a computer forensic expert.

17 A review of the following three main considerations will help crystallise the requirements that are demanded of the computer forensic expert, and will likely expedite the shortlisting process:

(a) whether a high-intensity review is required – a high-intensity review is conducted where the results of the forensic investigation are required in a very short period of time. For example, a high-intensity review is necessary in a situation where an employee is suspected of wrong-doing, and it is known that he intends to leave the jurisdiction soon after. It is therefore important to know whether the expert has the resources to conduct a high-intensity review within the limited timeframe if so required;

(b) the number of computer devices targeted for review – generally, the greater number of computer devices that are targeted for review, the more time and resources required by the expert to complete the review within a stipulated timeframe; and

(c) whether a low-profile "undercover" review is required – in certain situations, the computer forensic review has to be executed in a low profile manner so as to avoid alarming the subjects under investigation. Certain experts will possess more experience and resources to conduct this variety of "undercover" review.

2. Briefing your expert

18 When the computer forensic expert is well-briefed, he is likely to be more able to employ the resources at his disposal to complete tasks with minimal supervision. In contrast, where the briefing has not been conducted thoroughly, the expert may be unable to anticipate the tasks and output expected of him, deploy his resources in a less-than-optimal fashion, and require constant feedback or input to achieve the stated deliverables.

19 The two-way briefing process is therefore an important one which should not be overlooked, and is most effective when the client, the client's

information technology ("IT") department (if there is one) and the client's lawyers engage the forensic experts actively. Each of these parties will invariably be involved in one way or another in the computer forensic review process, and their collective input at the briefing stage is crucial for the briefing to be an effective one.

20 As with any briefing concerning a litigious matter, an exposition of all the relevant facts by the client is essential. When it is necessary to involve computer forensic experts in the matter, one should not assume that the computer forensic expert only needs to know what computer systems and electronic devices the client or his opponent uses. A skilled computer forensic expert is much more than just a technician and can add significant value to the conduct of a matter if provided with a comprehensive background of the relevant facts.

21 It is therefore advantageous to brief the computer forensic expert together with the lawyers. The experts should be provided with the following information:

(a) background and context – this information will enable the expert to tailor the type of forensic review to the specific requirements of the matter. Contrary to popular belief, there is no one standard method by which a forensic review may be executed, and the client has a large role to play to enable the expert to identify the ideal forensic review process. For example, if the investigation concerns the potential copyright infringement of proprietary software, the expert will rely on specific tools or programs in order to execute a comparison of the software source code. In contrast, if the matter relates to ex-employees who may have taken the company's confidential and proprietary information, different tools and analytical techniques will be used to search the ex-employees' electronic devices for incriminating emails;

(b) number, type and capacity of electronic devices targeted for review – this information will enable the expert to allocate the appropriate resources for the task, as well as avert a situation where an expert subsequently discovers that he does not have the necessary tools to conduct a review of certain devices;

(c) the profiles of the people who are being subject to investigation – the forensic review will be a more comprehensive one when the focus is placed on the people subject to investigation, as opposed to

having the focus placed on the electronic devices targeted for review. Using the information provided by clients, experts are able to build profiles of the investigated persons, and these profiles help to calibrate the forensic review strategy adopted. The main types of information that should be provided include, for example, how heavily a certain person relies on his or her electronic devices, what level of technological proficiency that person has, the person's gender, character, and longevity in the company.

(d) timeframe for the forensic review to be completed – the review process can be a lengthy one, spanning the stages of information gathering, analysis and presentation. It is therefore imperative for the client to communicate the timeframes in which the forensic review must be completed, so that the expert can evaluate the resources necessary for those timeframes to be observed; and

(e) special parameters for the forensic review – the expert should also be briefed of any special parameters that must be observed for the execution of the forensic review. These parameters include, for example, whether the review should be conducted "undercover", whether a search and seizure of electronic devices is necessary, and whether any information targeted for review exists on a cloud server (for example, emails on MSN Hotmail or Gmail – although covert reviews at present will be unlikely to unearth information stored in online repositories controlled by the person under investigation).

22 Besides recommending the appropriate computer tools and forensic review strategies, the computer forensic expert should draw from his experience and be alert to other considerations, which the client or the client's lawyers might not have considered.

23 At the conclusion of the briefing process, parties should aim to have clarity with respect to the following issues:

(a) the deliverables that the expert needs to achieve – these can include affidavits relating to the forensic review process or to the import of the forensic data, and statistical reports;

(b) the expert's role in analysing the forensic information – depending on the complexity and nature of the review, the expert may be able to assist in the analytical process by doing first-level reviews of the data; and

(c) the costs involved – contrary to popular belief, the costs of conducting a forensic review are not always prohibitive. If the briefing process is executed well, the experts should be able to provide a solution that is both customised and cost-efficient, the usual inverse relationship between these two outcomes notwithstanding.

III. INFORMATION GATHERING AND ANALYSIS

24 It is important at the information gathering stage to ensure that one is:

(a) on the one hand, as comprehensive as possible with regard to the target devices and locations from which information is to be gathered so as to ensure that all relevant information will be collected, analysed and placed before the Court; and

(b) on the other hand, as fastidiously selective as possible with regard to the target devices and locations so that information gathering efforts are focused on the relevant devices and locations. An abundance of caution may sometimes lead information gathering efforts to target irrelevant devices and locations which may detract from efforts towards key target devices and locations, and increase the time and costs spent at this juncture.

25 The information to be gathered and the target devices concerned will also be affected by how an organisation stores its information, particularly as we progress into a world where hosted cloud solutions have become increasingly popular. If an organisation stores its information on its own servers, it would probably have certain procedures in place for legal or litigation holds, and the computer forensic expert would do well to familiarize himself with these.

26 In deciding which devices to target, other factors to consider would be whether it would be necessary to shut down a sizeable number of the organisation's computers, the length of time for such a shutdown, the length of time it would take to reboot systems and whether it would be acceptable to the organisation in the first place. Discussions may have to take place on how best to reduce downtime for the organisation or the individual. These additional factors, however, appear to be of decreasing significance: most computer forensics companies do not need to shut down an organisation's entire network in order to carry out their work, and

physical images of individual computers are captured relatively quickly. Furthermore, it has become more acceptable to capture "live" forensic data from servers that cannot be shut down, such as mission critical servers.

27 As hosted cloud solutions become more popular, one interesting question which arises is how convenient it would be to extract such information from the cloud service provider. Would the cloud service provider tolerate any downtime to its servers? The short answer to this is that, like computer networks in organisations, servers used to host cloud applications do not have to be shut down for computer forensic work to be carried out. These servers tend to be virtualised environments which can be imaged live. Incidentally, cloud providers and third party software developers are also producing applications that allow cloud users to implement their own litigation holds for data stored in the cloud, although this would be an issue that should be considered at the time such service contracts are entered into.

28 Given the ease with which electronic evidence can be deleted or modified, the preservation of the chain of custody of such evidence is of paramount importance in the collection exercise. Steps taken to preserve the chain of custody ought to be recorded in detail to avoid any *ex post facto* accusations of evidence tampering.

29 The steps to be considered at the information gathering stage comprise the following:

(a) identifying the relevant information in question;

(b) identifying the *dramatis personae*;

(c) identifying the total number of target devices that need to be collected and reviewed; and

(d) the actual collection and imaging of devices.

1. Identifying the information in question

30 The information that needs to be gathered and analysed depends on, amongst other things:

(a) the type of information in question;

(b) the possible location(s) of the information;

(c) the owner or user of the information; and

(d) the legal and factual issues at hand.

31 For example, the information concerned may be stored in web-based email such as Gmail or Yahoo! Mail. Due to advances in email protocols and the extension of functions and facilities provided by web-based email service providers, it is now possible for copies of web-based email to be stored not just on web servers provided by the service provider but also on multiple email clients and mobile devices. In many instances, users also have the option of downloading or synchronising their web-based emails onto their computers so that this information is available in more than one location. Such web-based emails may exist:

(a) on the web-based platform of the service provider in question;

(b) in the local hard disk drive of the server(s) or computer(s) used by the target organisation or individual; and/or

(c) on a plurality of mobile devices that the target organisation or individual may utilise.

32 Separately, the information concerned may also be Microsoft Office or PDF documents contained in storage media or even source code written in text-based or proprietary formats.

33 When instructing a computer forensic expert on the type of information to be gathered, one should be as specific as possible concerning the factors set out above as this will likely affect the tools and methodology that the computer forensic expert will need to employ to collect the information, and eventually to effect analysis of the same. Usually, to convey this level of detail to the computer forensic expert, recourse must be had not just to the lawyers, but also to the organisation's IT department.

2. Identifying the *dramatis personae*

34 It is important to identify the *dramatis personae* of the matter as this may in turn affect the determination of which devices or storage media are relevant to the issues at hand, and in turn, affect the information gathering and collection process.

35 There is also the possibility of a potentially expansive knock-on effect in this identification phase: the storage media and mobile devices of the

individual concerned, as well as those belonging to the individual's associates, employees, friends or family members, may all come under forensic scrutiny, depending on the individual facts of each case.

36 For example, in cases concerning employees and the copying of confidential trade secrets or information, the employees may sometimes use online storage platforms such as Dropbox or Google Docs, amongst others, to store confidential and relevant information. In such cases, a relevant inquiry would also be the level of access that such individuals – both implicated and otherwise – have to trade secrets and other confidential information belonging to the organisation.

37 It is also often necessary to instruct computer forensic experts to query the computer or other hardware that the individual was using at the material time. Such a query may reveal information such as the recent internal network sites and websites visited by the individual, as well as any external storage media, if any, that was being used by the individual.

38 It may even be possible to infer, from an analysis of file access times on the computer and the external storage media, which files the individual had copied from the computer to the external storage media.

