CYBERSECURITY LAW & STRATEGY

OCTOBER 2019

Data Privacy Reviews: The Cornerstone of a Data Breach Response

By Andrew Goodman

On May 25, 2018, General Data Protection Regulation 2016/679 went into effect in the EU. Better known as the GDPR, EUGDPR.org calls it the "most important change in data privacy regulation in 20 years." Unlike a number of previous data privacy regimes, the GDPR came with a sharp set of teeth, calling for a fine of up to €20 million or 4% of the previous year's global turnover, whichever is greater. Companies were now on notice that they had to be extremely careful in how they responded to a data breach or face the consequences.

In addition to the GDPR in the EU, there are several pieces of legislation in the U.S. that seek to protect personally identifiable information (PII). These include: the Fair Credit Reporting Act of 1970, which addressed consumer information in the files of consumer credit reporting agencies; the Health Insurance Portability and Accountability Act of 1996, which contained provisions meant to safeguard a particular type of PII — personal health information (PHI); and the Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999), which seeks to control the ways financial institutions control private information of their clients.

Finally, the California Consumer Privacy Act (CCPA) is set to take effect on Jan. 1, 2020, with the goal of enhancing privacy rights and consumer protection for California's nearly 40 million residents. The CCPA carries with it a fine of between $100 and $750 per affected California resident. Going forward, entities doing business in the U.S., UK and globally need to ensure they have a process in place to respond if their data is ever compromised.

Each organization will plan a response to fit its size and structure. Internal stakeholders may include some or all of the following: chief financial officer, chief technology officer, the data protection officer or data privacy team, IT, legal, compliance and human resources. External support comes from outside counsel, where one law firm will suffice or multiple firms will be engaged depending on geographic scope and political issues. A technology vendor with the

requisite forensic expertise will be able to determine what happened, how and to what extent.

The last external party is in some ways overlooked but nevertheless the most important: A managed document review vendor can quickly and accurately review the information that was affected by the breach to determine what PII might have been implicated and to whom it belonged in order to help all the others stakeholders assess risk, shape the response and, where required, notify regulators and potentially impacted individuals. This article focuses on why including a managed document review vendor in your incident response plan is critical.

Responding to Data Subject Access Requests (DSARs) under the GDPR are the type of PII review that is the most similar to a regulatory or litigation document review in that the data has not yet been produced to the requesting party and any PII or sensitive personal data, or SPD, other than that of the Data Subject will need to be redacted before being produced to the Data Subject. To the extent an organization deals with a constant stream of DSARs in the regular course of business, a managed document review provider will be able to put a process in place to standardize and streamline the review process, and leverage technology to the extent possible to reduce manual effort associated with the required redactions.

Other data privacy reviews — data breach, incident response, PII review, cyber reviews — have the opposite focus: the goal is not to redact PII before it is produced, but to review a corpus of documents that have presumptively been exposed and then to expeditiously determine the extent of the exposure. As such, the impacted organization will need to identify individuals whose PII may have been exposed as quickly and completely as possible, including a report listing the potentially impacted individuals, their contact details and the categories of PII that were potentially exposed, including whether any were minors.

There are a number of factors that go into this analysis, and a managed review vendor has to be nimble enough to deal with any and all the client and counsel deem necessary for a particular review, including:

- **Scope:** The scope of the review can be narrow (limited to a few states) or very broad. The impacted data could come from individuals in multiple states in the U.S. and from multiple member states in the EU, where Data Protection Authorities from different states and different jurisdictions within a state do not always take a uniform approach to how they enforce the GDPR. It is important to have a managed document review vendor in place that can quickly review the data for the applicable PII categories, as provided by the client or counsel, and report back on which jurisdictions are in play and adjust as additional jurisdictions are identified or in response to political considerations aimed at keeping up relations with a particular regulator.
- **Timing:** Timing is always of the essence in data privacy reviews, as the proverbial barn door has already been open for some time before the incident has been discovered. And most data privacy regulations — especially the GDPR — assign deadlines for particular responses. As such, any PII from EU individuals must be prioritized. Other timing considerations include:
    - Companies may have contractual requirements obligating them to notify their business partners of a data breach. While the company can send a courtesy notification to customers that might be affected, a fast PII review can confirm whether such a company was actually affected and also identify others that had yet to receive a notification.

