ACCESSDATA

WHITE PAPER


# UK Telecommunications Companies Leverage Software Tools to Manage Large Data Collections in Litigation and Government Investigations

UK companies in every major industry are at risk for cybersecurity intrusions and the telecommunications industry has learned they are especially vulnerable. The major data breach that hit TalkTalk in 2014—in which approximately 21,000 customers had their personal data compromised—continues to ring alarm bells for telco executives in the UK.

*The Guardian* reported that class action litigation may be in the works, pointing to a meeting of lawyers representing about 50 TalkTalk customers who were defrauded by cybercriminals after having their data breached. Moreover, the Information Commissioner's Office (ICO) recently concluded a lengthy government investigation into TalkTalk's data security practices, imposing fines and issuing a report that was critical of the company's efforts to safeguard customer data.

Of course, this risk is neither unique to data breaches in the UK, nor to industries that serve consumers directly. Equifax, the U.S.-based credit reporting company, recently confirmed a massive cybersecurity incident that may have exposed as many as 400,000 people in the UK to having their personal data stolen. This data includes names, dates of birth, email addresses and telephone numbers—rest assured the litigation and government investigations are heating up already.

## Rise of Litigation and Investigations

In addition to the risk of financial fraud that can impact individual consumers, data breaches are now serious risks to UK corporations on many levels. One element involves how a company that has suffered a breach handles the identification, notification and remediation phase of the incident. This is more than just a matter of sound business ethics, it's now codified in a regulatory regime of its own.

For example, the General Data Protection Regulation (GDPR) contains all sorts of rules to govern the way personal data is protected within the EU and is exported beyond the EU's boundaries. As part of that GDPR compliance, the ICO is currently developing clear guidance that will set out when organisations should be reporting, and the steps they can take to help meet their obligations under the new data breach reporting requirement.

> it's more common now for an organisation to be served with a regulator's demand to produce internal evidence in response to an enquiry … and to do so on very short notice, sometimes as little as 48 hours.

"The public needs to have trust and confidence that a regulator is collecting and analysing information about breaches, looking for trends, patterns and wider issues with organisations, sectors or types of technologies," said Elizabeth Denham, Information Commissioner at the ICO. "It will help organisations get data protection right now and in the future."

This rising regulatory pressure on UK companies—starting with the telecommunications companies that have already drawn the ire of the ICO—has resulted in a new compliance landscape. It has even touched off a number of interesting legal disputes about how the compliance duties of telecom companies may differ under the law from the duties of private software companies, as we saw played out in Belgium when authorities sought call records from Skype.

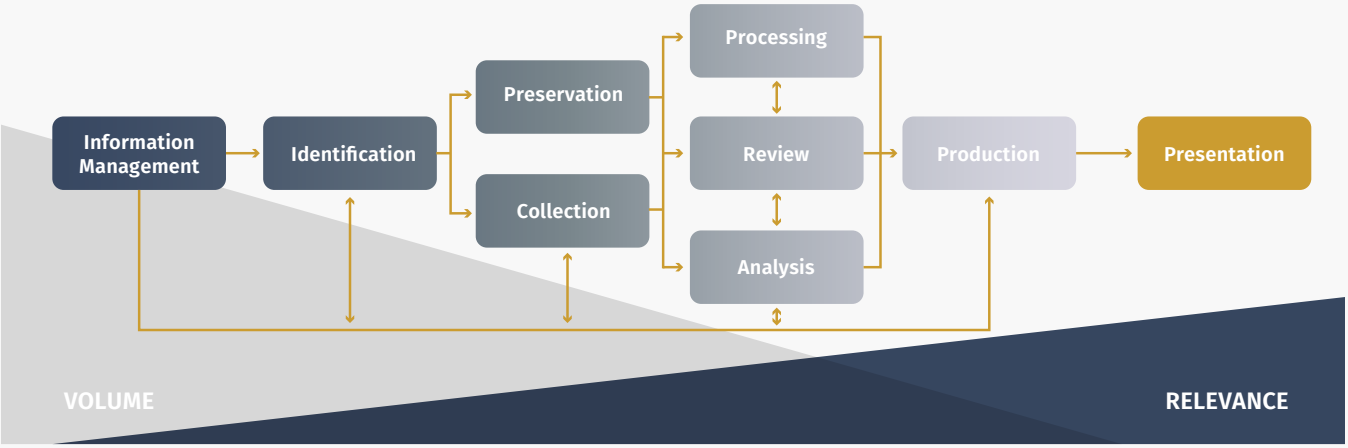
## Technology to the Rescue

Regardless of the event that precipitates the litigation or investigation, it's more common now for an organisation to be served with a regulator's demand to produce internal evidence in response to an enquiry … and to do so on very short notice, sometimes as little as 48 hours. Given the realities of the information age in which we now live, this evidence—typically, correspondence between company executives and other corporate documents—consists of electronic data that resides on email servers and other data repositories.

