IBM Enterprise Content Management
Thought Leadership White Paper

June 2012

Information governance in anticipation of civil litigation in the UK

Mitigating expense and risk with proactive information governance

IBM

Contents

Introduction

This paper has been written by Chris Dale of the UK-based eDisclosure Information Project[1] and in conjunction with the IBM UK Enterprise Content Management group[2]. The eDisclosure Information Project brings objective and informed comment to lawyers, judges, suppliers and clients and is aimed at encouraging the better use of technology in electronic disclosure for litigation. IBM's Information Lifecycle Governance solutions focus on the secure collection, classification, archiving, discovery and timely disposition of all critical enterprise information.

The paper's title, *Information governance in anticipation of civil litigation in the UK*, derives from the fact that the disclosure of documents and other data for civil litigation purposes is a source of both expense and risk. Both of these can be mitigated by a proactive information governance strategy which includes prospective disclosure obligations amongst its objectives.

Disclosure of documents – inevitably mainly electronic documents – is generally a reactive, lawyer-led process which starts afresh with each new case, approaching the company's data stores as if they were terra incognita to be explored from a standing start. This approach is inevitably expensive, disruptive and prone to over- or under-collection and it does not lend itself to the early and accurate estimate of the prospects of a successful outcome, or the likely costs. For those companies who can expect any volume of litigation, it makes sense to design an information governance environment, which not only takes advantage of any prior knowledge about the organisation's information domain but also proactively minimises the volumes of information which are subject to discovery by executing the appropriate policies.

Scope of the paper: The UK litigation driver for better information governance

Litigation is not the only driver for implementing a proactive information governance strategy. Regulatory and internal investigations raise similar issues and there are operational benefits, as well as significant IT cost reductions, which drive the requirement for better control of data.

This paper focuses primarily on the role of information governance in minimising legal risks and costs in the context of the UK civil litigation system and in helping organisations secure a better outcome to their legal challenges.

In cultural and statistical terms, litigation is less a feature of business in the UK than it is in the US[3]. The UK policy emphasis has been on the encouragement of settlement and that, together with the very high costs of bringing actions to trial, has reduced the number of cases which are seen to a formal conclusion through the courts[4].

Many companies, however, must litigate, or at least show themselves ready to do so to enforce or defend their rights or to establish points of principle. Whilst the principles discussed in this paper relate to the jurisdiction of England and Wales, they are relevant to companies from elsewhere.

The disclosure of documents and data is a fundamental duty in UK civil litigation, as it is in the US and elsewhere. The emphasis in the UK courts, however, is more on active judicial management and on proportionality rather than on sanctions for omissions and for procedural defects. Paradoxically perhaps, this places a higher premium on a proper understanding of a party's documents, on their ownership and location, and on their likely relevance. Where a US company would expect to have to disclose anything potentially relevant, a party to UK litigation has both the duty and the right to narrow the scope of disclosure. Companies which are in proper control of their information are better placed to do this and therefore reduce disclosure costs.

Courts are increasingly interested[5] in document retention policies and other internal procedures which affect the availability of documents for disclosure. There is less to fear, and at least as much to gain as in the US, for those companies who can show that deletion took place pursuant to a defensible policy[6].

The ability to narrow the scope of disclosure for civil proceedings is only one reason why UK companies need more granular control over their data. Regulatory investigations and internal investigations impose similar obligations as to disclosure. The UK Bribery Act[7] provides others. These other motives for information governance are considered below.

Not least of the benefits of information governance is that there are significant cost reductions and strategic benefits to companies which have control of their data.

Whilst the primary emphasis in this paper is on one specific pressure point, UK civil litigation, the principles and the risks, burdens and benefits, apply to other activities and in other jurisdictions as well.

UK civil litigation framework

The UK civil litigation context for electronic disclosure

The formal stage, *Disclosure* (the equivalent of Discovery in the US and elsewhere) is not, of course, the first time that a party and its lawyers will want to focus on documents and data. The instruction of lawyers is generally accompanied by the client's selection of what is considered by the clients to be key documents. *Pre-action protocols* generally require a "letter before claim" and a "full written response", both of which must "list the essential documents on which the [party] intends to rely". Each party may ask the other for "further relevant documents not in [Party 1's] possession and which [Party 2] wishes to see". This is not intended to be pre-action disclosure, but the lawyers can benefit from having early visibility of documents at this stage, preferably without incurring significant costs.