3. Identifying the total number of target devices that need to be collected and reviewed

39 The size of the operation and the number of target devices may affect the tools which a computer forensic expert might need to employ in the collection exercise. One should keep in mind that technology is progressing everyday and that new tools with the ability to increase the rate of data transfer and speed up the imaging process are released onto the market on a fairly regular basis. A large number of target devices may justify more expensive but more efficient tools to copy disk images or extract relevant data.

40 In certain cases, a large number of mobile devices involved may still have to be at the disposal of their respective users even while the investigation process is under way. It may then be necessary or convenient to image these mobile devices first, as opposed to computers or other storage media that may be imaged with less priority.

41 Conversely, there are also occasions where it is neither necessary nor possible to make full physical images of certain storage media. For relevant intents and purposes, an eight terabyte server might call for only the imaging of a specific twenty gigabyte share. This manner of intelligent forensic work saves time and effort all round, as well as clients a tidy sum of money. As has been emphasised earlier however, to obtain these optimal forensic results, communication between the lawyers, the organisation's IT department and the computer forensic expert is key.

42 It may also be convenient to request that, where possible, the computer forensic experts provide mobile tools and machinery that can be brought on-site to the target mobile device for imaging, rather than having the target mobile device sent to the computer forensic expert for imaging.

4. Imaging of devices

43 The imaging of the devices *per se* is largely an automated process, although it is necessary for the computer forensic experts to check in on the progress of the process where required.

44 The larger the size of the storage medium, device to be imaged or the image which needs to be created, the longer the imaging process takes. However, as has already been noted above, new data transfer technologies and improved hardware will eventually lead to faster imaging times across the board.

45 The usual practice is to create one master image which is always preserved in its original state, free from tampering. Working copies of this master image are then made and these copies may be analysed and interrogated. This is to ensure that in the event that it becomes necessary to produce more working copies of the images or to replace a corrupt working copy of an image, the master image is always available without having to resort to re-imaging, which can be very inconvenient particularly when the target device is in use or mission critical.

5. Analysis

46 In any matter, one would only be interested in files and documents which are relevant to the issues at hand. Naturally, not all files in the images may be relevant. It should be remembered that the image will also likely

contain various irrelevant files and documents such as system files needed for the operation of the software or hardware in the device from which the image was taken.

47 If the target device was a personal device such as a personal mobile phone or laptop, it is likely that the device will contain a large quantity of irrelevant information which may be also be personal and private.

48 In order to narrow down the category of relevant files, one might consider the following techniques:

(a) filtering off known operating system or application files, based on hash libraries, which are in all likelihood unlikely to form part of any contemporaneous evidence relevant to the matter;

(b) specifying a time period which would be most relevant to the issues at hand. Most computer forensic experts will be able to narrow the scope of files for review and analysis in accordance with the relevant time period, so that files created, accessed or modified during the relevant time period will be included in the scope for review and analysis, while all other files which do not fall within this time period are excluded. This can significantly reduce the number of files and correspondingly the amount of time needed for review and analysis; and

(c) employing keyword searches using keywords relevant to the matter to pick out documents germane to the issues at hand. Careful thought should be put into what keywords would be most appropriate as there is a risk that using too generic keywords will likely hit on a large number of false positives that will only increase the time required for document review and analysis.

49 A commonly litigated issue that often requires computer forensic analysis concerns employees who have resigned from one employer and are looking to join or set up a competing entity. In these situations, the dispute arises when the employer alleges that the employee has taken trade secrets or confidential information and is looking to profit from these in due course. In such cases, it may sometimes be useful to review website visits and network shares recently initiated by the employee on both the local network of the employer and on the internet. This may help to determine the employee's true actions and intentions with respect to the alleged trade secrets or confidential information.

50 Where external storage media such as compact discs, digital video discs, thumb drives or external hard disks are suspected to have been used to copy confidential files, it is also necessary to review the results of the query pertaining to the relevant target device to see if it is possible to determine or infer if any files or documents containing trade secrets or confidential information have been copied onto the external storage media, particularly where the employee has contemporaneously resigned. If so, this can lead to an inference that the employee intends to use the trade secrets or the confidential information for the benefit of a competitor and as such, would potentially be in breach of his duties as an employee.

IV. SEARCH AND SEIZURE ORDERS

51 Search and seizure orders are generally seen as extremely draconian remedies as they involve granting a litigant the power to invade the personal or private space of other parties on the grounds that evidence relevant to the matter at hand is at risk of being destroyed by the party subject to the search and seizure orders.

52 To obtain such an order, the litigant must satisfy the Court that:[2]

(a) the plaintiff has an extremely strong prima facie case;

(b) the damage suffered by the plaintiff would be very serious;

(c) there is a real possibility that the defendants will destroy relevant documents; and

(d) the effects of the search order are proportionate to the legitimate object of the order.

53 The locus classicus on search and seizure orders is the case of *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55 ("*Anton Pillar KG*"), which, given the decade in which it was decided, dealt with the inspection and the copying of only hard copy documents. However, it would appear that the same principles still apply today when considering whether a Court should grant a search and seizure order.

54 Given the nature of search and seizure orders and their objective in the preservation of evidence, applications for such orders are made on an *ex*

2 *Asian Corporate Services (SEA) Pte Ltd v Eastwest Management Ltd (Singapore Branch)* [2006] 1 SLR(R) 901 at [14].

parte basis so that the element of surprise is retained and the adverse party is not given any opportunity to destroy the evidence.

55 Subsequent to the execution of the search order, the affected party may then apply to set aside the search order and claim consequential damages.

1. The impact of the electronic age

56 The traditional execution of the search order typically involved the seizing of hard copy documents alleged to have been at risk of destruction by a dishonest defendant.

57 As in *Anton Piller KG*, the usual order made is to allow the plaintiff and/or his solicitors to enter the premises of the defendant to inspect and take copies of hard copy documents so as to preserve the same on the grounds that the relevant documents would be destroyed if the defendant caught wind of the action commenced against him.

58 With the ease of storing information and documents in soft copy formats and the convenience of access in the digital age, the manner in which search and seizure orders are framed will have to change.

59 While documentary evidence was traditionally recorded on hard copy paper, it was a relatively simple matter of taking a photocopy of the hard copy paper to be delivered up under the search and seizure order. However, where the evidence to be delivered up under a search order exists in electronic form, specific steps necessary for the preservation of the evidence in electronic form will have to be followed. These steps will usually be carried out by a computer forensic expert. In summary, these are as follows:

(a) identify the relevant computer devices on the premises;

(b) photograph the same *in situ*;

(c) perform a forensic preview to find evidence in the List of Items of the Order of Court;

(d) where evidence is found, confirm with the plaintiff's solicitors that data collection can proceed;

(e) once data collection is complete, a back-up of the images is made and both hard drives are sealed in tamper-proof evidence bags;

(f) documentary evidence, such as a chain of custody report, is completed on-site; and

(g) where evidence is not found, return computer device(s) to the defendant(s).

60 The methodology in the collection and preservation of electronic evidence takes into account some of the characteristics of electronic evidence, particularly electronic documents, which clearly distinguish it from hard copy documents. Specifically:

(a) electronic documents can exist in multiple types of storage media which must be stored correctly;

(b) electronic documents are easy to manipulate in that they can be copied, changed, deleted or transmitted easily;

(c) electronic documents are usually generated in large volumes;

(d) electronic documents usually contain metadata, that is, data about data. The Supreme Court Practice Direction No 3 of 2009 ("Supreme Court Practice Direction") defines metadata information as "the non-visible and not readily apparent information embedded in or associated with electronically stored documents and may include both application metadata, which is created by the application software used to create the electronic documents, and system metadata, which is created by the operating or storage system";[3]

(e) unlike physical paper which can be relatively easily destroyed, it is not as easy to destroy electronic documents. Electronic documents which have been deleted by the user can potentially still be recovered using forensic techniques; and

(f) electronic documents sometimes depend on external hardware and software in order to be properly parsed.

2. Jurisdictional issues

61 Electronic evidence can be stored on multiple types of storage media, including online storage media such as web-based email, online storage sites such as Dropbox or Box.net and even cloud drives or server storage.

3 Supreme Court Practice Directions No 3 of 2009 (2007 Ed), Part IVA, at para 43A(3).

62 Given this, it may be argued that where the physical server of such online storage media is outside of Singapore and therefore outside of the territorial jurisdiction of the Singapore courts, the Court would have no power to make an order for the delivery up of such documents and evidence.

63 However, the preferred view is that the Court's jurisdiction should not be so circumscribed in an age where information relevant to a matter will commonly be physically stored in a location outside of the Court's jurisdiction, but easily accessible to the defendant who would have submitted to or would likely be within the Court's jurisdiction.

64 In any event, the Supreme Court of Judicature Act (Cap 322, 2007 Rev Ed) ("SCJA") does not circumscribe the Court's power in this manner. Paragraph 5(b) of the First Schedule to the SCJA states that the Court has the power, before or after any proceedings are commenced, to provide for the "preservation of evidence by seizure, detention, inspection, photographing, the taking of samples, the conduct of experiments, or in any other manner". It is therefore clear that the Court does have the power to make an order for the preservation of evidence, regardless of its actual storage location.

65 In the context of Mareva injunctions, there is little doubt today that the Court has the power to grant an order for a Mareva injunction to prevent a defendant from dealing with his assets which are located both domestically and abroad. The standard forms for an order for a Mareva injunction contemplate the Court being able to grant a domestic or worldwide Mareva injunction *in personam* against the defendant in question where the defendant is within the Court's jurisdiction.

