

Advantage

NAVIGANT FORENSICS ADVANTAGE
JULY 2011

Welcome	2
Losing data; Losing public confidence	3
Overview of Federal Rules of Civil Procedure as it pertains to eDiscovery	6
Dealing with data across multiple jurisdictions	10

Welcome



Phil Beckett

Director of Forensic Technology
+44 (0)20 7469 1192
phil.beckett@navigant.com

Technology continues to impact our world in a growing and increasingly unpredictable way. Be it the US declaring that cyber-attacks will be classed as an act of war or the more mundane super-injunction debacle and how Twitter became instrumental in leading the debate. I am afraid our newsletter will probably not feature on the BBC News website, but I hope it will provide commentary and insight into the hottest topics in the forensics and discovery industry.

So, a very warm welcome to the inaugural issue of Forensic Advantage, a quarterly newsletter from Navigant's Forensic Technology practice.

In our first issue, we have featured three articles that illustrate different perspectives of data privacy, how they come into conflict and how this can be managed.

- » Our first article, written by the former Information Commissioner, looks at the risks of losing data.
- » Our second article highlights the attitude towards discovery in the US and how that has a global impact.
- » Our final article describes the European-perspective on data privacy and describes how having flexible yet sophisticated solutions can help organisations manage any conflict between privacy and data requests.

I hope you enjoy our first issue. I welcome all feedback. If you've received this issue indirectly from someone else, and would like to receive future newsletters directly, please click on the "Subscribe" feature and we will gladly add you to our distribution list.

Kind regards,

Phil Beckett

Losing data: Losing public confidence

"The Minister would like a quick word". That invitation in late 2007 – arriving as I exited from a heavy session giving evidence on a completely different subject to a House of Lords Select Committee – kicked off the "Government Data Loss Saga". In a cramped office in the Commons at the other end of Parliament, the Minister responsible for Her Majesty's Revenue and Customs told me in confidence – almost in a whisper - that HMRC had lost two discs containing the Child Benefit details of 25 million people. "I never knew you could get so much data onto two discs". When I saw the Chancellor of the Exchequer, Alistair Darling, at the Treasury the next day, his face was no less ashen. Politicians – and their civil servants - were quick to appreciate the reputational damage, despite lacking any detailed knowledge or direct responsibility for what had happened in a remote office in the North-east of England. The buck stopped at the top and they knew it.

I was then the Information Commissioner, responsible for data protection, and they knew they had to report the loss to me and seek our advice. We were clear that, although there was no legal obligation, the public had to be told and the banks had to be involved. The main risk – especially if the discs were to fall into criminal hands - was that bank account details would be exploited. We were prepared to allow a few days for the banks to take precautionary measures and to allow a little more time for HMRC to search for the discs. But transparency, and rebuilding public trust and confidence, were paramount.

Sadly, the next few weeks brought an avalanche of further stories about lost personal data. 3 million learner drivers whose details had been lost by a processor in the USA, 600,000 military recruits, numerous health records, the entire prison population, laptops here, memory sticks there. Anyone involved in investigating where and how data has gone astray is faced with the challenges of checking data and audit trails which are only as good as the original design. Too few senior managers are aware of the consequences when control is lost – or perhaps never properly existed in the first place.

And too few managers know that there are tight controls on passing on data from one organisation to another, especially when sending it outside the EU. Many of the governmental losses and compliance failures only came to light when checks were made as follow-up to the initial problems. But by then the government was on the back foot and public confidence in the ability of government to safeguard their personal details fell to an all-time low.

A plethora of reports and actions documented how things had gone so badly wrong. The investigations were rigorous, but were never able to discover where the missing data had got to. Did the child benefit data reach criminal hands? Did the laptop thief appreciate the sensitive and value of what he had stolen? How extensively was the personal data of so many people

Richard Thomas CBE
Adviser, Centre for Information
Policy Leadership
Hunton & Williams

UK Information Commissioner
2002-9

actually disclosed? Even if the answers to these and other questions could not be established, lessons had to be drawn. Kieron Poynter, senior partner of PriceWaterhouseCooper, documented the managerial, technological and supervisory failures inside HMRC. Sir Edmund Burton, a retired General and expert in Information Assurance, probed the reasons for the loss of the military service records. The Cabinet Secretary looked across the Whitehall as a whole and produced a comprehensive package of reform. The Prime Minister asked me and Mark Walport (Chief Executive of the Wellcome Trust) to undertake a review of data-sharing. My Office took formal enforcement action against HMRC and the Ministry of Defence, to turn the recommendations of the reports into binding obligations.

