

Lockdown! Compliant Preservation of e-Documents for Litigation & Regulatory Investigations

The foreseeable threat of regulatory investigation, litigation or the onset of proceedings now require organisations in the United Kingdom to make accountable decisions about the *timing* and the *scope* of preservation of electronically stored information (“ESI”). This duty is independent of statutory retention periods for various corporate records such as accounting, PAYE, tax, and other corporate filings. It applies to every location where enterprise data is located, including remote devices and employee home computers.

This is a source of considerable angst for records managers, archivists, IT, and in-house counsel because there is limited regulatory guidance in the statute books and inchoate directions from the courts on the extent of an organisation’s duty to preserve ESI prior to the commencement of formal disclosure in a litigation or regulatory context.

The challenge of when and how to effectively segregate and ring-fence relevant ESI is especially urgent because routine records retention and information management protocols are generally insufficient to satisfy the legal duty to *preserve* ESI. We live in a world where a younger generation of workers are comfortable with round the clock, synchronous communications on heterogeneous platforms, across diverse time zones.

Routine records management procedures will not accurately capture transient, active, replicant or residual data, and the associated metadata on employee electronic devices. For instance, we now negotiate contracts by email, modify them in a blog, breach them in an SMS text, and violate confidentiality in an instant message (“IM”), whilst travelling across jurisdictions. How do you preserve the contents of relevant SMS texts, tweets and instant messages for long term judicial or regulatory evaluation? What might be the consequences if you fail to do so?

The Legal Duty:

The primary regulatory guidance on ESI preservation in England and Wales is provided by the 2005 Practice Direction (“PD”) to Part 31 of the Civil Procedure Rules (“CPR”) which directs parties to a dispute to discuss any issues that may arise regarding the preservation of electronic documents.

This obligation to preserve ESI is consistent with settled UK case law. Justice Megarry set the benchmark in *Rockwell Machine v. Barrus* [1968] 1 W.L.R. 693 at 694, ruling that an organisation has a common law duty to preserve relevant documents in its possession or control whenever litigation is reasonably foreseeable. He stated as follows:

“It seems to me necessary for solicitors to take positive steps to ensure that their clients appreciate at an early stage ... the importance of not destroying documents which might by possibility have to be disclosed. This burden extends ... 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.”

The duty to triage ESI preservation was more recently summed up in *Hedrich v Standard Bank* (2008) EWCA Civ 905 where the Appeal Court affirmed the ruling in *Myers v Elman* (1940) A.C. 282. The court recognised that organisations have the ultimate responsibility for *executing* preservation obligations, but their lawyers have a duty of careful investigation and supervision in the process. The lawyer's obligation is to investigate the situation carefully and to ensure so far as possible that full and proper disclosure of all relevant ESI is made. However, he cannot be expected to challenge his client's assertion that all relevant ESI has been produced unless he has extraordinary reasons to doubt his client's statement.

In a pre-litigation context, Guideline 1 of The Sedona Conference Commentary on Legal Holds ("Commentary") elaborates that the duty arises when an entity is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation – virtually all the time for large corporations.

A series of persuasive US cases, some of which have been relied on by English courts, have shed further light on this duty. In *Re Bristol-Myers Squibb Securities Litigation* 205 F.R.D. 437 (2002), p.440 the court noted that since the bulk of corporate documentation is now held in electronic form, the discovery of computer evidence was critical to a proper investigation of alleged fraud. Hence, electronic evidence discovery should be a routine practice and an integral part of fraud investigation and litigation.

In *Miller v Phillip Holzman*, 2007 WL 172327 (D. D.C. Jan. 17, 2007), the court stated that the duty to preserve electronic documents applies to evidence which the party knows or reasonably should know is relevant to existing or future litigation and the destruction of which may prejudice relevant parties to that litigation. In *Danis v USN Comm., Inc.*, 2000 WL 1694325 at 1, 32-33 (N.D. Ill. Oct. 23, 2000) the court established that the obligation exists independent of any order of the court or request from another party and is imposed directly on organisations.

Recent ESI Preservation Failures:

Are your lawyers properly equipped to discharge this obligation? The auguries are not good. Just like in the cartoons where the coyote runs off the cliff and is fine until it looks down, recent decisions indicate that in-house lawyers and their litigation counterparts do not fully understand their role in ensuring compliance with ESI preservation obligations. They only become aware of their failings when staring down the barrel of a Judge's gun or when caught in the cross-hairs of a negligence claim.

