

e-Discovery and EU privacy laws — Part II

As discussed in Part 1, e-Discovery is creating difficulties for European organisations with overseas affiliates involved in foreign civil litigation or criminal or regulatory proceedings (see *Privacy & Data Protection Journal*, Volume 8, Issue 6, pp. 8–11). The subject is now occupying the attention of the Article 29 Working Party. Until it releases its guidance paper, industry will be forced to devise, in a highly uncertain environment, an appropriate compliance strategy to address the data privacy concerns that e-Discovery exercises raise. This second part explores some measures that industry and some regulators have been debating.

To recap, some of the e-Discovery scenarios that confront industry today include situations where:

- (i) as a result of an anticipated (but not yet pending) foreign litigation, a European organisation becomes subject to a duty to preserve potentially relevant materials — for example, emails and business documents — in the expectation that they may need to be disclosed later;
- (ii) a European organisation must respond to broad pre-trial discovery requests once foreign litigation commences; and
- (iii) a European organisation becomes subject to a duty to preserve or produce documents in connection with foreign criminal or regulatory proceedings.

In all of the above scenarios, the materials and information sought can, and frequently do, include personal data within the meaning of EU data protection laws.

EU privacy implications of e-Discovery

The EU data protection law implications of e-Discovery exercises are relatively easy to identify, but much more challenging to solve. They give rise to a host of issues, such as:

- furnishing adequate notice to affected European individuals;
- ensuring the underlying legitimacy of the collection

and processing (and, frequently, international transfer) of personal data;

- maintaining appropriate limitations or controls on the scope of the data collection exercises; and
- abiding by international data transfer rules.

Furnishing notices

E-Discovery exercises invariably raise an issue of notice — namely, organisations need to ensure that any affected staff and, potentially, third parties are informed of the collection and processing of their personal data in connection with foreign litigation or, potentially, criminal or regulatory proceedings.

In the past this may have been done in general terms via handbooks, employment contracts and other devices. However, organisations must now consider whether such notices were adequately detailed to address the current situation. In cases where there is a possibility of employees having engaged in inappropriate or unlawful conduct, either as a matter of foreign or local laws, questions of timing are also raised. Organisations naturally will want to avoid inadvertently tipping off individuals suspected of wrongdoing.

A further issue arises where personal data relating to non-employees are collected, raising the question of whether, and how, notice can reasonably be furnished to these persons, who may have a very tenuous relationship to the organisation.

Legitimacy of processing

European organisations engaged in e-Discovery exercises motivated principally, if not wholly, by foreign litigations, law or regulations, naturally need to be mindful of the need to ensure they do not fall afoul of EU legitimacy rules. There can be a difficulty in ensuring that a lawful basis exists under national data protection laws for processing the data at issue.

(Continued on page 4)

Dan Cooper, Of Counsel at Covington & Burling, concludes his two part series by exploring a variety of current solutions designed to mitigate risks associated with e-Discovery confronting all European organisations

Dan Cooper is speaking at the 7th Annual Data Protection Compliance Conference in London on 'The pitfalls and perils of corporate investigations'

For more information on the Conference, which takes place on 2nd and 3rd October 2008, visit www.pdpconferences.com

(Continued from page 3)

Frequently, the question is whether a European organisation gathering and disclosing personal data as a result of an overseas litigation, involving not the organisation but its foreign parent or affiliate, can rely on the 'legitimate interests' or 'legal claims' conditions found in nearly all EU Member State laws. If not, the organisation may need to consider obtaining consents from staff, which can be risky in light of the employer-employee relationship.

Proportionality and data security concerns

E-Discovery, by its very nature, tends to give rise to overly broad, and thus disproportionate, data collection and processing exercises contrary to EU proportionality rules.

Third parties, notably opposing parties (or, more accurately, their legal counsel) in the civil litigation context and foreign officials in the criminal or regulatory context, are responsible for preparing the relevant information requests, and have an obvious incentive to draft those as expansively as possible.