All the reports made similar points. Data Protection really does matter. It is not a nerdy subject, remote from real life. The Data Protection Principles are inter-connected and set out good practice which no-one can afford to ignore. They include, for example, purpose limitation, limited retention periods and security. This was illustrated well by Sir Edmund Burton's report which looked far beyond the stupidity of one man leaving a laptop in a car. Why in the first place was so much data collected on 600,000 people, many of whom had done no more than express an interest in joining the armed forces? What purpose was being served? Why was the data kept so long – up to 10 years in some cases? Why was it all loaded on to a single laptop? Why weren't laptops encrypted?

Next, getting it right always involves three key strands – the right approach to policies and procedures, the right approach to Information Technology and the right approach to people. The last is probably the most difficult, but – as the weakest link - the most important. All staff handling personal data (which is now most staff in most organisations) need to be made aware of the risks and to be trained in good practice, and there needs to be organisational and personal accountability at a sufficiently high level. It is no longer acceptable to dump data protection into the hands of the lawyers, the IT department or any other silo. It is the classic horizontal subject which pervades all activities relating to people – whether they are customers, citizens, suppliers or employees. Small wonder that the Cabinet Secretary's report led to training requirements for every single civil servant, to a complete overhaul of IT security and to far-reaching governance reforms, such as appointing a Senior Information Risk Officer (SIRO) for every department and featuring data security on the agenda of all Audit Committees and in annual Statements of Internal Control.

I have not concentrated on governmental data losses because the public sector is worse than the commercial or voluntary sectors. Plenty of horror stories came my way from High Street names, from lesser-known businesses, from NHS hospitals, from local authorities and from charities. But it was at central government level that we have the fullest and frankest accounts

of what can go wrong, what does go wrong and what needs to be done. And the high and continuing profile – in media and political terms – demonstrated how the public care and how painful - not least in reputational terms - it can be when the chickens come home to roost. If nothing else, the last few years have brought home the need to understand what personal information you are handling, the consequences if things go wrong and the need to take quick investigatory and remedial action where unauthorised disclosures do occur.

The data loss saga brought home the value of data-mapping, risk management, "privacy by design" techniques and Privacy Impact Assessments. Data protection now affects virtually every organisation of whatever size or sector. Even the smallest organisation can now process vast amounts of sensitive personal data. The digital age - with powerful devices, instant wireless, mobile and fixed communications, open networks, more effective search and analytical tools and ever-cheaper data storage capacity - creates seemingly endless opportunities to gather and interpret information about us, our activities and our preferences. Data about anyone can be easily copied and aggregated around the world across vast, interconnected networks.

Data protection must also be modernised. It has perhaps been too theological in the past. The Centre which I now advise at Hunton & Williams argues for a genuinely 21st Century regulatory framework with clear objectives focussed on real threats and risks. The new framework must ensure a good balance between the benefits and the harms of processing personal data. It must avoid stifling innovation by being technologically neutral and future-proof. And it must be internationally compatible, or at least inter-operable.

The sad truth is that scandals are needed to wake up those who need to act. But once public confidence is lost it can be very hard to re-gain. This can be damaging for governments, but fatal for businesses.

During my time as Information Commissioner, data protection certainly came of age. But do any of us as citizens and consumers really know what is happening to our data? And how many of us in the business community know what we should and should not be doing with so much data at our fingertips?

Overview of Federal Rules of Civil Procedure as it pertains to eDiscovery



Aaron Philipp
Associate Director
San Francisco
+1 415 356 7149
aaron.philipp@navigant.com

Electronically stored information remains one of the more daunting and distracting aspects of litigation life. How corporations and their counsel deal with electronically stored information prior to and during litigation can – and usually does – dramatically impact the course of the litigation and increase the costs of prosecuting, defending, and ultimately resolving claims.

In December of 2006, the Federal Rules of Civil Procedure were amended to reflect the fact that an overwhelming majority of information requiring discovery in litigation is electronic. Electronically Stored Information (or “ESI” as it is more commonly referred to today) was included in the amendments to make it clear that ESI is discoverable. The Federal Rules of Civil Procedure Amendments from 2006 imposed a new set of burdens and created a new set of obligations that materially impacted the litigation landscape.

Some of the key rules as it pertains to Discovery are:

Rule 26 (a)

Under Rule 26(a), prior to any discovery request a party must provide other parties with:

“a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things” in its possession that it may use to support its claims and defenses.

Rule 34 (a)

Rule 34(a) was amended to remove any vagueness or ambiguity over what constitutes a discoverable document. Specifically, the word “Document” includes any designated documents or “electronically stored information” or any designated documents “stored in any medium” from which info can be obtained. The word “Document” includes e-data unless specifically distinguished.