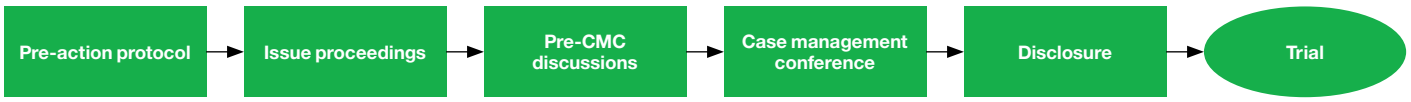

Figure 1: Key stages in the UK civil litigation process

A circular conflict can arise here: the client wants an early estimate of both prospects and costs, and generally does not want to commit to significant expense without having some estimate of both; any proper assessment of prospects and costs however, requires an understanding of the issues and the basic facts which can only truly be ascertained from reviewing at least some of the documents. Assessing pure cost, irrespective of the merits, is almost impossible without some understanding of the volume of data likely to be involved and the potential complexity of managing it.

Even before one considers the formal disclosure requirements, there are clear benefits to the client in having sufficient understanding and control of its own documents to allow both the identification of the key documents needed for an early assessment of the merits and some idea of the potential scope of the data sources. The *Case Management Conference* and the discussions that ought to precede it, come too late for this analysis to influence the risk assessment and decision-making which should come before positions become entrenched in the litigation.

The disclosure rules – Part 31 CPR[8] and Practice Direction 31B[9]

The disclosure rules appear in Part 31 of the Civil Procedure Rules and its associated Practice Directions. A document is widely defined as being "anything in which information of any description is recorded". Disclosure is not automatic, but the court almost invariably makes an order for standard disclosure, that is, for disclosure of documents on which a party relies, which adversely affect his own case, or which support or adversely affect another party's case [Rule 31.6]. This narrower test replaced the test of 'relevance' which appeared in the Rules down to the introduction of the Civil Procedures Rules of 1999.

The search need only be a "reasonable search" [Rule 31.7] having regard to factors such as the number of documents involved, the nature and complexity of the proceedings, the ease and expense of retrieval, and the significance of any document likely to be located during the search. The rules "do not require that no stone should be left unturned"[10].

The CPR is subject to the "overriding objective" set out in Rule 1 which imposes a duty to deal with cases "justly" by, for example, saving expense and dealing with cases proportionately. The courts have an express duty to manage cases actively to this end and their case management powers include the right to "take any other step or make any other order for the purpose of managing the case and furthering the overriding objective".

A consequence of this, but one that is insufficiently exploited by parties, is that where it can be done justly, the duties such as disclosure may be narrowed. Very significant costs savings may follow where opponents and the court can be persuaded to narrow the ambit of disclosure. A party can only do that if it is equipped to understand its own document sources and, crucially, to do so early enough to influence the decision-making at the Case Management Conference.

Practice Direction 31B of 2010 deals specifically with the management of electronic disclosure. For big cases it requires that parties discuss their sources, and work cooperatively to agree on the tools and techniques and other things necessary to manage disclosure efficiently and effectively. The PD expressly requires parties to consider the use of technology. It is accompanied by an Electronic Documents Questionnaire which provides a structured way for parties to exchange information and allows agreements and orders to be made on an informed basis.

A pending new rule, 31.5, will remove the default option of standard disclosure and require courts to decide what disclosure is really necessary. Again, a party who understands its own data is best placed to maximise the discretionary element in favour of reduced disclosure.

In *Goodale v Ministry of Justice*[11], Senior Master Whitaker encouraged an approach which sought to identify the information custodians that really matter and to limit disclosure, at least to begin with, to those custodians. The express purpose behind this judgment was to reduce the volume of documents reviewed by both parties. Master Whitaker also drew attention to the potential for modern software tools to limit the documents sent for review. This judgment, coupled with the practice direction obligations to discuss the scope of disclosure, again gives power to the well-informed party.