66 Accordingly, the issue of whether the Court has power to grant an order for the delivery up of electronic evidence located physically in other jurisdictions, but accessible to the respondent of the search order, should therefore be dealt with similarly. The Court would have the jurisdiction to order the delivery up and preservation of electronic evidence *in personam* against the defendant, wherever it may be located, as long as it remains accessible to the defendant.

67 If the defendant refuses to comply with the search order, then he would similarly be liable for contempt proceedings, just as he would be if he does not comply with the terms of a Mareva injunction issued against him.

68 One additional issue that arises is that, unlike hard copy paper, online storage media usually requires a user to provide a username and password before access is granted to the user's account on the relevant storage medium.

69 The standard form search order in the Supreme Court Practice Directions already contemplates that where the evidence resides on a computer, the defendant must immediately give the plaintiff's solicitors effective access to the computers, with all the necessary passwords, to enable them to be searched. Drawing an analogy with criminal procedure, section 40 of the Criminal Procedure Code 2010 ("CPC 2010") empowers the Public Prosecutor to authorise any police officer or authorised person to, *inter alia*,:

> … require any person whom he reasonably suspects to be in possession of any decryption information to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.[4]

70 It is an offence not to comply with the requirements of such police officer or authorised person.[5] Similarly, any person who is subject to a civil search order containing terms with similar effect may find himself facing committal proceedings if he fails to disclose passwords as required.

71 As such, the same ought to apply to any online storage medium, be it web-based email, social network accounts, online storage platforms or otherwise. There should be no additional hurdle to cross in this regard simply because the predominant medium for information has changed.

3. Privacy concerns

72 There is generally no right of privacy in Singapore. However, the issue of privacy does often arise in a situation where electronic evidence is seized because of the manner in which individuals tend to mix their personal documents together with documentary evidence that may be relevant to the matter.

73 It is very common for individuals to use their electronic devices, whether personal or employer-sanctioned for both personal and office use.

4 Section 40(2)(c), CPC 2010.

5 Section 40(3), CPC 2010.

This results in the sometimes inextricable mingling of both personal information and relevant documentary evidence in the same electronic device.

74 For this reason, the Court's practice appears to be that, even where the Court does grant an application for a search and seizure order involving the imaging of electronic devices, caution is also exercised in ordering that the images not be reviewed until further order of Court.

75 Subsequent to the execution of a search order, the party that wants to review the images normally proposes a review protocol, which may be agreed upon by the parties or ordered by the Court upon the application of the reviewing party. The protocol takes into consideration necessary measures to safeguard any personal, private and irrelevant information on the images, thereby preventing trawling. Ideally, this protocol also incorporates safeguards that prevent any privileged information on the images from being disclosed.

76 Parties will likely rely on the electronic discovery provisions under Part IVA of the Supreme Court Practice Directions with a view to agreeing on the terms of the review protocol. Any application for the review of any seized images and documents should also be made with these provisions in mind, given that these provisions give a good indication of a process and procedure of review that the Court would approve of.

77 As the standard form search order in the Supreme Court Practice Directions does not address any of the privacy concerns of seizing images of electronic devices containing personal (and irrelevant) data mixed with relevant electronic documents and data, amendments may have to be made to the existing standard form search order to provide that the party seizing the images may not review the images until a review protocol has been agreed between parties or until further order of Court.

78 Alternative approaches are also being explored at present for the purposes of saving time and costs during the discovery phase. The *ab initio* joint inspection of documents, for example, is becoming increasingly common, streamlining the discovery process and doing away with the need for any subsequent application to the Court for review.

4. Conduct of computer forensic experts

79 When enforcing a search order, a computer forensic expert must always remember that his primary duty is to the Court. His role is to assist with identifying computer devices within the premises, identifying listed items on said computer devices and collecting and preserving these items as evidence in a forensically sound manner.

80 Where technical obstacles are encountered, these should be highlighted to the client's legal counsel for discussion and for determination of the next course of action. The computer forensic expert should always keep in mind that the purpose of the search order is to search for the listed items in the order of Court and to collect and preserve these. The search order does not grant the computer forensic expert the right to make demands or to interrogate parties.[6] Importantly, at all times the computer forensic expert should conduct himself with courtesy, politeness, fairness and transparency. This will create goodwill and respect from opposing counsel, supervising solicitor(s) and the other parties involved in the matter.

V. DRAFTING CONSIDERATIONS FOR EXPERT REPORTS

81 After the bulk of the forensic data has been gathered and analysed – a process that may span months or even years – lawyers and experts alike would have acquired a firm understanding of the material legal issues and the forensic evidence that serve to provide clarity on those legal issues.

82 The next challenge is the translation of this understanding into an expert report or affidavit that may be easily received and digested by the Court. This is not an easy task, because one effectively has to convey a large amount of information, often technical in nature, to an audience that does not have the luxury of time to absorb every single piece of information yielded by the electronic forensic exercise.

83 It must also be remembered that the judge or registrar hearing the matter may not be technologically savvy. In the course of analysing the forensic data, parties are frequently exposed to many esoteric concepts and terms-of-art specific to the nature of the forensic data. Over time, this may cause parties to develop a certain strain of tunnel-vision: litigants and

6 *Fong Wai Lyn Carolyn v Airtrust (Singapore) Pte Ltd and another* [2011] 3 SLR 980 at [96]–[97].

lawyers become so focused on the specifics of a particular matter that they forget that their audience may be dealing with the subject-matter for the first time.

84 In order to overcome these challenges in drafting a good expert report, the principal guiding considerations are:

(a) using a drafting structure which the Court is familiar with;

(b) "translating" technical concepts or terms; and

(c) utilising non-traditional forms of presentation.

1. Drafting structure with which the Court is familiar

85 By applying common drafting conventions for legal submissions to the expert report, one gains a vehicle through which even complicated concepts and extensive amounts of forensic evidence can be effectively communicated to the Court. Typically, a drafting structure that the Court is familiar with will comprise, in order from start to end:

(a) a clearly-stated conclusion or goal of the expert report;

(b) a brief framework of contents;

(c) signposting the main body of content with topic sentences / headings;

(d) any weaknesses in the forensic evidence that need to be addressed;

(e) a strong restatement of the conclusion.

86 A clear conclusion at the beginning of the expert report acts as a strong anchor to ground the reader's understanding of the report, mentally preparing the reader with an end-goal. This also helps to provide context for the rest of the report, as the reader will more easily comprehend the relevance of the text once he is able to identify a connection between the information he is reviewing and the conclusion that he is intended to reach.

87 One should also consider investing effort to include a brief framework of contents to demarcate the various sections in the expert report. As a general rule of thumb, this framework should be included once there are more than three distinct and separate sections to the expert report. This is especially useful in situations where the Court has had previous experience

with the subject matter, and the Court wants to proceed directly to the sections dealing with new information that is germane to the issues at stake. The distinct chapters also help the drafting party avoid the common mistake of intertwining separate points together, or drafting as if they were literally transcribing a "stream of consciousness".

88 The topic sentences act as mini-conclusions to each main section or paragraph in the report. As discussed above, when the reader is provided with a visible end-goal, he will be better able to comprehend the information presented to him.

89 One should also not shy away from identifying obvious weaknesses in the forensic data and to deal with them in the expert report itself, clients' instructions notwithstanding. Quite apart from the expert's overriding duty to the Court, dealing with these weaknesses actually serves to strengthen the expert report, because the drafting party retains the initiative to address the weaknesses on his terms. In contrast, the credibility of the expert report would be undermined if these weaknesses are not addressed and are instead highlighted for the first time in the adverse party's expert report.

90 The expert report should end with a strong restatement of the conclusions drawn from the available forensic evidence. One should take full advantage of this opportunity to remind the audience of the strength of the forensic evidence uncovered as well as the impact that this evidence has on the determination of the legal issues identified.

2. "Translating" technical concepts or terms

91 When faced with the task of explaining new concepts or terms of art in the expert report, the common approach is to include a paragraph defining the said concept or term of art. While this is certainly a necessary step, this is by no means sufficient in and of itself. One should keep in mind the following techniques to ensure that technical concepts or terms are effectively communicated across to an audience:

(a) drawing a relationship between the new concept or term to everyday concepts that a layman audience would identify with;

(b) avoiding the assumption that the audience has any knowledge of the subject matter; and

(c) building up a base of knowledge for the audience.

92 An example would serve to illustrate the above. In a scenario where there is a claim that an ex-employee of a company had taken confidential information from the company's network of computers without authorisation and subsequently retained the confidential information on personal cloud storage services, one of the challenges that the drafter of the expert report would face would be the explanation of what "cloud storage services" are, including concepts such as web-based email and online storage services such as Dropbox. It would be useful, for example, if "cloud storage services" could be likened to common and popularly used email platforms such as Gmail or Yahoo Mail to illustrate the point that a computer user is accessing data which is not stored on his own computer, but on computer servers located elsewhere.

93 One should also take care to avoid assuming that the audience has any knowledge of the subject matter. In the above example, while the term "cloud storage services" may seem to be a technologically advanced concept that requires a thorough explanation, one cannot assume that the audience is fully aware of the concept of "network of computers" in the first place, or for that matter how the ex-employee had gained access to the said network without authorisation. *A fortiori* the issue of how the confidential information was taken from that network to begin with.

94 It is through this process of meticulously explaining various related concepts that one builds up a base of knowledge for the audience, so that they have sufficient context and understanding to appreciate the significance of the forensic data uncovered.

95 An additional benefit of doing this is that once the knowledge base has been firmly established, related concepts can be introduced relatively easily. For example, in the above scenario, after the audience understands that the confidential information which the ex-employee has taken is not stored on his own computer but on cloud storage services, one could explain why it is important to prevent the ex-employee from disclosing his cloud storage passwords to the world at large, lest other parties are able to gain similar access to the confidential information stored on these services.