Rule 34 (b)

This rule Permits requesting parties to request the format in which they would like to receive electronically stored information. Specifically, the rule states:

- » If objection is made or no format requested, then producing party must state the form(s) it intends to use.
- » If form not specified, responding party must produce as ordinarily maintained or in reasonably useable form
- » Absent order, party only needs to produce the same information in one form

Rule 26(f)

- » Requires parties to develop a proposed discovery plan concerning any issues relating to:
- » identification and disclosure of electronically stored information
- » scope of electronic discovery (e.g., topics, time periods, sources of data, use of search terms, whether information is “reasonably accessible,” etc.)
- » preservation
- » production formats
- » agreements for assertion of privileges after inadvertent production

Rule 26(b)(2)

Accessible vs. Inaccessible

- » A party need not provide discovery of ESI from sources that the party identifies as “not reasonably accessible” because of “undue burden or cost.”
- » A party claiming that ESI is not reasonably accessible has the burden of proof; that party may move for a protective order.
- » Even if the burden is met, the court may still order discovery if the requesting party shows “good cause.”
- » If discovery is ordered, the court may set conditions and reallocate costs.

Rule 26(b)(5)

- » If information is produced that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it.
- » After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved.
- » A receiving party may promptly present the information to the court under seal for a determination of the claim.
- » If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it.
- » The producing party must preserve the information until the claim is resolved.

Rule 37(f)

“Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

U.S. Based Litigation with European eDiscovery Components

As electronic discovery has matured, relevant electronic records have been sought not only domestically but internationally, this has created unique challenges related to privacy, security, and data export. Unfortunately, the challenges often vary by jurisdiction.

The U.S. courts have found that a foreign based party to litigation is required to comply with Discovery requirements under the Federal Rules of Civil Procedure. Specifically, the *Societe* and *Reino de Espana* cases highlight the court's position on this.

Reino De Espana v. Bureau of Shipping, et al, 1:03-cv-03573 SD NY

Reino de Espana brought the action, in relation to Prestige sinking off the coast of Spain on November 2002, against American Bureau of Shipping. During the course of the litigation, ABS sought sanctions for Spain's alleged spoliation of material evidence.

As background, ABS served Spain with a document request seeking, among other things, the production of email communications and other electronic records concerning the handling of the Prestige casualty. Spain made no objection to the production of electronic documents, and disclosed some responsive documents. In July of 2004, ABS notified Spain that its discovery production was deficient, and clarified that it sought electronic records from approximately thirteen different government ministries. Spain objected to ABS's request as overbroad and unduly burdensome, and maintained that it had already produced all non-privileged responsive records. Nevertheless, ABS renewed its request for responsive emails and electronic records. At that time, Spain represented that it would ensure that all non-privileged responsive records were produced.

In January of 2005, ABS narrowed its discovery request by asking Spain to limit its search of responsive emails and electronic records to approximately ninety-eight names and fifteen government email addresses. Spain rejected this request on the grounds that it constituted a fishing expedition, and that the computers of government officials are subject to Spanish privacy laws and government privileges, and cannot be searched without the individual user's consent.

In October of 2005, ABS moved to compel further production of electronic discovery. After a two-day evidentiary hearing, the Court ordered Spain to complete its forensic search for email records that the Court has concluded are relevant, and to produce these records to ABS on a rolling basis and was not able to stand behind the local privacy law to prevent search and production of ESI.

Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522

The government-owned French manufacturer of an aircraft that crashed in Iowa sought a protective order in a U.S. District Court action filed on behalf of persons injured in the crash. The manufacturer claimed that discovery from the manufacturer of documents in France had to be sought under the Hague Evidence Convention rather than under the Federal Rules of Civil Procedure.

The Court decided that it would not adopt a rule that U.S. litigants had to resort to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters before seeking discovery against foreign litigants under the Federal Rules of Civil Procedure. The Hague Convention does not prevent a U.S. District Court of jurisdiction to order production of documents located abroad. The Court also ordered that discovery of documents in foreign countries to take into account any special problems of a foreign litigant in providing discovery due to its nationality, location of the documents, or sovereign interests.

Looking at these two cases and others, there are a number of key themes that can be deduced that illustrate the court's general attitude to European aspects of eDiscovery, they are:

- » If a party comes voluntarily to the US (for example to do business) then they are more likely to be ordered to produce records, as opposed to a purely European-based party;
- » The courts will value foreign government statements highlighting the issues with data protection and privacy, however, if they do not make these then the courts are likely to give these issues less weight; and it is only where there is a real risk will the discovery request be denied;
- » Generic blocking statues where the aim is to simply block all data will carry less weight than specific legislation (e.g. bank secrecy laws);
- » It is on the party opposing the inclusion of European documents in a Discovery request to prove why this violates European law, specifically;
- » If the producing part shows that the requested documents have been produced from a US source then the court will take this into account; and
- » If the producing party is using documents from the European jurisdiction for their own case, then the Court will not take kindly to them trying to prevent discovery of documents from this jurisdiction.