In *Abela v Hammonds Suddards (a firm)* Chancery Division Claim No. HC07C01917, [Lawtel](#), 2 December 2008, the claimants made allegations of negligence, breach of fiduciary duty and deceit against the defendant law firm and a deceased partner. The defendant law firm failed to disclose relevant emails, and the family of the deceased partner destroyed his personal computer prior to litigation. The court emphasised the key role of information organisation and preservation in ESI disclosure (called "e-disclosure" in the UK and "e-discovery" in the US) by stating at paragraph 122(4) that:

“The starting point for assessing whether and if so how a reasonable search might be undertaken, must be an accurate account of what data or data sets are available, on what media they are stored, in what format or formats they are stored, how the information is organised, and what the overall quantities of data are.”

The court directed Hammonds to utilise this broad and clear standard “to take steps so as to be in a position to supply a more detailed account of the stored data”. The court further ruled that the claimants were entitled to learn from the deceased partner’s family “with reasonable clarity and detail” what his computer contained and whether he had stored documents elsewhere.

In *Hedrich v Standard Bank* (2008) EWCA Civ 905 (30 July 2008), the claimant in a breach of contract claim alleged that he could not retrieve relevant electronic documents. He later produced a set of recovered emails which he asserted were fully responsive to the defendant’s request. However, full disclosure of electronic files was given by the claimant only at trial, at which point devastating adverse evidence came to light forcing him to discontinue the claim. The claimant’s solicitor then faced the ignominy of defending negligence allegations.

Legal Compliance Trends

The indications are that the current judicial and regulatory environment is increasingly intolerant of organisations that fail to produce responsive ESI in a timely manner. There has been a spike in global regulatory investigations, predatory litigation and judicial enforcement since the toxic loans turmoil that started in 2007.

A recent survey by information risk management vendor Recommind indicated that 41% of UK IT chiefs reported an increase in requests for ESI in the past year. Another survey by Millnet indicates that litigants in commercial disputes have enjoyed more competitive advantage in the last six months than at any time in the last nine years as a result of ESI disclosure failures. Authorities no longer accept that IT problems are to blame for failing to produce relevant ESI, holding instead that such failure is evidence of obstruction or deception.

To make matters worse, a raft of national laws have created compliance obligations beyond the borders of the originating country in response to nefarious corporate practices which wiped out over \$900 billion in shareholder value since the Enron era. For instance, the US Sarbanes Oxley Act created worldwide obligations for US listed companies, including criminal penalties for altering, destroying or concealing documents.

More recently, the Obama administration outlined its proposals for new financial industry regulations which will affect foreign affiliates of any company that has an industrial loan arm – virtually all major retail companies in every sector. The UK Treasury and the Financial Services Authority are in the process of rolling out similar sweeping reforms. These proposals all include overt mandates for investigations, prosecutions and fines, and will spawn aggressive global enforcement action. At the same time, the EU Commission

is ramping up its cross-jurisdictional muscle flexing – evidenced by the recent record fine of €1.06 billion against Intel for breaching competition laws.

Likewise, the 2006 amendments to the US Federal Rules of Civil Procedure (FRCP), created universal ESI preservation obligations in all cases commenced in US Federal courts. This covers conduct outside the US in cases brought under far reaching statutes such as the Alien Tort Claims Act (ATCA) and the Foreign Corrupt Practices Act (FCPA). Numerous companies have been caught in this intricate web, including Shell, Halliburton, Siemens, Pfizer, and British American Tobacco. For organisations operating in several jurisdictions the problems are multiplied by varying levels of privacy laws.

Business Impact

The business impact of this heightened level of regulatory and judicial scrutiny is that enterprises which ignore the ESI preservation risks inherent in local and remote working, as well as the management of employee Web 2.0 communications do so at their peril. Since over 93% of enterprise records are electronic, and the volume and mix of data types is exploding, millions of electronic documents are now routinely collected from all locations where an organisation has custody, control or access to electronic documents – be it in London, Lima, or Timbuktu.

The dynamic nature of ESI means that critical documents can easily be overwritten, modified, destroyed, or corrupted during normal use. It does not matter whether this happens accidentally or maliciously. The result is the same – loss of potentially relevant evidence giving rise to probable criminal penalties, fines or court sanctions for spoliation.