3. Utilising non-traditional forms of presentation

96 One should also consider utilising non-traditional forms of presentation to supplement the expert report. For example, in certain

scenarios the import of the uncovered forensic data can be explained easily through the use of PowerPoint presentations, because PowerPoint presentations easily allow for graphic diagrams or representations that may more efficiently illustrate technical points made in the expert report. More importantly, however, the use of presentations also permits the conveyance of proprietary data to the Court in a form as close to its native manifestation as possible, without compromising on the quality or accuracy of the data.

VI. DEALING WITH EXHIBITS TO THE EXPERT REPORT

97 Another common dilemma that arises in the course of drafting an expert report: how much of the uncovered forensic data should be included as exhibits?

98 There is a real tension between the intuitive inclination to include as much of the forensic data as possible to demonstrate the weight of evidence, and the practical reality that the audience reading the expert report is more likely to gloss over the forensic data if it is too voluminous and technical.

99 In resolving this tension, the following considerations are key:

(a) the amount of forensic data needed to establish a certain claim;

(b) the possibility of presenting the forensic data in such a manner as to avoid confusion of the audience; and

(c) the usefulness of the forensic data in helping to establish a timeline of events.

100 One way around this problem might be the inclusion of forensic data directly in the text of the expert report, so that the audience is able to easily follow the development of events. For example, if the forensic data includes email correspondence complete with times and dates, including that email correspondence in the text of the expert report will greatly enhance the audience's understanding of the development of events as they had unfolded. Generally, if the forensic data is crucial in establishing a timeline of events, that forensic data should be included as an exhibit to the expert report.

101 One should also refrain from including too much forensic data in the expert's report to avoid a situation where the audience is inundated with similar pieces of forensic data, particularly where the forensic data exists in

the form of file fragments with technical lines of code interspersed between legible and relevant text. It should be kept in mind that a balance must be struck between including the necessary raw technical evidence in order to establish one's case and distracting the Court from the key issues for which the technical evidence is being adduced in the first place. As a matter of good practice, the expert's report should repeat the same or similar evidence in order to properly focus the Court's attention on the germane issues.

102 For example, if a single email is able to shed light on a material issue, there will not be a need to exhibit all the other email correspondence which incidentally contain that first email, whether as an attachment or otherwise.

103 Similarly, if the issue was whether a person had ever accessed a certain computer file, it might be preferable to exhibit only a few computer log files reflecting the access, instead of exhibiting every single computer log file reflecting the same. If one were inclined to include all the available forensic data simply to demonstrate the weight of the evidence gathered, one can instead consider exhibiting a few material pieces of that forensic data and listing all the other instances of forensic data supporting that particular claim.

104 Another important consideration is the appropriate methodology for exhibiting forensic data recovered, in order to minimise confusion on the part of the audience. For example, if the forensic data includes thousands of mobile text messages in binary or machine-code format that is not designed for easy reading, it would be prudent to format the text messages for readability and to leave out irrelevant text messages so that the audience can focus on the key text messages. However, care should also be taken to guard against accusations that documentary evidence is taken out of context.

105 Similarly, if recovered text documents are interspersed with computer language, the drafter of the report might want to consider stripping away the computer language and preserving only the readable text of the documents, highlighting the relevant portions of the text where necessary. Of course, it should always be emphasised to the Court that such measures are undertaken to improve the presentation of the forensic data.

G. CONCLUSION

106 Inasmuch as electronic devices are part of our everyday lives in this day and age, suspicion of non-traditional forms of evidence remains rife in

society. This tendency appears to manifest itself equally in the various stakeholders of our justice system, from judges, lawyers, lay witnesses to even clients themselves. At the back of our collective mind, steeped in paradigms forged in the furnace of yesteryear, remains the doubt that each and every piece of digital evidence has been somehow "hacked" or "tampered" with. At the same time, however, this selfsame mind accepts, without kerfuffle, the veracity of any manner of physical evidence. The idea of fraud or forgery is present, but always only in a remote capacity.

107 The only way around this prejudice is through it; and the only way to dispel preconceived notions about computer forensic evidence, therefore, is to capitalize on the best practices regarding their presentation as recommended in this chapter. The gulf between technical proficiency and perceived credibility is a sizeable one, and in order to properly bridge this gulf, it may be said that (to borrow from, aptly, a server-software metaphor) what takes place at the front-end is as important, if not more important, than what goes on at the back-end.

108 As these best practices take root as the minimum norms to be expected in court, so too might the idea of computer forensic evidence as normal, ordinary evidence, to be treated no differently from traditional forms of documentary and physical evidence.

THE USE AND IMPACT OF SOCIAL MEDIA ON CIVIL LITIGATION

ANG Ching Pin
LLB (National University of Singapore), LLM (Harvard University)

LIM Seng Siew
LLB (National University of Singapore)

TAN Sze Yao
BA Law (Cantab), LLM (Columbia University)

YEONG Zee Kin*
LLB (National University of Singapore), LLM (Computer & Communications Law) (Lond)

I. INTRODUCTION

1 With the increasingly widespread use and reach of social media in Singapore and around the world, the medium is expected to maintain, and perhaps expand, its game-changing role in civil society for the foreseeable future. Singapore's 2011 General Elections, the United States Presidential elections of 2008 and the Arab Spring beginning from 2010 are instructive examples of the realised impact of social media in the socio-political arena.

2 Social media has also led to paradigm shifts in the legal sphere. In the United Kingdom, a district judge allowed a reporter to tweet in court during the hearing of Julian Assange's extradition; details revealing the identity of Welsh footballer Ryan Giggs, who had obtained an anonymised injunction from the English courts concerning his alleged affair with Imogen Thomas, were posted on Twitter and reported by international press sources; court papers were served on defaulting mortgagors through Facebook accounts in Australia; and in the United

---

* Some of the ideas in this article sprung from the discussions of the panel "The Use and Impact of Social Media on Civil Litigation" chaired by Lim Seng Siew, with members Thio Shen Yi, SC, Wong Siew Hong, Rama Tiwari and Assistant Professor Eliza Mik. This article also re-uses material from the Supreme Court's "Report on Contributions and Final Findings: Public Consultation on the Use and Impact of Social Media in Civil Litigation", which was presented at the conference.

States divorce papers were ordered to be served by email, "Facebook, Myspace or any other social networking site." Indeed, social media has wrought so much havoc in our existing legal frameworks that in October 2011, popular motor journalist Jeremy Clarkson voluntarily lifted a privacy injunction in the English High Court case of *AMM v HXW*,[1] an injunction which had previously prevented the British press from reporting claims by his former wife that they had an affair after he remarried. Clarkson was reported as saying: "Injunctions don't work. You take out an injunction against somebody or some organisation and immediately news of that injunction and the people involved and the story behind the injunction is in a legal-free world on Twitter and the Internet. It's pointless."

3 Pre-empting the concerns of Clarkson more than a year prior, the Supreme Court of Singapore in August 2010 circulated a consultation paper seeking feedback on the use and impact of social media on litigation. Key findings and recommendations arising from the consultation paper were presented at the panel discussion during the e-Litigation Conference 2011.

II. WHAT IS SOCIAL MEDIA?

4 According to Wikipedia, "[t]he term 'social media' refers to the use of web-based and mobile technologies to turn communication into an interactive dialogue. … Social media are media for social interaction, as a superset beyond social communication. Enabled by ubiquitously accessible and scalable communication techniques, social media substantially change the way of communication between organizations, communities, as well as individuals."[2]

5 In contrast to this organic conception, Andreas Kaplan and Michael Haenlein prefer a more technical definition of social media, seeing it as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."[3]

1 [2010] EWHC 2457 (QB).

2 See <http://en.wikipedia.org/wiki/Social_media>.

3 Andreas M Kaplan & Michael Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," (2010) 53(1) Business Horizons at pp 59–68.

6 Combining the above two definitions into lay-terms, "social media" would appear to refer to technologies that allow for the interactive creation and exchange of user-generated content. This interpretation would accordingly allow for a variety of online interactive communities to fall under the social media rubric, ranging from traditional text and picture platforms such as Facebook and Twitter to the literal virtual worlds in "World of Warcraft" or "Second Life".

III. SERVING COURT PROCESSES THROUGH SOCIAL MEDIA

1. Service within Singapore

7 In Singapore, social media may already be used for service of court documents. Under the Rules of Court, three modes of service are contemplated: personal, substituted and ordinary service. We will consider the potential for the use of social media for each mode of service in turn.

(a) Substituted service

8 Substituted service of court documents by social media has already been allowed in other jurisdictions. In the unprecedented case of *MKM Capital v Corbo & Poyser*,[4] the Supreme Court of the Australian Capital Territory allowed the plaintiff to effect substituted service of a default judgment on the defendants using Facebook. In *Knott v Sutherland*,[5] an Alberta court allowed a plaintiff to give notice of its action via Facebook. The New Zealand High Court, in an unreported decision, also permitted substituted service on a defendant using Facebook[6]. In the United Kingdom, the High Court allowed substituted service of an injunction via Twitter.[7]

4 No. SC 608 of 2008. The decision appears to have been made in December 2008 but is unreported.

5 Unreported decision, see <http://wiselaw.blogspot.com/2009/09/alberta-court-allows-substituted.html>.

6 See <http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=10561970>.

7 See <http://www.guardian.co.uk/technology/2009/oct/01/twitter-injunction>.

9 Given that other jurisdictions have used social media effectively for substituted service of documents, there is no reason why the Singapore courts should divorce themselves from this practice. This is particularly so given that our existing laws permit such a mode of substituted service. Moreover, it may be said that it is important for the practice of law to leverage on the latest developments in information technology as well as adopt the best practices of overseas jurisdictions where appropriate. Of course, the courts can and should prevent any blatant abuse by parties (*eg*, posting the notice of proceedings on a public Facebook wall rather than using the personal message application, insufficient proof furnished to show that the relevant account holder is the defendant in the legal proceedings etc.) when using social media to serve court documents.