There are numerous cases in which parties were punished for e-disclosure failures. What is important to note, in the context of this paper, is the positive encouragement to negotiate narrower disclosure given by a proper interpretation of the rules and by the Goodale judgment. They encourage a move away from plodding mechanically through the rules and towards transparent, cooperative decisions more in line with the actual objectives of the parties, but only within the grasp of those who are in control of their document collections.

The practical implications of compliance with UK rules

The UK Civil Procedure Rules differ in many respects from the US Federal Rules of Civil Procedure. There is no formal concept of legal hold with the precise procedural hurdles which that has produced in the US; the only recent case directly involving failure to preserve data was a clear-cut example of deliberate destruction after the commencement of litigation[12]. The battles over the scope of requests is replaced by the disclosing party's own assessment of what should be disclosed following the rules set out above and qualified by the required discussions and cooperation.

It would be a mistake, however, to see the UK alternative as either trivial or inexpensive. There have been standout cases (as referenced throughout this paper) in which parties were penalised in costs, suffered serious reputational damage and, in one case at least, actually lost the case because of disclosure failures.[13] The landmark case for those concerned with corporate information governance however, is *Earles v Barclay's Bank*[14]. The judge, HHJ Simon Brown QC, was critical of the defendants' conduct of disclosure in the course of the litigation and punished them by reducing the costs to which they would otherwise have been entitled. He was critical also of their solicitors saying, "The Practice Direction is in the Civil Procedure Rules and those practicing in civil courts are expected to know the rules and practice them; it is gross incompetence not to".

The real importance of the judgment, however, lies in the judge's observations on the information management duties of companies which can expect to engage in litigation. Whilst accepting that the UK has no equivalent to the US legal hold obligations the judge said this:

One expects a major high street bank in this day and age of electronic records and communication with an in-house litigation department to have an efficient and effective information management system in place to provide identification, preservation, collection, processing, review, analysis and production of its ESI in edisclosure in litigation and regulation.

That is more than merely a judicial expectation: common sense suggests that a company which can expect litigation in the ordinary course of its business will at the very least make a calculation, based on experience, of the proactive costs of having the "efficient and effective information management system in place" as set against the anticipated cost per year of managing that information reactively for disclosure purposes.

Summary of procedural implications

The Civil Procedure Rules include a formal requirement to be able to discuss electronic sources of information at a specific stage in the process. The need to assess risk and costs at an early stage is a commercial (as opposed to a purely procedural) reason why a company needs to understand its own sources. Being equipped to do this reduces the per-incident cost of acquiring that information.

These cases show the risks in costs and reputation of not being in control of the data. More positively, a company which can make its lawyers quickly aware of both the overall scope of the potential document pool and the detail of specific classes of documents can expect advice and action more quickly and at lower cost as well as a better negotiating position vis-à-viz opponents.

Electronic disclosure for civil litigation therefore provides one compelling reason why companies need to institute information governance. It is by no means the only one.

The relevance of good information governance

Wider reactive implications justifying proactive governance

Because responsibilities, and the accompanying budgets, are often distributed within companies, it is not always easy for a company to see the full range of activities which would be embraced by company-wide information governance and which pools the requirements of business, legal and compliance, and IT. Other obvious areas to consider include the following:

- Few large companies can ignore the possibility of becoming involved in US litigation with its implications of very broad requests, legal hold and preservation rules.
- Any litigation with a foreign element raises trans-jurisdictional implications of law, language and practical matters.
- EU data protection and privacy implications require rule-bound retention policies which impose (or at least suggest) deletion of personally identifiable information no longer required for the purpose for which it was collected and which identify what consents might be needed.
- The automation of retention policies also allows the deletion of documents which might otherwise be discoverable in US proceedings but which are not presently the subject of a legal hold and for which the rules provide a "safe harbor".

- Regulatory and internal investigations impose similar obligations as to disclosure, often with an urgency and with implications that exceed those of civil litigation.
- The UK Bribery Act imposes an obligation to show that "adequate procedures" existed to prevent bribery, and information management is clearly an important part of this.
- Freedom of Information Requests and Subject Access Requests have serious implications, not least the costs of handling them.
- Data leaks bring serious implications of notification, cost and reputation.

Implementing a proactive information governance strategy not only protects sensitive information but also provides organisations with clear visibility of all information domains, their custodians, the relevant retention justification and the business areas where that information adds value. It also provides the legal department with the quantified metrics and tools it needs to accurately forecast legal and discovery costs.