Dealing with data across multiple jurisdictions



Phil Beckett
 Director of Forensic Technology
 +44 (0)20 7469 1192
 phil.beckett@navigant.com

Privacy legislation and the demand for documents to satisfy litigation and/or regulatory requirements can often come into conflict. Technology, however, when applied in an intelligent and flexible manner can provide a solution.

As the world continues to globalise, and with technology meaning that people can work efficiently regardless of location, data is becoming ubiquitous. This is being increasingly recognised by courts, organisations and regulators here in the UK, in Europe and the rest of the world, most notably America. It is important, however, to recognise other competing forces that are designed to protect individuals' privacy, especially in Europe.

Both the European Convention on Human Rights (ECHR) and the European Union Directive 95/46/EC ("the Directive") have privacy at the heart of their agenda. Article 8 of the ECHR states explicitly that 'Everyone has the right to respect for his private and family life, his home and his correspondence', and although this strictly only applies to public authorities, the horizontal effect means that every organisation needs to take note. In addition, the drivers behind the Directive included the "protection of individuals with regard to the processing of personal data and recital (2)". This makes it clear that when processing data, the practice must respect the right to privacy.

What is apparent is the obvious conflict between privacy-related laws and the need to process data (in its widest sense) in respect to litigation, disputes, investigations and regulatory matters. This has been recognised in a document generated by the Article 29 Data Protection Working Party on pre-trial discovery for cross-border civil litigation. It includes the following points:

- » "...the Working Party considers that it is unlikely that in most cases consent would provide a good basis for processing." – this is because they do not consider it to be freely given, where the individual has "...a real opportunity to withhold his consent without suffering any penalty, or to withdraw it subsequently..."
- » "...controllers should restrict disclosure if possible to anonymised or at least pseudonymised data. After filtering ("culling") the irrelevant data – possibly by a trusted third party in the European Union – a much more limited set of personal data may be disclosed as a second step."
- » "Where the transfer of personal data [to third countries] for litigation purposes...[and] a significant amount of data is to be transferred the use of Binding Corporate Rules or Safe Harbor should be considered. However, the Working Party reiterates its earlier opinion that Art. 26 (1)(d) cannot be used to justify the transfer of all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought one day in US courts."

Before going on, it is important to note that:

- » The ECHR and the Directive have both been implemented across Europe, though with slightly different nuances and interpretations; and
- » These are not the only legislative measures that impact data, for example; in certain countries

interception of communications legislation needs to be considered.

However, I am not a lawyer and would not seek to give any sort of legal advice, needless to say it is important that it is sought when dealing with data in different jurisdictions.

What is essential is the need to have a flexible, scalable and robust solution in place to deal with the multitude of options available to organisations; both to allow them to comply with their legal duties to the Court and/or regulator, as well as satisfying the requirements of privacy-related legislation. This solution is most easily presented through the use of case-examples showing how a solution can be crafted to meet these challenges:

- » Working in respect of an internal corruption enquiry, our solution was deployed to ensure all data was successfully captured in a forensically sound manner, processed and searched on-site, before responsive documents were extracted to the UK to be hosted for legal review. All data, other than that which was responsive, remained in the control of the client on encrypted drives in secure storage, should the case warrant a further analysis.
- » Responding to a US-based litigation, a solution was implemented on a client site in mainland Europe which allowed for the entire review process to be carried out on-site. This included hosting a team of lawyers able to review documents and ensure that only those necessary for the case were extracted to the US.
- » As part of an investigation into allegations of intellectual theft and fraud, our solution was deployed and allowed the data to be captured, processed and reviewed on-site. The review was carried out in order to identify any responsive documents that contained private-information. All data was then redacted, before the responsive documents were sent to the US for a more thorough legal review.
- » In respect to a regulatory-enquiry, we were able to deploy to over twenty countries and securely capture all relevant data on-site. This was then filtered according to date range and file-type, before being returned to the UK for further analysis and ultimately hosting for legal review.

The differing implementations of European legal initiatives, along with diverse attitudes in different countries to enforcement and sanctions, mean that there is no straight-forward solution that meets all requirements every time. In most cases, a 'view' will need to be taken as to what processes are carried out, where they are carried out, and how they are reasoned.

It is important to have the technical resource, infrastructure and flexibility to enable all of these requirements to be met, regardless of the nuances involved. This needs to be done in an efficient and cost-effective manner, without losing any of the sophisticated review and processing features available such as; linguistic and relationship analysis, near de-duplication and e-mail threading, as well complex and transparent search features. Technology, when implemented intelligently, can greatly assist organisations meet these conflicting challenges.



www.navigant.com

DISPUTES & INVESTIGATIONS • ECONOMICS • FINANCIAL ADVISORY • MANAGEMENT CONSULTING

©2011 Navigant Consulting, Inc. All rights reserved. Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See www.navigantconsulting.com/licensing for a complete listing of private investigator licenses.