Unhelpfully, foreign civil procedural rules, such as the US Federal Rules of Civil Procedure, may encourage this result by requiring production of information that merely may lead to the discovery of admissible information (rather than the admissible evidence itself).

Organisations also need to consider how they can best go about extracting the relevant information from their electronic systems and hard-copy files in such a way that the information remains appropriately secure. Security should be maintained both at the time of collection and when disclosed to parties, such as tribunals and litigation adversaries.

International transfers

In nearly all cases, e-Discovery efforts lead to the transmission of documents and materials to foreign (non-EU) jurisdictions like the US, whose data protection regimes have not been deemed adequate by EU authorities, and made available to third parties or

disclosed in legal or regulatory proceedings accessible to the public. This invariably implicates European rules regulating the international transfer of personal data. Although the Directive and many Member State laws allow organisations to transfer data to establish, exercise or defend against legal claims, this derogation is quite often applied narrowly and excludes claims brought against a European organisation's foreign affiliate or parent. Therefore, European organisations need to consider implementing an appropriate compliance option, whether involving consents, transfer contracts or, in the case of the US, the EU-US Safe Harbor framework. European organisations also need to bear in mind that the immediate transfer to a foreign affiliate may be followed by an onward transfer to unrelated third parties, such as foreign litigants, courts or regulators.

Possible solutions

Multi-national organisations confronted by e-Discovery scenarios are in the process of devising a number of ad hoc solutions intended to, albeit not completely resolve, but mitigate some of these known compliance problems. Whether regulators ultimately endorse any of these various measures is yet to be seen, although organisations adopting some or all of them — given the absence of clear mandates from EU regulators — should be in a much better position where a data protection authority subjects an e-Discovery exercise to regulatory scrutiny.

Pre-emptive document preservation

Many multi-national organisations, particularly those based in the US and those regularly defending or bringing lawsuits, historically have adopted global pre-emptive document preservation policies, under which business documentation and communications are stored in anticipation of future litigation or criminal or regulatory investigations.

These practices go beyond the preservation of materials that occurs once a litigation or investigation is

reasonably expected to materialise. As a general practice, such a policy is questionable as a matter of EU data protection law, as often the relevant materials are held indefinitely and ultimately not produced.

Instead, organisations should establish bright-line tests or initiating 'litigation holds' or 'freezes' when litigation or investigations appear probable, rather than preserving materials based on speculation or mere rumour that litigation may take place.

Organisations should develop and implement a retention policy, under which documents are pre-emptively preserved or held only where reliable indicia of future litigation or investigations are present. Reliable signs include: actual knowledge of a pending dispute, awareness of corporate acts or omissions that violate applicable laws, receipt of pre-litigation correspondence (for example, letters before action) or communications from legal counsel or regulators.

Furnishing notices and soliciting consents

Although an organisation may be able to argue that affected employees have been notified by means of generic notices, it ideally should furnish more detailed and focused notices before an e-Discovery exercise commences. Often, employees themselves will be asked to preserve or produce the relevant information, making it a reasonably simple matter of incorporating appropriate disclosures in the communication conveying the request, whether it take the form of an email, internal memoranda or something else.

Of course, this approach may need to be rethought where the European affiliate is being asked to produce materials in connection with investigations conducted by foreign regulators or law enforcement that could implicate locate staff. Relatedly, an organisation stands to benefit from seeking the consent of affected European staff where feasible.

Although concerns have been expressed by some European regulators over collecting employee consents generally, these concerns tend to be

less present in many e-Discovery scenarios. A European employee may have every interest in assisting an affiliated organisation to defend itself in a foreign litigation, recognising that an adverse litigation outcome for that organisation could have a residual negative impact on the European affiliate. For example, where a US parent company is seeking to defend the validity of a business-critical patent or IP rights in a US litigation brought by a competitor firm, a European employee possessing relevant documents will have an incentive to ensure the documents are produced so that the company can prepare an effective defence. The consequence of failure may be an immediate downturn in the organisation's US and global business.