A wider range of information sources

It is clear from what is said above, that whilst eDisclosure/ eDiscovery is important it is not the only imperative. Storage may still be cheap, but its management costs money, and potential risk lies in holding masses of material whose scope is unknown to anybody. More positively, it is worth considering the wasted value of the business information which is locked up in unsorted data.

In parallel with the growth in volume comes enormous diversity in the types of sources and content types to be found in most organisations. It is no longer enough to secure the email, the Microsoft Office files, the structured data and SharePoint information. Whilst these continue to grow in absolute terms, new data types bring implications of quantity, size and retrieval difficulties.

An increasing amount of information is held as audio or video and, like social media information, raise both eDiscovery and compliance issues. Regulators responsible for financial dealings around the world have long required that recordings be made, both to preserve information in respect of particular transactions and as part of a broader compliance function. FINRA[15], to take one example, has published formal guidance on applying its communications rules to blogs and social networking sites so that "firms are able to effectively and appropriately supervise their associated persons' participation in the sites"[16] with associated training and monitoring obligations.

Finally, data held in transactional database systems and line-of-business applications, are equally relevant to litigation, and tend to constitute a large volume of the total information that IT can be called upon to deliver in response to legal enquiries, usually at short notice.

Express regulatory requirements are not the whole story – the proliferation of media types and the growth in their use, gives companies a range of their own reasons for wanting to control and possibly preserve information created outside their own IT environment.

The role of forecasting in influencing case outcomes

In every litigation case, both parties have choices they can make throughout the process, before the case reaches the court. These decisions are more often driven by economic considerations than by principle.

Being able to forecast the case costs, continually and accurately, based on previous experiences, current facts and speculative outcomes, gives both parties the intelligence they need to make informed decisions. Claimants can decide to abandon the claim early because of projected costs; defendants may negotiate earlier settlements out of court to minimise their exposure; both parties can approach the Case Management Conference much better prepared to control the scope of disclosure by being able to calculate, often on the spot, what burden will be placed on them by a proposed change of scope by the opposite party. Any of these decision points can radically alter the direction of the claim.

Forecasting tools give the legal department a broader visibility of actual and projected costs across multiple cases, allowing them to negotiate more favourable terms with external counsel and other third parties. In addition, it allows them to improve their financial planning by knowing exactly when the peaks in case costs are likely to occur. This may in turn affect strategic and tactical decision-making.

The proactive implementation of a structured information governance system gives the legal department the tools they need to collect and analyse historical case information based on cost, time, resources and other metrics. Based on these metrics and with clear visibility of the information sources, data formats, volumes and custodians across the organisation, the tools are able to forecast the impact that alternative decisions will have on the case outcome.

Defensible disposal as a cost and risk management tool

The cost of disclosure is a function of the volume of information to be analysed, the selection criteria applied, and the choice of internal or external legal advisers who assess it.

By introducing detailed retention schedules across all enterprise information sources – documents, emails, media, transactional data, and others – and by automating the consistent execution of disposition cycles, redundant and obsolete information is purged and the overall volume of information held by the organisation can be substantially reduced. As a result of this discipline, when the need for electronic discovery arises, the volume of information that needs to be analysed is correspondingly reduced, minimising the disclosure costs.

There are fundamentally three types of information which need to be retained by organisations: information which has retention rules applied through regulatory compliance, information which must be retained because there is a legal duty to preserve it, and information which is actively used and required by the business to operate.