UK corporate executives are increasingly turning to technology tools that can help meet their compliance obligations to review vast troves of electronic data and produce responsive evidence in the event of a litigation or regulatory enquiry. Specifically, they are relying on the use of electronic discovery (e-discovery) software in order to deal with huge amounts of data and to extract relevant information.

Electronic discovery software collects, extracts and organises the data from all kinds of servers and devices. Importantly, these tools allow in-house teams to discreetly conduct an e-discovery project—collect sensitive data, search for the responsive evidence needed and produce it to the regulators—without involving too many internal or external professionals who might not need to know about the enquiry that is underway.

Some organisations actually use three or four different products throughout the e-discovery workflow, which requires the data to move from one tool to the next. But many UK corporate executives have discovered the benefits of cost-efficiency and risk management that can be realised by using a single software platform to manage the entire spectrum of evidence collection, processing, review and production.




*Traditionally, no matter which tools an organization uses to address the EDRM at a minimum the data must be identified, then collected, processed for analysis, internally reviewed and culled—and then that reduced data set must be processed again for import into a legal review tool for outside counsel.*

## The E-Discovery Workflow

There is a comprehensive model that is commonly used to support e-discovery requirements in the complex commercial litigation that is prevalent in the U.S. and we're increasingly seeing more components of that model show up in the UK as well.

Here are the key steps in the e-discovery workflow that are important for UK corporate teams to understand in order to better meet their compliance obligations in response to regulatory enquiries:

### Data Collection

Collection is a crucial part of the e-discovery process and corporate teams should leverage the power of software tools to quickly gather the universe of potentially relevant data from their various information systems. For example, the right e-discovery software products can ensure data is not being altered, dropped or missed during collection.

While certainly not a requirement, forensic data collection capabilities are especially valuable in an e-discovery software solution. Forensic collection has important advantages, as well as heightened defensibility, including the ability to audit the collection and the ability to collect deleted files. In other words, an organisation that uses an e-discovery software tool with forensic collection capability not only chooses the strongest level of collection stability, but also shows regulators that it's at the front of a developing trend in compliance.

### Processing

The processing phase is the real workhorse of any good e-discovery software tool. Within this phase, all data that was collected previously gets extracted and turned into information that can be culled down for greater relevance. As such, speed and accuracy are at a premium and the ideal software solution should be one that can easily and affordably scale using existing hardware to achieve fast processing speeds.

As always, the best advice is to run a thorough proof of concept test with your own sample data set and a full understanding of the service level objectives when responding to a regulatory enquiry. The single criterion that varies the most across e-discovery vendors is accuracy, so make sure you're using a tool that has a proven track record for not only speed and culling rates, but also thoroughness and accuracy of its processing engine.

### Review and Analysis

The analysis phase of the e-discovery process entails taking the large and unorganised set of data from the processing phase to determine what electronic evidence you have that will be responsive to the regulatory demand you received. The best e-discovery software tools help you get this done quickly by categorizing, refining and bucketing data.

The most well-known functions are keyword searches and culling. All software applications and support processes should have an efficient and effective method for using keywords to analyse and reduce the subject corpus of data down to a manageable subset. In addition, your software should be able to quantify and present which documents did and did not meet your search criteria. These reports and metrics are critical input to note as they can influence whether or not you'll need to perform additional collections as the investigation develops. Reporting can also help to quickly determine if chronological or conceptual gaps exist in the current data set.

### Evidence Production

Production completes the arc of the e-discovery process. The way data gets out of a system is a key part of the production process and you should be able to export it from the system in various formats without incurring an additional expense or using a third-party application.

Production includes much more than just printing documents out or emailing a batch file to the government investigative team. For example, today's productions come in many formats and some may never see paper, so your e-discovery software has to be capable of handling not only the traditional production duties of redacting, printing and numbering—but be able to produce data in its many formats and iterations. Having said that, the UK and EU regulatory worlds are far from giving up on paper, so your software tool should also make it easy to click and print.

## Conclusion

Telecommunications companies in the UK have been forced to confront their exposure to cybersecurity incidents and other emerging online data management challenges. These are not only serious business threats, but they also involve the risk of potential litigation and government investigations.

Faced with the daunting challenge of responding to high-stakes enquiries under tremendous time pressure, UK telecom companies are embracing a new set of technology tools to help them meet these demands. Specifically, the use of e-discovery software, like AD eDiscovery®, is increasingly becoming commonplace in the UK as a way for making it easier to organise and access data involved in time-sensitive compliance matters demanded by commercial litigation or government investigations.



**Visit us online:**

**www.accessdata.com**

**Global Headquarters**
+1 801 377 5410
588 West 300 South
Lindon, Utah

**North American Sales**
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

**International Sales**
+44 20 7010 7800
internationalsales@accessdata.com