10 It was with this purpose in mind that amendments were made to Order 62 of the Rules of Court[8] to signal that "the use of electronic means (including electronic mail or Internet transmission)" may be directed by the court as one of the modes of effecting substituted service.[9] This form of words is sufficiently wide that it can cover the range of electronic transmission from electronic mail to posting on discussion forums or social media pages as discussed above.

(b) Personal service

11 Personal service under the Rules of Court entails service of documents by a physical act of delivery to the defendant personally.[10] Apart from physical delivery, case law also requires that the defendant must be informed that the document which is handed over to him is an originating process: in *Banque Russe v Clark*,[11] it was held that merely handing the defendant a copy of the writ in an envelope without informing him about the writ was insufficient. From the foregoing, it is possible to extract the following legal requirements for effective personal service:

> (a) that the person effecting service and the defendant are both present at the same "location"; and

8 Rules of Court (Amendment No 4) Rules 2011, with effect from 30 September 2011.

9 Order 62, rule 5(4).

10 See Order 62, rules 1–4.

11 [1894] WN 203.

(b) that the defendant is informed of the nature of the document which has been given to him.

12 It may be possible to effect personal service via social media if the appropriate social media tool is employed. This requires a deeper understanding of the different types of social media tools which are available. For the purposes of our discussion, the primary features which fall for consideration are:

(a) Non-instantaneous means of communications which may be of a private or public nature. These function as the Web 2.0 equivalent of the electronic mail and discussion forums which we are probably more familiar with. Hence, the relevant features, using Facebook as an example, would be to send a message to a friend (similar to sending an e-mail); or to write something on the "wall" of a friend on Facebook (similar to a public discussion forum).

(b) Instantaneous means of communications which are typically private in nature. These function as the Web 2.0 equivalent of private chat rooms. Hence, the use of instant messaging software (for example Google Talk, MSN Messenger, ICQ, Yahoo Messenger, etc.) whereby one may chat with a friend. These features are also available in social media websites (*eg*, Facebook chat).

13 It is posited that it may be possible to effect *personal* service of documents using any of the instantaneous communications means described in (b) above. In an online chat, the interlocutors have to be present online at the same time, which would arguably satisfy the requirement that the person effecting service and the defendant are both present at the same "location". Many of the instant messaging software also allow a party to send an electronic document over to the other party. Should the sending party identify the nature of the document during the course of the chat with the receiving party, he has the option of accepting or rejecting it. In the event that the electronic document is rejected, it will not usually be transmitted. Accordingly, it appears possible for personal service to be properly effected in a situation where (a) the defendant and the party effecting service are *online at the same time*; (b) the party effecting service identifies the nature of the electronic document *before* he sends it across to the defendant and (c) the defendant *accepts* the electronic document thereafter. Whether this interpretation satisfies the legal requirements for

personal service remains, however, an open question until the issue is referred to the courts for their consideration.

14 Additionally, if there is a pre-existing contractual relationship between the parties and there is a clause in the agreement which is broad enough to include social media as an agreed means of personal service, it may also be possible to effect personal service in that manner. The agreement between parties has to be broad enough to encompass the use of social media (whether through instantaneous means or even non-instantaneous means), in order for such service to qualify as personal service under Order 62 rule 3(2):

> Personal service of a document may also be effected in such other manner as may be agreed between the party serving and the party to be served.

15 However, from a policy perspective, the following considerations have to be borne in mind if we are to consider using social media for personal service in Singapore:

(a) potential prejudice to defendants who do not receive actual notice of the proceedings;

(b) risk of trivialising a fundamental step of proceedings, *ie*, the commencement of proceedings;

(c) potentially opening the floodgates to a slew of setting aside applications based on irregular service;

(d) the difficulty of justifying personal service by social media where the defendant is physically located within Singapore and capable of being served physically, since there is no good reason why the party effecting service should be able to commence proceedings in what is still considered to be a casual manner when the defendant can be personally served. This difficulty is compounded by the fact that such a mode of personal service would not be subject to scrutiny by the court beforehand whereas the same manner of service would require leave of court if it were to be effected as a form of substituted service; and

(e) the uncertainty of whether parties are physically within or out of jurisdiction.

(c) Ordinary service

16 It may be possible to use social media for ordinary service of documents that are not required to be served personally under the Rules of Court, as Order 62 rule 6(1)(d) prescribes that documents may be served "in such other manner as may be agreed" between the parties and rule 6(1)(e) states that documents may be served "in such other manner as the Court may direct".

17 The premise for ordinary service under Order 62 rule 6(1)(d) is agreement, which means that the terms of agreement are paramount. It is not uncommon, within the context of a contractual relationship (*eg*, bank and customer), for the terms and conditions to deal with the issues of giving notice and service of process. Thus, ordinary service of documents via social media would be permitted where an appropriately drafted clause in the contract is broad enough to include social media as an *agreed means* of ordinary service.

18 Similarly, under Order 62 rule 6(1)(e), where the court is convinced that social media is a suitable means for effecting ordinary service, it may so order. In making such an order, it would be prudent that the exact social media or other electronic means are properly identified. For example, an order should state that ordinary service will be properly effected by emailing a copy of the document to a particular email address, or by posting on the wall of a specified Facebook account which has been established to be accessible by the party to be served.

19 However, short of agreement between the parties and sanction by the court, it seems clear that the ambit of ordinary service does not otherwise extend to the use of social media as the other prescribed methods of ordinary service under Order 62 are restricted to commonly accepted modes of service like post and fax. Practically speaking, short of a suitably drafted clause in an agreement signed between parties before the dispute arises, it is unlikely for ordinary service to be effected through social media. It is highly implausible that the party to be served will agree to any form of service *after the dispute has arisen* since such parties are usually uncontactable or uncooperative; otherwise, ordinary service would usually be more conveniently carried out via one of the other specified methods under Order 62 rule 6(1).

20 Order 62 rule 6 was amended to clarify that one of the manners of ordinary service that the court may direct under Order 62 rule 6(1)(e) includes the use of electronic means:

> (4) For the purposes of paragraph (1)(e), the manner in which the Court may direct service of any document to be effected includes the use of such electronic means (including electronic mail or Internet transmission) as the Court may specify.

21 This is the twin of a similar addition to clarify that electronic means are an acceptable mode of substituted service. Although there has not been any application thus far for ordinary service by social media, the validity of such orders are now beyond doubt. This provides litigants with an additional option for ordinary service. The use of electronic mail is now pervasive and almost second nature. To a large extent, it has become the preferred mode of communication. It is now possible for a litigant to obtain an order – during the pre-trial conference or the hearing of a summons for directions – that ordinary service on his adversary be effected by electronic means, *eg*, electronic mail, through his Facebook or LinkedIn messaging function, etc. One can easily imagine the use of this option of ordinary service by electronic means as an additional mode of ordinary service on an adversary that has a habit of not receiving documents that are served on him.

2. Service out of Singapore

22 A second way in which social media may be used in the service of documents is the *service of originating processes on foreign defendants*. In a situation where the plaintiff knows for certain that the other party cannot be physically served or served in the traditional manners prescribed by the laws of the foreign country but is known to be active on social media, it will clearly be useful to consider the feasibility of personal service via such media. While substituted service of the originating process out of Singapore may be an option in such situations, Chief Justice Chan Sek Keong observed in his Opening of the Legal Year 2010 speech that parties should not be saddled with wasted time and costs in going through what they know will be futile attempts at (traditional) personal service. Thus, social media may be an effective means of effecting service of originating processes on foreign defendants.

23 The engagement of social media in this way, however, brings to the fore the twin issues of the court's potential long arm jurisdiction as well as potential breaches of foreign law and international comity. Under Order 11 rule 3(3), an originating process which is served out of Singapore does not have to be served personally on the person to be served so long as it is served on him according to the laws of the foreign country where service is effected. While service by social media is not expressly precluded under this rule, research of the position in other commonwealth jurisdictions has shown that service by social media is not a generally permitted form of service although it has been allowed for substituted service. Thus, any attempt to effect service by social media on a foreign party within the framework of Order 11 must comply with the laws or public policy of the foreign country. To serve an overseas defendant using social media outside the framework of Order 11 may be perceived as an exercise of exorbitant jurisdiction by the issuing court.

24 Further, as Order 11 rule 3(2) provides that no order of court can be taken to authorise the doing of anything contrary to the law of the country where service is to be effected, it follows that any service of an originating process out of Singapore by social media will not be allowed by the Singapore courts to stand if service is against the laws or public policy of the jurisdiction where the defendant is located. Even if the defendant does not apply to set aside service of the originating process or to set aside any judgment obtained by the applicant in Singapore, it seems almost certain that any attempt by the applicant to enforce in the foreign country a judgment obtained in contravention of that country's law will be extremely problematic.

25 Nonetheless, the need to act according to international norms in the interests of comity of nations has to be balanced against the need to provide legal protection to our citizens and residents from errant foreign defendants, even if the latter involves a policy which may not sit well abroad. The observations of the Chief Justice underscore the importance that the legal procedural system must be developed to better serve the needs of our citizens and residents.

IV. SOCIAL MEDIA IN THE COURTROOM

> "[O]ne of the essential qualities of a Court of Justice [is] that its proceedings should be in public, and that all parties who may be desirous of hearing what

> is going on, if there be room in the place for that purpose, - provided they do not interrupt the proceedings and provided there is no specific reason why they should be removed – have the right to be present for the purpose of hearing what is going on."[12]

26 The rule of law dictates that justice should be done in public, and that what goes on in court ought to be open to public scrutiny. However, as Bayley J points out in the above passage, there is a triumvirate of limitations to this principle: (a) whether there is sufficient physical room for the public; (b) whether the public is interrupting or affecting the conduct of proceedings; and (c) whether there are any specific reasons that the public should be removed.