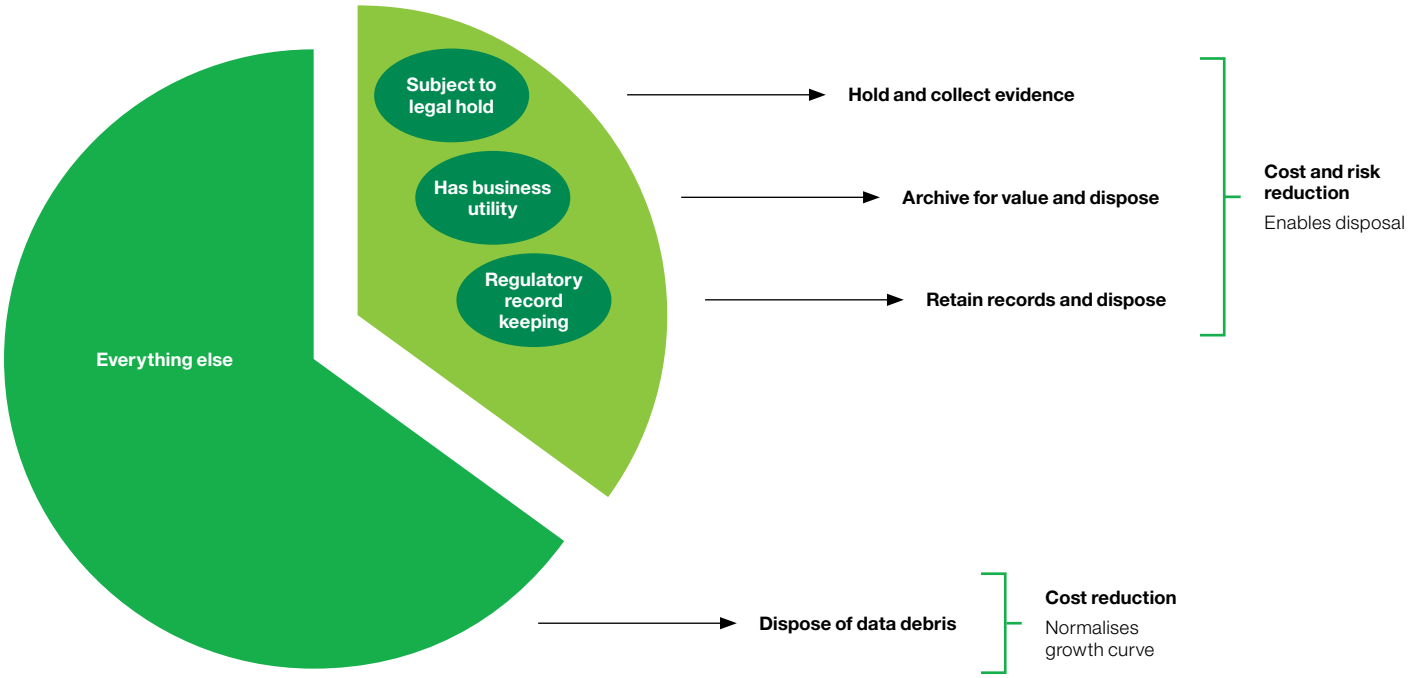

Figure 2: Enterprise information – retention requirements

Information governance gives organisations the tools they need to effectively "tag" all corporate information with one or more of these retention bounds and execute regular disposal cycles. The net effect of this process is that any information that remains "untagged" is, by definition, not essential and can therefore be defensibly disposed of by the IT organisation. This process is also referred to as 'defensible disposal'.

Being able to reduce, methodically and justifiably, the total volume of information held by the organisation significantly reduces the cost of discovery. It also gives the legal department a higher chance of identifying both relevant and irrelevant information much earlier in the litigation process.

Key steps towards adopting better information governance

It becomes vital for companies to identify the person or persons to take charge of all this, not just with responsibility for keeping and finding it when required for eDisclosure purposes and for other essentially defensive purposes, but also for maximising its business value.

This paper does not purport to cover the full range of steps which can and should be taken within organisations to identify and mitigate the risks. A basic list would include the following considerations:

- Make a senior appointment of someone with an overview of business, legal, compliance and IT.
- Identify recurring issues and the identifiable costs of managing them.
- Focus on an incremental approach rather than fighting on every front at once - that is part of the reason for starting by identifying pain points and cost headaches.
- Identify the wider company strategies to which these policies will be servants. This obviously includes those (generally in legal, compliance and IT) who are expected to react to eDiscovery and analogous events, but extends also to business units, marketing and others who create and use information.
- Discuss plans with the lawyers, accountants and consultants with whom the company normally works. This does not necessarily imply a major consulting exercise with each of them, but it is important to get their input (and perhaps their buy-in) to proposals which affect them. They are likely to have seen similar situations before.
- Perhaps redefine your expectations of these third parties, discarding those who do not have a proactive plan that brings benefit to the company.
- Talk to regulators, to the tax office and others who set external expectations.
- Consider a partnership with a provider who understands both your business and the end uses of the information.

