Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: Practice Guide

DIGITAL DATA COLLECTIONS IN ACCORDANCE WITH THE DISCLOSURE PILOT SCHEME

By Sophie Beattie, EnCE, CDFE, Certified GDPR Practitioner
Senior Director - Forensic Investigation and Expert Witness Services, Consilio

Consilio Institute: Practice Guide

DIGITAL DATA COLLECTIONS IN ACCORDANCE WITH THE DISCLOSURE PILOT SCHEME

TABLE OF CONTENTS

Disclaimers

The information provided in this publication does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this publication are provided for general informational purposes only. While efforts to provide the most recently available information were made, information in this publication may not constitute the most up-to-date legal or other information.This publication contains links to third-party websites. Such links are only for the convenience of the reader; Consilio does not recommend or endorse the contents of the third-party sites.

Readers of this publication should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this publication should act or refrain from acting on the basis of information in this publication– without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

Use of this publication, or any of the links or resources contained within, does not create an attorney-client relationship between the reader and the author or Consilio. All liability with respect to actions taken or not taken based on the contents of this publication is expressly disclaimed. The content of this publication is provided "as is." No representations are made that the content is error-free.

SUMMARY

The preservation and collection of electronically stored information (ESI) is the foundation of any disclosure exercise. Any doubt cast upon the integrity of evidence gathered and produced can have a costly and negative impact to your case.

The gathering of ESI must be conducted in accordance with the Practice Direction 51U - Disclosure Pilot Scheme.[1] The Disclosure Pilot scheme is in place to assist parties and ensure a proportionate approach to the matter is taken. The Disclosure Pilot governs your disclosure, sets out the relevant duties of all parties involved, and specifically lays out requirements in relation to the preservation of ESI in order to produce relevant "documents."

Within the Disclosure Pilot, the definition of a "document" is open-ended and intentionally wide. Traditional paper documents, as well as digital documents, audio files, picture files, and video files stored on any available device or platform are to be identified and potentially investigated for relevancy to the matter. This also includes the metadata of documents and files, meaning data should be collected and preserved in a forensically-sound manner.

A data mapping exercise should be conducted to generate a defensible and comprehensive list of places that ESI could be or has been stored. This process is assisted and logged by a document known as the Disclosure Review Document. Data preservation exercises should be considered and carried out as soon as possible to ensure ESI of possible relevance is not changed or deleted during general day-to-day business activity.

The Disclosure Pilot highlights that reasonable efforts should be made to avoid non-relevant ESI being disclosed. During the data mapping phase, an assessment should be made of each data source available to determine its likelihood of containing relevant and disclosable information.

Culling data is best conducted post collections, using industry-standard eDiscovery or Digital forensic tools. This is to ensure that potentially relevant documents are not missed and all available data such as attachments, or archives are searchable. The process should be conducted with a defensible, recognised and repeatable workflow.

Legal advisors should coordinate efforts with their client and the eDiscovery provider as their first point of call to ensure that all potentially relevant ESI is preserved in a forensically-sound, defensible, and compliant manner to ensure it can be used in a court of law.

The Disclosure Pilot Scheme

Disclosure is an important part of litigation that involves identifying, collecting, and reviewing ESI and hard copy documents. The Disclosure Pilot Scheme was introduced on 1st January 2019 as set out in Practice Direction 51U of the Civil Procedure Rules within the Business and Property Courts of England and Wales. The scheme was initially introduced as a two-year pilot and is often referred to as "the Disclosure Pilot." As of 5th February 2021, the Disclosure Pilot was extended until 31 December 2022 with the intention of amendments being implemented by the disclosure working group after this time.

The aim of the scheme is for clients to take more time to plan how data is collected, searched, and reviewed, with the aim of eliminating much of the peripheral or wholly irrelevant material that has traditionally been part of pre-disclosure reviews. Paragraph 3.1(6) of the Disclosure Pilot highlights that parties are to use reasonable efforts to avoid providing documents to

[1] *Practice Direction 51U - Disclosure Pilot for the Business and Property Courts, available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-51u-disclosure-pilot-for-the-business-and-property-courts.*

another party that have no relevance to the Issues for Disclosure in the proceedings. In practice, these savings will not be made if data is over-collected from the start or targeted keywords or other search criteria are not applied to minimise redundant information.

The scheme includes a Disclosure Review Document or "DRD" (found in Appendix 2 of the Disclosure Pilot). In the simplest of terms, the DRD is a planning document utilised to identify key issues in the dispute and achieve an agreement on the scope of your disclosure exercise. The DRD, which replaced the legacy Electronic Document Questionnaire (EDQ), is a useful document in relation to the data preservation and collection phase of the disclosure exercise. The document, when complete, details custodians, data sources, and date range parameters that are deemed to be potentially relevant to the case.