A laundry list of persuasive US cases have made this point, yet organisations in the UK seem to be stuck in reactive mode. Recommind found that 69% of UK IT chiefs allocated less than 5% of their IT budget to e-disclosure, including the preservation of ESI, with nine out of ten dedicating less than 10%. The recent decision in *Digicel v Cable and Wireless*, (2008) EWHC 2522 (Ch) is a warning shot of what might be to come. In this mobile telephone interconnection dispute, the defendant, Cable and Wireless, made unilateral and wholly inadequate decisions about where and how to find relevant ESI. Justice Morgan ordered a more rigorous effort, including the expensive restoration of archived information on back-up tapes.

Since, most companies must rely on their employees to both retain and preserve data within the matrix of company policy and the constraints of regulatory obligations, you must consider all stakeholders' ways of working and ensure that your information architecture and data management protocols provide a structured, defensible framework for ESI retention and preservation. This should be a systematic process which recognizes that employee practices will forever be as unpredictable as an unruly teenager. They will bypass policy and use the most convenient tools, including private ones, as long as they feel that they won't be penalised. **A useful starting point is a well articulated strategy for information organisation and access (IOA) – the use of complementary and ancillary technologies to improve findability of enterprise data. This strategy will**

make it easier and more cost-efficient to find and preserve accurate ESI in response to a regulatory or litigation request.

The Timing and Scope of Preservation:

Since the triggering event in an investigation or a lawsuit can, and often does occur, long before action is commenced by a regulator or an opposing party, deciding when the duty is triggered requires reasoned analysis of all the available facts and is not amenable to a systemised checklist. Guideline 4 of the Sedona Commentary on Legal Holds suggests that this judgement should be based on good faith and a reasonable investigation of all the available facts. Trans-Atlantic judgements indicate that the duty is triggered once an organisation knows or ought to know that it is in peril of litigation or investigation.

The scope of ESI to be preserved is determined by their relevance to the subject matter, but will generally include all documents on which an organisation intends to rely on, those which support or adversely affect any party's case and those which have been ordered by a court or a regulator to be disclosed. Ultimately, organisations should be ready to supply specific, fact-based, and rational grounds for their ESI preservation choices. If you plan to rely on an external expert ensure that he can explain your federated or distributed information architecture, and be able to state an opinion as to the reasonableness or good-faith of the system's operation.

Best Practice Steps:

As regulators and courts increasingly exercise their oversight powers, it can be expected that they will hold organisations accountable to explain the evaluations which underpin their ESI preservation protocols. The following tips may provide useful guidance:

(1) The Chinese proverb “dig your well before you are thirsty” is particularly apt. Be proactive and establish a transparent, documented and defensible methodology for the preservation of ESI once a regulatory investigation or litigation is foreseeable. This process should be driven by senior stakeholders from legal, IT, records, and compliance.

(2) Implement an effective information management framework that ensures that records generated by the business are kept and destroyed in a legally compliant manner. This structure will generally provide a consistent methodology and the volume thresholds in which data is deleted, overwritten, or stored to off-line or back-up systems.

(3) Preserve metadata. The metadata associated with an electronic document can be just as important as the data in that document because it establishes the *context* in which the electronic *content* was created. The courts and regulators expect that the metadata associated with ESI will be kept intact.

(4) Implement an information organisation and access (IOA) strategy as the essential cornerstone of the above procedures. AIIM runs an excellent programme

which can enhance an organisation's ability to systematically create, implement, and administer a holistic information management and compliance strategy.

(5) Constantly monitor custodian based-retention practices. Employees tend to store data in the most convenient manner regardless of policy. Portable media or storage devices can now hold vast amounts of data which can exist at any given time only on that device. Along with Web 2.0 social networking platforms, they can be crucial in establishing relationships, timelines, and exceptions to hearsay objections. Remember that different functions handle data in different ways. For example, mahogany row executives often deploy *private email systems* that are known only to a handful of people. You must guard against the concealment of such potential sources of ESI.

(6) Deploy archiving technology that meets evolving data retention and preservation obligations, and don't rely on backup tapes as an archive.

(7) Centralise and consolidate preserved ESI into one or just a small a number of repositories if your organisation is routinely involved in litigation or regulatory investigation, or once you anticipate any of these events. This will reduce the cost and disruption normally caused by the e-disclosure process.

(8.) Develop a transparent and consistent process for ingesting preserved ESI back into an enterprise archive once the investigation or litigation is fully concluded.

John Okonkwo is dual qualified US Attorney and UK Solicitor specialising in information governance, with a focus on e-discovery and e-fraud. He is a professional member of AIIM and the Association of Certified Fraud Examiners (ACFE).

john@ducainformbes.com

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.