    - For publicly traded companies, is the breach material enough to require the company to submit a Form 8-K? If yes, the timing of such a filing should ideally not be close to any regularly scheduled reporting, such as the filing of the 10-Q or 10-K. All of this is driven by quickly identifying the extent of the potential exposure and what reporting obligations that triggers or does not trigger. Again, time is of the essence.
    - Timing is also crucial if the company has recently been acquired. It is possible that the only outstanding issue is to determine the extent of the potential breach and then whether that will result in a reporting requirement. Time becomes even scarcer if the merger is scheduled to close imminently — the acquiror will want to put some certainty around its potential liability and decide whether the transaction can or cannot close.
- **Scale:** The amount of data that was potentially exposed is another key factor that needs to be addressed along with timing. The right managed review vendor will not only have experience with PII reviews, but also a large number of permanent employees trained in recognizing PII and how to do so in the context of an incident response. This will allow them to scale up or down as required, either to meet priority timelines such as responding to a DPA in the EU or to ramp up on a moment's notice when a spear-fishing attack was thought to have affected one mailbox, when a few days later (and with the clock still ticking) forensic analysis determines that the number is actually in the hundreds! A managed document review vendor will also be able to work with the technology vendor to run proprietary and commercially available PII screens to determine which documents might contain PII and reduce the volume that actually requires review and to construct a workflow to isolate the ones with actual PII as soon as possible.
- **Categories of PII**: In general, the following categories of PII need to be captured: Social Security number, Taxpayer ID number, passport number, driver's license number, credit card number, bank account and routing number, date of birth and online account number and password. Other information may be relevant as well, depending on the industry and geographical location. For instance, PHI needs to be captured, especially for health care companies, nonpublic personal information (NPI), such as account numbers should be captured for financial services companies and policy information should be captured for insurance companies. Non-U.S. jurisdictions may consider the notification information itself — street address, phone number and/or email address — to be PII. For each potential instance of PII, the managed document review team needs to determine whether it is notifiable — for example, is a partial Social Security number or the last four digits of an account number enough to trigger a notification requirement? Is a bank account number without a routing number sufficient? An experienced managed review vendor will help raise these issues as early as possible and provide examples so that the client and counsel can make a decision and head off the need for rework that will cost money and, more importantly, time.
- **PII Report**: At the end of the day, the managed document review provider will be able to furnish the client and counsel with a report that shows the number of potentially impacted individuals and the potential geographic scope of the impact. This gives them actionable intelligence to determine where their obligations lie and whether threshold reporting requirements have or have not been met and to develop a strategy to meet those requirements. An experienced managed document review vendor will be able to

provide a thorough and accurate report that meets the client's and counsel's needs as quickly as possible.

Conclusion

Companies need to insure that under the various data privacy regimes in the U.S., the EU and around the world, they are doing their best to plan for the worst-case scenario — a data breach. A key part of constructing the team to implement this plan is to identify a managed document review provider that has developed an expertise in PII reviews in the data breach/incident response context. Such a provider will be able to deal with the challenges of scope, timing, scale, identifying notifiable PII and preparing a notification report so that the company and its counsel can quantify and manage its risk quickly and accurately.

*****

Andrew Goodman, Associate Vice President of Litigation Services, QuisLex, has over 20 years of experience actively managing and supervising large-scale, complex document reviews in numerous industries and practice areas. He has trained multiple large teams on document review and creating privilege logs, and is currently responsible for spearheading QuisLex's litigation training programs. He also manages key aspects of QuisLex's client and vendor relationships. Andrew frequently speaks on topics related to e-discovery and legal project management. He received his J.D. and M.B.A. from Washington University in St. Louis and earned a B.A. with honors from the University of Michigan.