27 Lord Neuberger of Abbotsbury, in a speech entitled "Open Justice Unbound?" delivered at the Judicial Studies Board Annual Lecture 2011,[13] has suggested that because of the combination of limited space in modern courtrooms and limited interest amongst the public, "the justice system may need to adapt in order to ensure that it truly remains open to the public."

28 Among Lord Neuberger's suggestions is an encouragement to permit "tweeting" in the courtroom subject, of course, to proper safeguards. "Why force a journalist or a member of the public to rush out of court in order to telephone or text the contents of his notes written in court, when he can tweet as unobtrusively as he can write?", he asks rhetorically.

29 Lord Neuberger's exhortations have met with mixed responses around the globe. A summary of the positions of four major jurisdictions in relation to social media in the courtroom is presented below, beginning first with Lord Neuberger's own jurisdiction.

1. The United Kingdom

30 On 14 December 2011, the Lord Chief Justice of England and Wales handed down a new practice guidance entitled "The Use of Live Text-Based Forms of Communication (including Twitter) from Court for the Purposes

12 Bayley J in *Daubney v Cooper* (1829) 109 E.R. 438; 10 B&C 237 at p 240.

13 In his speech "Open Justice Unbound?" delivered at the Judicial Studies Board Annual Lecture 2011 on 16 March 2011.

of Fair and Accurate Reporting".[14] The guidance directed that "tweeting", texting or e-mailing from courts would be automatically permitted for the media and legal commentators. However, according to the guidance, members of the public would still have to apply for permission to communicate "live" from the courts. Additionally, judges throughout England and Wales retain a discretion to prohibit live, text-based communications from court "at any time" if they appear to be interfering with the administration of justice.

31 The promulgation of this practice guidance is consistent with the Lord Chief Justice's previous "Interim Practice Guidance" to the courts, litigants, lawyers and the media issued on 20 December 2010, where he stated that "[t]here is no statutory prohibition on the use of live text-based communications in open court. But before such use is permitted, the court must be satisfied that its use does not pose a danger of interference to the proper administration of justice in the individual case. Subject to this consideration, the use of an unobtrusive, handheld, virtually silent piece of modern equipment for the purposes of simultaneous reporting of proceedings to the outside world as they unfold in court is generally unlikely to interfere with the proper administration of justice."[15]

32 The new practice guidance is also consistent with the consultation report on the use of smart phones and live, text-based communications in court released by the office of the Lord Chief Justice on 7 February 2011. The consultation report was drafted after taking into account the views of the legal profession, the government, prosecutors and journalists on what the permanent rules about "tweeting" in court ought to be. In the report, it was stated that in some instances only members of the press – not the public – attending court may be permitted to utilise Twitter and other forms of live, text-based communication. "The combination of instant reporting without the self-restraint presumed to be exercised by accredited members of the media might lead to a greater likelihood of prejudicial reporting," the report said. Separately, the report also put forward the

14 See generally Lord Judge, *Practice Guidance: The Use of Live Text-Based Forms of Communication (including Twitter) from Court for the Purposes of Fair and Accurate Reporting* (14 December 2011).

15 See Lord Judge, *Interim Practice Guidance: The Use of Live Text-Based Forms of Communication (including Twitter) from Court for the Purposes of Fair and Accurate Reporting* (20 December 2010) at paras 10–11.

suggestion that courts could restrict Twitter use to accredited reporters, or consider applications from the public on a purely case-by-case basis.[16]

33 In the new practice guidance, Lord Judge noted that while the "most obvious purpose of permitting the use of live-text-based communications would be to enable the media to produce fair and accurate reports of the proceedings", his primary reservations against such use have always been in criminal trials, where "the danger to the administration of justice is likely to be at its most acute … [for example,] where witnesses who are out of court may be informed of what has already happened in court and so coached or briefed before they then give evidence". Lord Judge also noted that the use of real-time social media would possibly also have deleterious effects in civil or family proceedings, where "simultaneous reporting from the courtroom may create pressure on witnesses, distracting or worrying them".

34 By way of background, it should also be noted that on 2 February 2011, the United Kingdom Supreme Court released a policy statement concerning "The Use of Live Text-Based Communications from Court".[17] In the statement, it was made clear that "any member of a legal team or member of the public is free to use text-based communications from [the Supreme C]ourt, providing … [they] are silent and … there is no disruption to proceedings in court".

35 The Supreme Court did, however, prescribe several exceptions to the rule: in particular, where reporting restrictions have been put in place by the court, or in cases requiring anonymity. In these situations, the use of live text-based communications would still amount to contempt of court. The policy statement also stressed that "the cases which come before the [Supreme Court] do not involve interaction with witnesses or jurors; and it is rare for evidence to be adduced which may then be heard in other courts". Indeed, this qualification was subsequently echoed by Supreme Court President Lord Phillips of Worth Matravers, who made clear the distinction between trials and appeals: "We are fortunate that, by the time a case reaches the Supreme Court there is very seldom any reason for any

16 "License to Tweet? UK Judges Consider banning Public From Sending Live Updates Inside Court", Associated Press (8 February 2011).

17 The Supreme Court of the United Kingdom, *Policy on the Use of Live Text-Based Communications from Court* (2 February 2011).

degree of confidentiality, so that questions about what should and should not be shared with those outside the courtroom do not usually arise."[18]

36 This cautious permissibility has been emulated in Scotland as well, where Lord Justice General Arthur Hamilton, the most senior criminal judge in the land, recently permitted the media to send "live text-based communications" for the first time in a Scottish court, after applications by several media organisations covering a perjury case. It was significant that the "tweeted" proceedings comprised only the sentencing hearing, and not a substantive trial *per se*. Elizabeth Cutting, head of judicial communications for the Judicial Office of Scotland, was cautiously optimistic about the situation: "[The Twitter experiment in this perjury case] has gone very well as far as I'm concerned, but anything else will have to be done on a case by case basis. There's a huge amount of judicial discretion in this: it's very much down to judges what they do or don't allow in court."[19]

2. The United States

37 The Supreme Court of the United States has not yet considered the implications of Twitter or Facebook use in courtrooms, but the lower courts are divided about the issue. A Connecticut state court judge allowed reporters to tweet updates from the high-profile murder trial of Steven J. Hayes, a decision that defence lawyers are trying to argue prejudiced the proceedings.[20] In 2009, a federal judge allowed a reporter to tweet from a gang trial in Wichita, Kansas.[21] However, also in 2009, District Judge Clay Land in Georgia refused to let a reporter tweet from his courtroom, saying that the tweets would run afoul of federal rules of criminal procedure prohibiting "broadcasting" from criminal court.[22]

18 Kelly Fiveash, "UK Supreme Court Greenlights Twitter Usage", *The Register* (3 February 2011).

19 Severin Carrell, "Tweeting in Court Spreads to Scotland", *The Guardian* (28 January 2011).

20 William Glaberson, "A Grisly Murder Trial, in 140-Character Bits", *The New York Times* (15 October 2010).

21 Roxana Hegeman, "Twitter Boosts Public Access to Federal Courtrooms", Associated Press (6 March 2009).

22 Declan McCullagh, "Judge Bans Twitter From Court", CBS News (9 November 2009).

38 More recently, in August 2010, Circuit Judge Diane Druzinski removed a juror from a trial in suburban Detroit after the young woman, Hadley Jons, wrote on Facebook that it was "gonna be fun to tell the defendant they're guilty".[23] A recent investigation by the Reuters news agency in the United States revealed that at least 90 verdicts in the last decade have been challenged because of alleged Internet infractions by jurors, and that more than half occurred in the last two years.[24]

39 Courts nationally are sharply split on whether to allow mobile phones (and other electronic devices that facilitate tweeting and Facebook access) into courtrooms. Around the country, some judges have banned the use of Twitter as prohibited "broadcasting" that could get information to jurors and witnesses that they are not supposed to have.[25] However, given how the Supreme Court itself has long held that the First Amendment generally requires trials to be open to the public (and how Justice Stephen Breyer himself has a Twitter account), there is also an argument that the eventual position taken by the United States will be a progressive one. In this connection the writings of Chief Justice Warren Burger in 1980 appear to be apposite: "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing". Today, methods of observation may well have changed, but Chief Justice Burger's sentiment remains as germane as ever.

3. Canada

40 The problem of juror indiscretion, while not new in Canada, is causing great concern because the threat to a fair trial has grown exponentially with the social phenomenon of jurors sharing information online, rather than just confiding confidential details in the company of family and friends. An added element for Canadian jurors is that it is against Canadian law for them to discuss what happens in the jury room – unlike in the United States, where jurors can talk freely about how they arrived at a verdict.

23 Ed White, "Juror Hadley Jons Punished for Posting Verdict on Facebook", *The Huffington Post* (2 September 2010).

24 Janice Tibbetts, "A jury of your TWITS – Social media wreaks havoc in the courtroom", *Winnipeg Free Press* (9 January 2011).

25 William Glaberson, "A Grisly Murder Trial, in 140-Character Bits", *The New York Times* (15 October 2010). See also above at paragraph 5.

41 The explosion of real-time social media has certainly exacerbated the problem for Canada. At present, there are no known cases in Canada of a juror putting a trial in jeopardy as a result of less-than-discreet online postings. Commentators are nonetheless cautious. Justice Frances Kiteley, an Ontario Superior Court judge and co-chair of the Canadian Centre for Court Technology, summarises the position thus: "I don't think it's known that members of a jury are tweeting or on Facebook. That doesn't mean it doesn't happen … Given the statistics of the use of social media, the chances of having 12 people not accessing social media when they're on a jury is slim to none."[26] Justice Kiteley has devised her own template that she reads at the start of trials, warning jurors to stay off real-time social media and to curtail searches concerning any of the people or places or issues involved in the case.