Issues and Models for Disclosure

The Disclosure Pilot requires parties to identify and seek to agree Issues for Disclosure, defined as the "key issues in dispute, which the parties consider will need to be determined by the court with some reference to contemporaneous documents in order for there to be a fair resolution of the proceedings."

Each issue should have a model of disclosure assigned to it setting out the approach to disclosure on that issue. There are five models of disclosure:

- **A – Known Adverse Document Disclosure**
  - Parties do not have to disclose documents to support their own case if there is no relevant material to disclose but they cannot avoid the obligation to disclose any adverse documents of which they are aware. Parties are not under a pro-active obligation to conduct searches for adverse documents if they are not aware that any exist.
- **B – Limited Disclosure**
  - This is a non-search-based disclosure and will typically include documents on which the parties have expressly relied in support of their pleadings. As above, parties following this model are not under an obligation to search for material beyond the scope of the limited disclosure provided.
- **C – Request-led, Search-based Disclosure**
  - Typically, relevant for complex cases.
  - Searches are required and are typically agreed between both parties in the litigation or directed by the courts.
  - Model C requires an additional section 1B to be completed identifying the specific data sources and search criteria to be identified for each model C issue.
- **D – Narrow Search-based Disclosure (with or without Narrative Documents)**
  - Typically, relevant for complex cases.
  - This model is most familiar for disclosure; it is the model that is most similar to Standard Disclosure as followed prior to the introduction of the pilot.
  - Parties are required to disclose documents that may support or affect its claim or defence. This may or may not include narrative documents.
  - A narrative document is described as containing information relevant to the background or context or an issue but does not contain information related to the issue itself.
  - The court will dictate if narrative documents are required as part of the disclosure.
  - This model requires reasonable and proportionate searches to be conducted.
- **E – Wide Search-based disclosure**
  - This model is typically only ordered in exceptional cases.

- Disclosure is broader than model D and includes narrative documents, as well as documents that may lead to a train of enquiry.

Parties will agree on the model to be used for each issue, setting out the approach to disclosure on that issue. Models must be approved by the court and can be overruled where deemed necessary. Where parties disagree on the model to be used, the court will decide on the appropriate model and issue an order.

Preservation of Electronic Documents

The first step that legal advisors should take is to coordinate efforts with their client and their eDisclosure provider to ensure that all potentially-relevant material is identified and preserved in such a way that it can be searched, reviewed, and disclosed if relevant. The eDisclosure provider will help to identify cost-efficient methodologies and provide guidance and services to ensure potentially-relevant data is preserved in a forensically-sound, defensible, and compliant manner.

The term "document" is described within the Disclosure Pilot as any record of any description containing information. Paragraph 2.5 states a document:

- May take any form including but not limited to paper or electronic
- It may be held by computer or on portable devices such as memory sticks or mobile phones or within databases
- It includes e-mail and other electronic communications such as text messages, webmail, social media, voicemail, and audio or visual recordings

Paragraph 2.6 of the Disclosure Pilot, highlights that the term document extends to information stored on servers and back-up systems and electronic information that has been "deleted." It also extends to metadata and to other embedded data that is not typically visible on screen or from a print out. This open-ended definition of a document is intentionally wide to allow for the capture of all relevant data whether electronic or in hard copy.

Specific guidance is set out within the Disclosure Pilot in relation to the preservation and collection of ESI. For example, paragraph 3.1(1) highlights that a person who knows that it is or may become a party to proceedings must take reasonable steps to preserve documents that may be relevant to the proceeding.

Since parties have an obligation to begin preservation as soon as there is knowledge that a proceeding may take place, the preservation exercise often needs to be conducted prior to disclosure models being fully agreed or ordered by the court. Preservation should capture a wide universe of data to ensure that once the scope has been agreed, the required potentially relevant data is intact and can be collected.

Data preservation is the most vital stage of the litigation. ESI can be volatile and may be changed or deleted during everyday business. Paragraph 4.1 of the Disclosure Pilot, informs that preservation should include documents which might otherwise be deleted or destroyed. Many businesses have automatic data backup systems and data retention policies in place that are set up to overwrite or delete data after a certain period of time. Data retention polices and data backup processes should be identified and suspended if deemed to have an effect on potentially relevant data.

Legal hold notices, which instruct businesses to preserve all forms of potentially relevant ESI within their systems, therefore should be issued as soon as possible. Paragraph 4.4 of the Disclosure Pilot dictates that clients must be notified in writing by legal representatives of the need to preserve ESI, and in turn, clients are to respond in writing to confirm they have taken such steps. IT administrator assistance and specialist software applications may

be required to disable employee deletion permissions and mitigate the risk of data being removed from systems by general, everyday use. As an example, email data should be preserved by IT administrators, even if the user of the email account deletes emails from their account.

