NORTON ROSE FULBRIGHT

Cross-border cyber review: It's not your typical eDiscovery exercise

By David Kessler and Andrea D'Ambra, *New York Law Journal* — January 29, 2021

While there are tools, tricks, and processes that can be lifted from classic e-discovery processes, a cyber review is distinct with its own unique workflow.

2020 was a year of extremes in many aspects. After the exceptional impact of COVID-19, and perhaps, in part, because of the way the pandemic forced businesses to change their operations, the steep rise in cybersecurity attacks—particularly ransomware attacks—have crippled or impeded many companies. Recovering from these attacks requires the expertise of forensic investigators to identify the compromised systems, and specialized attorneys to identify and advise on the types of data requiring notification as well as the regulatory requirements impacting cyber breach cases. Under the current regulatory regime, the United States has 52 different data breach notification laws, a challenge in and of itself.

Today, however, many companies have either global operations or global customer bases and that means that most cyber incidents cross national borders. This creates additional complexities as the impacted organization not only has to identify and comply with breach notification laws in additional countries, but the response to the data breach may need to be adjusted to comply with a matrix of cross-border privacy and cyber laws. This is especially true of the process to review and identify the potentially impacted data subjects and the compromised personal data.

Cyber review is not eDiscovery

In order to provide the necessary information to regulators and provide the proper individual notification, the potentially compromised data must be reviewed to identify the implicated data and data subjects. While there are tools, tricks, and processes that can be lifted from classic e-discovery processes, a cyber review is distinct with its own unique workflow. And, just as cross-border discovery in litigation requires greater effort and more planning, cross-border cyber incidents (and their reviews) require even greater coordination and planning.

To help illuminate the complexity, we will focus on one example in the cyber review: data subject name normalization. Unlike e-discovery where the goal is produce documents, the goal in cyber review is to identify each *unique* individual whose data was compromised. Because the same person could be referred to—in a variety of ways—in multiple documents and databases, it is crucial that all of those references are captured to identify the unique person and all their potentially compromised information. If you do not, normalize them, you will over count them (making the incident look worse than it was) and send them multiple letters (potentially confusing the data subject). This technical

Davis Kessler is Norton Rose Fulbright's head of data and information risk in the US and is based in the firm's New York office. **Andrea D'Ambra**, also based in New York, is the firm's US head of e-discovery and information governance.

problem almost always exists in cyber review, but it is compounded in cross-border reviews. For example:

- special characters or accents in names that are perhaps used for a data subject in some databases, but not in others (e.g., Françoise versus Francoise).
- use of two names as a first name, vice a first and last name (i.e., is the data subjects first name "Jean Marie" or Jean?)
- determining which names are first names versus last names, for example in many Asian countries a person's surname is first, but for business purposes, they may reverse this (e.g., Meng Wai Ang versus Ang Meng Wai).

This is but one of a host of potential complexities, both large and small, that can introduce error, expense, and delay into the cyber review and the follow-on notification to regulators and individuals. For example, all cross-border reviews can be complicated by different languages, but cyber review requires understanding the format and significance of different national, organizational, and local IDs. Likewise, all cross-border reviews need to comply with local data protection and data localization laws, but the normal steps we take to minimize these conflicts are ineffectual in cyber reviews because the personal data is exactly what is at issue. In addition, because companies co-mingle data, it may not be known that a cyber review implicates data subjects from a variety of jurisdictions until the review is underway, which in turn could trigger short notification times that may have already expired. Thus, cross-border cyber review is not just different in the degree of complexities, but in the kind of complexities that can derail a response.

Planning is key

As discussed above, given the incredible time pressures and costs of a cyber review (especially in cross-border matters), it is crucial that it be efficient and that documents not be re-examined or recoded because necessary information was not extracted. While each code and each extraction takes time, going back over documents to find missing information is much more expensive and time consuming. With this is mind, it is necessary to understand the impacted company's business in each jurisdiction to determine not only what data breach laws may apply, but the nature of the personal information that may exist in the data.

Personal information may be much more subtle and nuanced in cross-border cyber incidents and unprepared reviewers may easily miss key information that needs to be reported to regulators, customers or the individuals themselves. For example, it can be as simple as the format of national IDs changes from country to country or as complex as the client is a government (or even defense) contractor in certain countries that impose very specific reporting obligations. Likewise, you may learn that while the client's current data hygiene practices are best-of-breed, older data stores may not be as clean when the compliance practices were not as immaculate or when a recent acquisition is still integrating its data handling procedures.