None of the above address the issue of notifying non-employees whose information also may be produced and disclosed in the course of e-Discovery. Here, the organisation may need to adopt a more pragmatic approach that recognises that some individuals may be too difficult to contact or that their privacy interests are so minimally affected by the proposed production, that seeking to furnish notice or secure consents would be unreasonable under the circumstances. However, such efforts may be warranted in the eyes of European regulators for other individuals, whose privacy might be materially impacted by the disclosure or who could be easily contacted by the organisation.

Establish a nexus

European organisations stand to benefit where they can frame the e-Discovery exercise as advancing their own commercial interests or legal rights, as opposed to the interests or rights of their foreign affiliates directly involved in proceedings. It would even be advantageous to perform the e-Discovery equivalent of an impact assessment (now familiar to organisations in other contexts, for example, employee monitoring), by memorialising or documenting what the company stands to gain or lose, in financial, commercial, reputational and other terms, based on the outcome of the foreign litigation or investigation.

Where it is possible to demonstrate a strong nexus between a European organisation's interests and the foreign proceedings, it may be able to rely upon some of the helpful exemptions that exist under EU Member State data protection laws: namely, those that relate to processing or disclosing personal data to protect an organisation's legal rights and interests, found in Articles 8(2)(e) and 26(1)(d) of the Data Protection Directive.

Exemptions of this type, where applicable, can help an organisation legitimise its processing of the relevant data, engage in an international data transfer, and potentially comply with other EU data protection rules.

Limit the scope

To the extent permitted, European organisations should strive to limit the scope of the e-Discovery effort, recognising that there may be an inevitable tension between permissive foreign procedural rules and restrictive EU Data Protection Principles.

For instance, under US federal civil procedure rules, discovery requests can be narrowed where the information sought could be acquired more conveniently from other sources, or the burden or expense associated with the production of the information outweighs its usefulness. Even where it may not be possible to narrow the scope of the requests consistent with applicable procedural rules, it may be possible to adopt document production techniques that are more likely to lead to the production of relevant information.

Rather than subjecting an entire workforce to broad sweeping requests for any relevant information, it would

be more consistent with EU proportionality rules to target relevant employee populations whose role or

responsibilities make it more likely that they will possess responsive materials.

Further, the organisation should focus employees on producing materials generated during the relevant timeframes, rather than encourage a broader initial production and then expect to further cull the materials before disclosing externally. Whenever practicable, the company should also encourage employee self-production, rather than seek to extract information by running undisclosed key-word searches of corporate systems and networks.

The latter approach, unless carefully managed and transparent to staff, remains much riskier, insofar as it may be improperly characterised as

illegitimate employee monitoring.

Relevancy assessments

Organisations should also try to conduct an initial relevancy assessment in the EU, before transferring any information to the non-EU jurisdiction where proceedings are anticipated or pending, consistent with EU relevancy rules exemplified by Article 6(1)(c) of Directive 95/46/EC.

Therefore, organisations should delete or redact any information falling outside the scope of the e-Discovery request locally, rather than forwarding it on to their colleagues or legal counsel, particularly those outside the EU.

“Organisations should establish bright-line tests for initiating “litigation holds” or “freezes” when litigation or investigations appear probable, rather than preserving materials based on speculation or mere rumour that litigation may take place.”

(Continued on page 6)

(Continued from page 5)

Today, so-called virtual data rooms remain very much 'in vogue' among law and consultancy firms engaged in much multi-jurisdictional due diligence and discovery work. There are undoubted benefits of such databases and systems from a data protection perspective; the virtual rooms can be more secure than physical repositories, and access to information more effectively monitored.