Collection of Electronic Documents

Where it is not possible to preserve ESI in its original location, the data should be collected/extracted and preserved as soon as possible. Data collections should be conducted by an experienced professional (e.g., the IT administrator of a particular system or a digital forensics expert) to ensure that potentially relevant ESI, along with its metadata, is extracted from the systems in its original form. As an example, the act of dragging and dropping or copying a document from a computer system to an external hard drive, will result in some changes to metadata dates and times associated with the document. This can cause difficulties with future processes such as the searching capabilities utilised for the review, and may also call into question the legitimacy or reliability of any disclosed documents. Specialist tools should be utilised to ensure that metadata remains unchanged. Collected data should be backed up and stored in an isolated and secure location to ensure tampering or data loss is not possible.

Data collections of preserved data residing in original systems will likely be required once disclosure models have been agreed or ordered. Once issues are agreed within the DRD, data may be able to be collected in accordance with the specific issues in a more targeted way. An example of this, in relation to email data, would be to apply date ranges to the universe of data to be collected to reduce the exported data to the relevant time period only. This would inevitably reduce time, cost, and population of irrelevant material during legal review. It is good practice to include a buffer into any date range collections as litigation requirements or date ranges may change over the course of the matter. It is often better to cast the net a little wider at the start to cover any potential changes further down the line, rather than having to recollect the data sources again. Recollections can add additional time delays and costs to the matter.

Culling of Electronic Documents

When determining how to best cull a preserved universe of data, being selective or "cherry picking" data at the outset can be a difficult and unadvised process to rely upon when working with Models C, D or E. Paragraph 31A, of the Disclosure Pilot highlights that a custodian or client must not make the selection of which documents are relevant to a matter. This process relies upon someone who's involved in the case to point you to specific data for collection. For example, a user could point you to a particular folder within their email account, where emails related to this matter are stored. However, relying on all emails being correctly placed in the folder over a number of years is a risk. The case of *Square Global Limited v. Julien Leonard*[2] is a good example to review, and states:

The client should not be allowed to decide relevance—or even potential relevance—for himself, so either the client must send all the files to the solicitor, or the solicitor must visit the client to review the files and take the relevant documents into his possession. It is then for the solicitor to decide which documents are relevant and disclosable.

It is also considered best practice not to run keyword searches at the point of a data collection. This is due to the limited functionality of a particular data source's native application vs. an eDiscovery or Digital Forensics application. Documents which are not text searchable such as some PDF or images

[2] *Square Global Limited v. Julien Leonard, [2020] EWHC 1008 (QB) (Eng.), available at https://www.bailii.org/ew/cases/EWHC/QB/2020/1008.html.*

within the potentially relevant data set should have optical character recognition applied (OCR), container files such as ZIP or RAR files should be expanded, and embedded data within documents should be prepared before keywords are applied. Using native applications related to a particular data source runs a high risk of missing potentially relevant material as you can't guarantee that all documents are searchable. It could also result in the other side producing documents that you do not have and, in turn, opening your process up for criticism.

Processing and Review of Electronic Documents

Using eDiscovery or Digital Forensic applications to process collected data ahead of culling is best practice. Processing data is where an application ingests data and makes the contents searchable. This involves extracting attachments from emails, expanding ZIP files, and extracting text from documents. In short, the tool creates a master database of all documents and relating metadata so that it can be searched. Processing ensures that the universe of data is indexed and can be searched using multiple parameters.

A review tool such as Relativity or Sightline takes the processed data and allows further review and analysis. As the data is now searchable, this allows for flexible workflows such as using date ranges, keywords, email threading, analytics, and other technology-driven workflows to review documents.

Conclusion

To conclude, it is important to follow recognised processes and workflows, guided by experienced eDisclosure experts when planning and conducting data preservation and collections exercises. This adds a layer of protection, independence, and defensibility to the foundations of the matter.

ABOUT THE AUTHOR

Sophie is a Senior Director at Consilio, a global leader in Legal Consulting & Legal Services. Sophie runs the digital forensic and expert witness teams across Europe and APAC and has been working in the digital forensic industry for more than a decade. She holds a degree in computer forensics and is an EnCE certified computer forensic examiner, who is also a certified counter fraud specialist. She has worked on a variety of high-profile criminal and civil cases and has assisted in over 400 criminal and civil cases in the United Kingdom covering cases involving harassment, murder, child pornography and fraud. She has been independently responsible for the collection, preservation and analysis for digital evidence retrieved from electronic media, as well and producing technical reports on the findings for law enforcement, corporates, lawyers, and independent parties.

Sophie works with Consilio's clients from the outset of any given matter, to assist with data mapping and scoping. Sophie provides advice of the most efficient and cost-effective preservation/collection methods and offer her services as an expert witness.

Sophie Beattie, EnCE, CDFE, Certified GDPR Practitioner

Senior Director - Forensic Investigation and Expert Witness Services

m +44 (203) 808.9622
e sbeattie@consilio.com

consilio.com