42 Toronto criminal lawyer and prominent blogger Edward Prutschi echoes the sentiments of Justice Kiteley. He contends that "[i]f we don't tell jurors specifically [not to use the Internet to inform their decision on how to vote …] I think we're inviting a breach … [e]very year that we wait, it becomes more and more likely that our bench is out of touch with our jurors".[27]

43 Nonetheless, in 2009 one of Ottawa's newspapers, the Ottawa Citizen, brought an application seeking permission for its reporters to use their mobile phones, laptop computers and other forms of electronic text messaging to report live on criminal proceedings against the Mayor of Ottawa, Larry O'Brien. In granting the application, Judge J. Douglas Cunningham rejected concerns about "putting the genie back in the bottle". However, he cautioned that his ruling was specific to that trial in particular, and that the emerging social media technologies could raise additional concerns in a jury trial.[28]

4. Australia

44 Australia's position in respect of real-time communications from court reached its most liberal zenith in 2009, when the Federal Court of Australia allowed "live-tweeting" from its courtrooms. This was the first time that

26 *Ibid*.

27 *Ibid*.

28 Javad Heydary, "Tweeting from the Courtroom", *E-Commerce Times* (21 July 2009).

any Australian court countenanced the use of Twitter during proceedings. Federal Court Chief Executive Warwick Soden stated then that so long as the individual judge presiding over the case was fine with the practice, the Federal Court would have no issues.[29]

45 Since then, the Australian position has been tempered a great deal, in particular by the highest court in the land. Recently, on 23 November 2011, the Australian High Court issued a timely reminder in the *Australian Federation Against Copyright Theft v iiNet* case, stating that the mere *use* of electronic devices in the High Court would be prohibited:

> We ask that you do not take any of the following items into the courtrooms when the court is in session: cameras, radios, pagers, tape players, tape recorders, mobile phones or any other electronic equipment.

46 Persons seeking to attend hearings in the High Court, therefore, are required to surrender all electronic equipment before entering the courtroom.

47 While this overall ban on electronic devices appears to be only in place in the High Court,[30] certain lower courts in Australia appear to be in support of the practice. On 4 November 2011, Magistrate Peter Mealy in the Melbourne Magistrates' Court barred all "tweeting" in the committal hearing of Simon Artz after he learned that media writer Margaret Simons had been "live-tweeting" the proceedings. Magistrate Mealy subsequently warned journalists in his courtroom, in no uncertain terms, that "[i]t will be contempt if [tweeting] does occur from this court".

48 It has also been noted that while few Australian courts (apart from the High Court) have explicit policies on the practice of permitting live text-based communications from a courtroom, this simply means that the onus would be on the media to obtain approval or permission. Bond University journalism professor Mark Pearson echoed a common and commonsensical sentiment when he stated: "In a preliminary hearing in a serious criminal matter where there are evidence issues and particularly

29 See Liam Tung, "Court Tweets Sustained But Paper Still Lurks", ZDNet Australia (21 October 2009).

30 See Nic Christensen, "Reporters' Live Tweeting from Court Risks Mistrials", *The Australian* (5 December 2011).

admissibility issues discussed, you can quite understand the judge or magistrate not wanting instantaneous reporting."[31]

49 Nonetheless, it does seem that apart from the absolute ban on electronic devices in the Australian High Court, the use of real-time communications from courtrooms in Australia remains a contentious issue. The permissibility of real-time social media use and communication, for now, appears to lie at the discretion of each individual presiding judge.

5. Singapore

In Singapore, the Supreme Court[32] and Subordinate Courts[33] Practice Directions already prescribe to judges the discretion to permit the use of social media within the courtroom in appropriate situations. Specifically, paragraph 21A of the Supreme Court Practice Directions states as follows:

> **21A. Use of electronic and other devices**
>
> (1) In order to maintain the dignity of Court proceedings, the Honourable the Chief Justice has directed that, in all hearings in open Court or Chambers before a Judge or Registrar, video and/or image recording is strictly prohibited.
>
> (2) Additionally, *all communications with external parties* and audio recording during a hearing are strictly prohibited without prior approval of the Judge or Registrar hearing the matter.
>
> (3) Court users are only permitted to use notebooks to take notes of evidence and for other purposes pertaining to the proceedings during hearings, provided that such use does not in any way disrupt or trivialise the proceedings.
>
> [Emphasis added.]

50 The use of real-time *text-based* social media falls squarely within paragraph 21(A)(2) of the Practice Directions. A Twitter user "tweeting", a Facebook user updating his individual profile status or a blogger updating his Wordpress blog about ongoing proceedings (from within the courtroom) would necessarily be "communications with external parties".

---

31 See Nic Christensen and Pia Akerman, "No Tweeting Edict 'A Timely Reminder' for Journalists", *The Australian* (5 November 2011).

32 Supreme Court Practice Directions, paragraph 21A(2) which came into effect on 15 May 2010.

33 Subordinate Courts Practice Directions, paragraph 138A(2) which is *in pari materia* with the Supreme Court's Practice Directions.

This is so since Wordpress, Twitter and Facebook updates are accessible over the Internet and certain categories of users will be alerted to such updates: the reporter's followers on Twitter and his "close friends" on Facebook.[34] Although, there is no absolute prohibition against the use of real-time social media in the Supreme Court, such use is prohibited "without prior approval of the Judge or Registrar hearing the matter".

51 It would appear, therefore, that the present Singaporean position envisages each individual judge or registrar having full discretion over whether or not the use of real-time *text-based* social media is to be tolerated within a specific courtroom or chamber. This is not unlike the position in each of the foreign jurisdictions reviewed earlier. It should be noted, however, that to date no written guidelines have been issued in Singapore as to the extent of real-time social media usage that would be permitted by the Judiciary in court.

6. Discussion

52 The use of real-time social media in court raises various fears such as witness bias or subornment, *viz*, witnesses may be susceptible to pressure, bias or advance coaching as a result of the information posted from the courtroom. These are legitimate concerns given that they have the potential to derail a trial and jeopardise a verdict, resulting in delays, wasted resources, increased costs or in the worst case, a miscarriage of justice. However, an absolute prohibition on the use of real-time social media in court is not the panacea, as implicitly recognised at paragraph 21A(2) of the Practice Directions, for three main reasons.

(a) Confusing the medium for the message

53 First, the temptation to confuse the medium for the message is a great one, but it is one we should rightly resist. The offence of contempt of court and the rule against commenting publicly on cases *sub judice* have existed

34 It does not appear that the use of *text-based* Twitter or Facebook would fall afoul of paragraph 21A(1), which is limited to "video and/or image recording", and unlikely to be interpreted expansively to include other types of modern reporting technologies. However, the posting of a photograph or video clip would necessarily fall afoul of this paragraph since the image or video clip would first have to be recorded within the courtroom.

since time immemorial. The specific *channels* utilised by would-be transgressors have evolved from oral speech, to the written word, previously in print and now, digitised text. But these channels remain mere conduits, each only a *medium* for transmission. They are not the message.

54 The real issue, therefore, would appear to be abusers of social media, abusers of the channels. It is inevitable that there will be individuals who seek to employ social media for ignoble ends. But in such cases it will not be Twitter or Facebook that command regulation, just as the proper panacea for reckless drivers would *not* lie in a blanket ban on automobiles. In these circumstances it is human behaviour that falls to be regulated, and for that we already have contempt (and other) laws in place.

(b) Holding back the tide

55 Second, the fear of real-time, *immediate* courtroom reporting via social media channels may be more illusory than real, given that same-day updates to online portals such as The Straits Times Online are permitted. Further, a conscientious journalist may write his report "real-time" on his tablet while in the courtroom, and then step out of the courtroom to post it on his blog using his tablet's built-in broadband connection to the Internet. Moreover, given the fine reputation of the Singapore courts as forerunners of technology, embracing social media would only cement our reputation for being technologically-savvy.[35] Given the bold position adopted by the Supreme Court of the United Kingdom, it is arguable that Singapore should at least consider the viability of adopting a similar approach (with appropriate safeguards).

(c) Increasing access to justice

56 Social media platforms like Wordpress, Twitter and Facebook provide journalists with new means of reporting events. In suitable cases of interest to the public, live blogging may be a means of providing interested members of the public greater access to the proceedings within the courtroom. This will also assist in our public education efforts as live

35 Even other jurisdictions which have had to address the grave concern of using Twitter in jury trials have not rejected outright the use of real-time social media in court. These specific considerations do not feature in Singapore's context and it stands to reason that our courts should likewise approach this issue in a measured and reasoned manner.

blogging will provide broader exposure to how our courts work and in that process, demystify our legal proceedings.

57 Ultimately, a law that cannot be enforced is indistinguishable from bad law. Given the intractable theoretical difficulties related to clamping down on neutral *channels* in general, there is every possibility that it might actually be counter-productive to attempt to curtail what has essentially become a way of life for the next generation not just in Singapore, but also the world.

V. SOCIAL MEDIA AS EVIDENCE

1. Safeguards for discovery of documents and preservation of evidence

58 The processes for discovery of documents and preservation of evidence have developed along with the evolution of digital communication. It is now established law in many jurisdictions, including Singapore, that electronic discovery of documents in a computer database and preservation of such electronic evidence are acceptable steps within the civil litigation process.[36] The Canadian courts have gone on to find that apart from documents and evidence contained in a computer database, posted content contained on social media such as Facebook are also "documents" capable of being discovered if the postings are relevant and fall under the party's control or power. The position remains the same regardless of whether the content on the website is maintained for public, private or limited viewing.[37]

59 While applications for discovery of documents and preservation of evidence on social networking websites have not arisen for the court's consideration in Singapore, these issues ought to be actively considered since social media may, in all probability sooner rather than later, come to be relevant in this context as well.