Conclusion

Proactive information governance is both a strategy and a discipline. It provides the line of business groups, the legal department and the IT organisation with the tools they need to:

- Understand and document the information retained by the organisation and the reasons for retaining it.
- Enforce disposition policies across all types of corporate information.
- Automatically and defensibly remove redundant and obsolete information.
- Reduce the volumes of data which need to be assessed for disclosure.
- Arm the legal group with better negotiating and decision-making tools.
- Forecast legal costs and analyse the impact of different legal strategies.

For organisations which anticipate litigation, whether that is based in the UK, the US or across multiple jurisdictions, implementing a proactive information governance framework is critical for reducing both the costs and the risks involved.

Litigation is only one of the potential events whose costs, risks and other implications are relevant in this context. The same tools and processes serve multiple purposes in most large organisations, giving legal, compliance, IT and the other business units the same motives to consider a proactive approach to information governance.

About the author

Chris Dale qualified as an English solicitor in 1980 after reading History at Oxford University. He was a litigation partner in London and then a litigation software developer and litigation support consultant before turning to commentary on electronic disclosure/discovery. He runs the e-Disclosure Information Project, which disseminates information about the court rules, the problems, and the technology to lawyers and their clients, to judges, and to suppliers. He is a member of Senior Master Whitaker's Working Party, which drafted the new Practice Direction and Electronic Documents Questionnaire. He writes the UK's only authoritative and objective web site and blog on the subject and is a well-known speaker and commentator in the UK, the US and other common law jurisdictions.

For more information

To learn more about IBM Enterprise Content Management and information governance solutions, please contact:

Trushar Javia
Email: jtrushar@uk.ibm.com

ibm.com/software/ecm/disposal-governance

1 http://edisclosureinformation.co.uk/edisclosureproject.htm

2 http://www-01.ibm.com/software/ecm/disposal-governance

3 http://www.fulbright.com/index.cfm?fuseaction=news.detail&article_id=7637&site_id=286

4 http://www.justice.gov.uk/downloads/statistics/courts-and-sentencing/judicial-court-stats.pdf

5 http://www.fulbright.com/index.cfm?fuseaction=news.detail&site_id=286&article_id=9907

6 US companies in fact have a "safe harbor" given by Rule 37(e) FRCP in respect of data not the subject of a legal hold and properly deleted pursuant to a policy that is both established and followed. The fear of sanctions, which drives so much excessive discovery, is largely misplaced. Since Zubulake v UBS however, the norm is to keep everything. What is described here therefore, is the de facto position rather than a strict statement of US obligations.

7 UK Bribery Act 2010 - http://www.legislation.gov.uk/ukpga/2010/23/contents

8 http://www.justice.gov.uk/guidance/courts-and-tribunals/courts/procedure-rules/civil/contents/parts/part31.htm

9 http://www.justice.gov.uk/guidance/courts-and-tribunals/courts/procedure-rules/civil/contents/practice_directions/pd_part31b.htm

10 Morgan J in Digicel v Cable & Wireless http://www.bailii.org/ew/cases/EWHC/Ch/2008/2522.html, quoting Jacob LJ in Nichia v Argos http://www.bailii.org/ew/cases/EWCA/Civ/2007/741.html

11 http://www.bailii.org/ew/cases/EWHC/QB/2009/B41.html

12 Rybak v Langbar http://www.bailii.org/ew/cases/EWHC/Ch/2010/2015.html

13 Al Sweadi v Secretary of State for Defence http://www.bailii.org/ew/cases/EWHC/Admin/2009/2387.html, where the government paid £1 million in indemnity costs and had to withdraw its opposition to the claim as a result of its failure to meet disclosure obligations; the court criticised a named officer as well as the department and its lawyers.

14 http://www.bailii.org/ew/cases/EWHC/Mercantile/2009/2500.html

15 Finanical Industry Regulatory Authority - http://www.finra.org/

16 FINRA Regulatory Notice 10-06 "Social Media Wed Sites" January 2010

IBM United Kingdom Limited
76 Upper Ground
South Bank
London
SE1 9PZ

Produced in the United Kingdom
June 2012

ZZW03113-GBEN-00