For example, data rooms can easily lend themselves to international transfers of personal data, as personnel in different geographies often are able to access and share materials. To illustrate, documents are scanned and often uploaded at an EU affiliate, so that law departments and legal counsel located in foreign countries can remotely review them at their leisure. While seemingly more efficient, this process of making information available to others inevitably gives rise to international data transfers.

Anonymisation techniques

European data protection regulators will favour attempts by organisations to anonymise the information or produce it in a redacted form such that the identities of individual persons remains concealed, thus arguably taking it outside the scope of EU data protection laws altogether.

Naturally, the viability of this approach often depends on the volume of materials being produced, the available technologies, and related factors. Where e-Discovery lends itself to the production of voluminous documents, emails and other materials, which is increasingly typical of modern US-style litigation, anonymisation may not be a realistic option.

This approach may also ignore the realities of modern litigation, in which an opposing party or regulator receiving information in a redacted form may suspect that the underlying aim is to conceal prejudicial facts, rather than protect the privacy of the individuals in question. That said, organisations can, and possibly should evaluate the costs and timing associated with developing bespoke

software that can be used to automatically encrypt materials, if only so that they can later demonstrate to European data privacy regulators that such an approach was considered and rejected on good grounds.

Contractual controls

A further necessary tactic involves subjecting third party agents involved in the e-Discovery exercise to appropriate contractual controls, in accordance with EU data protection rules such as Article 17(3) of Directive 95/46/EC.

One issue that can arise is whether external legal counsel or consultants assisting in the document production qualify as 'data processors,' based on the fact that they are acting on the organisation's instructions, or as independent 'data controllers,' based on the fact that they may be subject to independent ethical constraints and professional rules that could impact their handling of the data. In many jurisdictions, including the UK, this issue appears to be unsettled, and so it may be necessary for organisations and their counsel to discuss the matter and reach agreement at the outset.

Non adequate jurisdictions

European organisations need to give some thought to the obvious matter of international data transfers when foreign proceedings take place in a 'non-adequate' jurisdiction, recognising that third parties, such as opposing counsel or tribunals, are unlikely to agree to a formal data transfer contract or, for US transfers, enrol in the Safe Harbor as a condition for receiving the data. Helpfully, European organisations disclosing information tend, in the first instance, to furnish it to their foreign affiliate where there may be some scope for executing a data transfer agreement, or benefiting from a Safe Harbor enrolment.

Given the anticipated onward transfer of the information to third parties, it is usually necessary to consider the restraints the transfer mechanism places on further disclosures. For instance, EU model contracts may call for soliciting

the consent of employees to the onward transfer or, although relatively impractical, seeking to have the recipient agree to be bound by the contractual terms in turn. If the Safe Harbor is implicated, there may be scope for taking advantage of provisions, allowing US organisations to deviate from Safe Harbor principles (including the Onward Transfer principle) where Directive 95/46/EC or Member State laws would permit in comparable contexts — for example, to exercise, advance or defend against legal claims.

Court protective orders and 'in camera' reviews

Court orders help to ensure that a cloak of confidentiality is extended to particularly sensitive information produced or disclosed in the context of proceedings, and a good example is furnished by US Federal Rule of Civil Procedure 26(c)(1). Rule 26(c)(1) authorises a US federal court to impose conditions on how litigants may share information with one another, such as by limiting the persons permitted to access the information, permitting disclosure only under court order, and applying other suitable protections. Another related possibility involves 'in camera' reviews, whereby information or matters are first reviewed for relevancy by the court and then shared with opposing parties subject to appropriate controls.

Conclusion

E-Discovery will undoubtedly attract greater attention from industry and EU regulators in the coming months what with the opportunities for direct conflict between foreign discovery and procedural rules and EU data protection rules. While problems are liable to persist for the indefinite future, and no iron clad solutions is available, European organisations can at least adopt a variety of techniques to mitigate their risk in this uncertain area.

Dan Cooper

Covington & Burling LLP

dcooper@cov.com