---

36 See for example, *Alliance Management v Lane Pendleton* [2007] 4 SLR(R) 343; *Alliance Management v Lane Pendleton* [2008] 4 SLR(R) 1; and *K Solutions v National University of Singapore* [2009] 4 SLR(R) 254.

37 See for example, *Leduc v Roman* [2009] CanLII 6838 (ON S.C.)

(a) Discovery of documents on social media against parties to the proceedings

60 Under Order 24 rule 1 of the Rules of Court, the court may order any party to a cause or matter to make and serve on any other party a list of documents "which are or have been in his possession, custody or power" if the documents relate to the matters in question. The meaning of "documents" is not limited to paper but includes electronic information on a computer database.[38] Given the expansive definition of the term "documents", posted content on a website that is capable of being retrieved and converted into readable form may similarly constitute "documents" for the purposes of Order 24 rule 1.

61 It may previously have been contended that Order 24 is usually concerned with the physical possession or custody of documents and that online content cannot be said to be in a party's physical possession or custody and capable of production. However, the court in *Leduc v Roman*[39] addressed this point squarely when it held that a party's online postings can fall under his control or power since the party can post or remove content.

62 Given the wide ambit of our Order 24, it is certainly arguable that a party to an action may be allowed discovery of content on social media if it is proved to the court's satisfaction that a party's online postings are under his control or power and the content is relevant to the issues in question. In practice, parties can refer to Practice Direction No. 3 of 2009, which addresses the practical issues of making electronic discovery applications.

(b) Discovery of documents on social media against third parties

63 It has been discussed earlier that discovery of documents on social media may be obtained against a party to the action. It is pertinent to consider the related issue of whether a party may seek discovery from the owner of the social media site who is a non-party to the action but who has access to the documents in question. For example, where there is relevant information on the defendant's Facebook account, can the plaintiff bypass the defendant and seek discovery of those documents directly from Facebook instead?

38 See *Derby & Co Ltd v Weldon (No 9)* [1991] 1 WLR 652 and *Megastar Entertainment Pte Ltd v Odex Pte Ltd* [2005] 3 SLR 91.

39 [2009] CanLII 6838 (ON S.C.).

64 In this regard, it seems that the discovery of documents by a non-party under Order 24 rule 6(2) is possible where the non-party is within the jurisdiction of the Singapore courts; the documents are in the non-party's power, control or possession; and the documents meet the criteria of relevance, necessity and sufficient identification. This would probably be a useful option for the plaintiff where the defendant is unable to produce the content sought for but there is reason to believe that the content is still existing and retrievable, for example, on Facebook. This power extends to compelling a non-party *within* jurisdiction to produce online material situated *outside* jurisdiction.

65 However, while the court has wide powers to order a non-party to produce the documents in the interests of justice, the court will not have jurisdiction to order discovery by a non-party located *outside* Singapore. The plaintiff's recourse in that situation is to proceed against the defendant *in personam*.

(c) Preservation and inspection of evidence on social media

66 The issue of preserving and inspecting evidence contained on social media is fairly novel but nonetheless important, as the party seeking the evidence has to ensure that the evidence is not tampered with or destroyed. It cannot be gainsaid that if documents on social media are discoverable, the obligation of litigants to preserve documents on social media will follow once litigation is reasonably contemplated.[40]

67 It is thus important to consider if the Rules of Court allow the court to order either the party to the action or the non-party site owner to preserve evidence on social media for inspection. While a party has the option of hiring computer forensic experts to verify if another party has tampered with the evidence, there may be prohibitive cost consequences in taking this approach. Hence, the availability of court sanction for non-compliance with the court's order for preservation of evidence may be an important weapon in a party's litigation arsenal.

68 Using the Facebook example alluded to earlier, can the plaintiff apply for a court order compelling the defendant to preserve his Facebook page "in his possession" for inspection? Under Order 29 rule 2, the court has the

40 See for example, *K Solutions Pte Ltd v National University of Singapore* [2009] 4 SLR(R) 254.

power to make an order for the preservation of any property which is the subject matter of the cause or matter, or for inspection of property in the possession of a party to the cause or matter. As "property" may include property in the form of a document,[41] and the term "document" has a wide meaning as explained above, a case may be made out for the court to grant such an order against the defendant. It is less likely that the plaintiff can succeed in getting the court to compel Facebook to preserve the defendant's Facebook page for inspection since Facebook is not a party to the cause or matter.[42]

69 Not unexpectedly, reservations have been expressed as to whether a person's Facebook page can be defined as a "document". Documents are made with specific intent and forethought, with some investment of time and effort. The nature of communication on one's online social media profile page would not be the same as messages might be typed quickly, without much forethought, and thus easily taken out of context, misinterpreted and used to prejudice the defendant. It might be the case that it is too simplistic to categorise social media under the overly broad category of "document". Instead, it would be helpful if specific guidelines on the appropriate treatment of social media as evidence are developed. This would serve to avoid the chilling effects that inappropriate use of social media might have on online speech and on the willingness of citizens and netizens alike to adopt new communication technologies.

70 Separately, as Anton Piller orders complement the court's jurisdiction and power under Order 29 rule 2, the plaintiff may apply for an *ex parte* order to search and seize the defendant's computer to ascertain if the evidence has been tampered with, *if* he is a party over whom the court has jurisdiction. Documents in the possession of the defendant would include all electronic documents on a computer located in the premises specified in the Anton Piller order.

71 In this regard, it is arguable that the ambit of the Anton Piller order extends to social media, or following from the earlier example, the defendant's Facebook account. If the Facebook documents are accessible

41 See *Re Saxton (dec'd)* [1962] 1 WLR 859.

42 See *Douihech v Findlay* [1990] 1 WLR 269, although it may be possible to argue that Facebook should be joined as a defendant to the action if it has facilitated the wrongdoing by which the party seeking inspection of property has suffered: see *Singapore Civil Procedure 2007*, at 29/8/7.

from a computer within the premises, it is the copy of the documents *downloaded from Facebook and residing on the computer in the premises* that the Anton Piller order attaches to. When a Facebook page is accessed, (at least) one copy will reside in the internet browser cache. This copy would be within the possession of the defendant and hence subject to the Anton Piller order. Furthermore, by accessing Facebook on the computer, a copy of the Facebook page will also be in the computer's Random Access Memory (or RAM). This is in addition to the copy in the cache which resides on the hard disk.

72 Accordingly if copies of the defendant's Facebook page already exist in the computer's RAM or the cache at the time of the search, a strong case can be made out that these fall within the scope of the Anton Piller order. Otherwise, the challenge in the execution of the Anton Piller order is whether the defendant can be compelled by the party executing the order to access his Facebook page in order to bring the defendant's Facebook page into his possession within the premises specified in the Anton Piller Order.

2. Other concerns about social media as evidence

73 Quite apart from the foregoing, the unique qualities of social media engender several other concerns about the medium's suitability as evidence. One characteristic about social media that stands out, for example, is the high degree of informality involved. As alluded to earlier, messages tend to be typed quickly without much forethought and may be easily misinterpreted. Yet, unlike speech, there is some degree of permanence (or transience, depending on who is asked). Further, there could also be some difficulty determining the actual author of the messages. While these factors could result in their low probative value as evidence, would such factors also render social media inherently unreliable evidence?

74 Courts in Singapore and elsewhere have generally accepted e-mails as documentary evidence required to be routinely preserved, discovered and, if relevant, admitted into evidence at trial. Judges have routinely ruled on the probative value of the e-mails to prove a particular fact. Often e-mails, like social media messages, tend to be typed quickly, without much forethought and thus are often misinterpreted by parties. However, there is a key difference: e-mails do not occur in real-time. Tweets, Facebook updates and instant messaging services derive and bestow much of their utility in being near-instantaneous forms of communication. There appears, therefore, to

be a spectrum of inherent probativeness in the realm of electronic communications, with e-mails occupying one end and the different forms of social media (with instant chats at the extreme) occupying the other.

75 Another characteristic about social media is the wide spectrum of technologies that are employed for different services. Users of social media also span the entire gamut of computer literacy: some users are familiar with the intricacies of the underlying technology while others only know how to use the application. Given these factors, it would be a difficult matter of proof to determine whether data has been accidentally or deliberately deleted.

76 A concrete example: some social media sites have an auto-archiving function for old messages and some skill is required to retrieve such messages from the archive. If a litigant is unable to do so, is he in breach of his discovery obligations? Another example is that some social media sites automatically delete older content unless the user configures it otherwise. If a user fails to do so, has he breached his evidence preservation obligations?

77 At present the answers to these questions do not appear to be readily available. While there have been suggestions on ways to safeguard the reliability and credibility of online evidence – including the use of a Digital Notary to authenticate and verify digital evidence; the hiring an independent third party paid to download a relevant page or site and have the documents certified to be tamper-free before being presented as evidence; and to examine version histories and perform information collection from servers – many of these ideas remain untested and will only be proved in due time.

VI. CONCLUSION

78 The introduction and subsequent proliferation of social media have given rise to heretofore unconsidered legal issues. As the technology evolves, social media will surely continue to precipitate unprecedented legal issues. Rules of evidence and procedure will have to be changed to cope, as will attitudes of both litigants and the courts. In this connection, it is worth noting that the panel discussion at the conference arguably threw up more questions than answers. Fortunately, this is probably more a function of social media being a recent phenomenon than anything else. With time, it is hoped that the various issues will be resolved and the questions answered

– at the very least, before the next technological insurrection in social media takes root.