To be efficient, you only want to collect and extract the information you need to comply with your reporting obligations. Obviously, this necessitates knowing those obligations, which means (1) knowing where the client operates; (2) knowing its business; and (3) knowing the regulatory framework in each jurisdiction. While there is lots of overlap between countries and the reports a breached company will need to make, there are differences. It is better to be conservative and collect more information than necessary, then not have what you need and go back. An hour or two sitting down with business people within the organization (not just in-house counsel) can provide the necessary context properly to train reviewers to identify the right information.

Likewise, just like a cross-border discovery exercise, knowing where the data originates is key to setting up a review process that itself complies with all the applicable data protection laws. Many jurisdictions may have data localization laws that limit the ability to have third-parties review data outside of the original jurisdiction or, at a minimum, require special contracts to review the data. The most famous of these restrictions is the need for Standard Contractual Clauses (SCCs) for third parties to access and review the data of EU Data Subjects in third countries that have not be deemed to have adequate protection (e.g., the United States). If a global HR system has been compromised, before a U.S. review team starts accessing the data, it will likely be necessary to have the proper Data Processing Agreement and SCCs in place. Also, remember, that mere access to data from a different jurisdiction is considered a transfer by many data protection authorities.

Perhaps one of the benefits of cyber review versus litigation review is that the actual review itself need not be conducted by attorneys. In fact, in many cases, non-attorney reviewers are faster and more efficient at the data identification and extraction piece. Finding such personnel outside the United States can, however, prove to be more challenging, particularly when there are specific foreign language and data localization requirements. This challenge can be compounded by local labor laws and cultural norms around expected working hours. So while in the United States working nights and weekends on a time sensitive project may be expected, in many countries reviewers will decline to work extended hours even when offered overtime and bonuses. If reviewers will not put in more hours, then one may need to add members to the review team.

This comes with its own draw backs as with more reviewers comes more opportunities for error, and thus more vigilance is required by the quality control team. In some cases, the market for reviewers with particular foreign language skills can be exhausted in the local jurisdiction, which may require looking for reviewers with those language skills in jurisdictions where data transfer would still be permissible (for example using French Canadian reviewers to review French language documents, when the French/EU reviewer market is stressed or too expensive).

Lastly, two other potential complexities deserve mention. First, while the California Consumer Privacy Act (CCPA) broadly introduced data subject access requests in the United States, these have been a fact of data protection outside the United States for a long time. Notice of a cyber incident often spawns a spate of requests either for access or deletion (or both) as data subjects are reminded (or learn) that the client has their data. As the review unfolds, you should prepare the client to be able to respond to these requests efficiently and leverage your review database to help the client. However, because the cyber incident may put the client on reasonable notice of litigation or investigation, the client may not be able to delete the relevant personal information because of preservation obligations.

Second, where a cyber incident impacts employees in jurisdictions with Works Council (e.g., Germany), it is crucial that you and client understand their obligations to the Works Council under any agreements. Not only is it possible that the client has agreed to special notice obligations, but the review itself may be considered employee monitoring that may need approval (or at least notice). The Works Council may have concerns about how, where, and who is doing the cyber review or, at a minimum, may want to be kept informed of the event and progress.

Conclusion

Even small and medium sized companies are doing business abroad and, as such, are accumulating information about their vendors, suppliers, and customers outside the United States. As such, personal information about people from numerous countries is often comingled in the same data system. When it is compromised in a data breach, all of those laws and requirements are potentially in play driving up the cost, stress, and time pressure.

It is incumbent upon you to triage quickly, assess the scope of the potential situation and ensure you have a team with the requisite resources to address the potential global breadth of the incident. In parallel (and working with your forensic team), you need to quickly assess not just the scope of compromise, but the scope of the clients business and the potential locations of data subjects that may be within the compromised data. You need to plan a review that accounts for the complex data protection and breach notification matrix that applies to the client and the data at issue (which, depending on the client, may come as a rude shock). At the same time, you must not compound the problem, by creating a response (and review) process that does not comply with all the applicable data privacy and data protection laws.

As with any large task with heavy time pressure, there will be a strong urge to jump in and start working the data. However, a well-planned and well-informed review process that takes account of the laws that cover the review and the nature of the notification obligations will lead to faster and better conclusion.