Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Questions To Ask Experts Working With Your Data

Law360, New York (September 25, 2015, 11:19 AM ET) --


Deborah K. Foster

Recently, Ann Caresani wrote an article highlighting the importance of businesses implementing measures to protect and secure their employee data.[1] Caresani's article rightly identified various sources of data security risk, highlighted the importance of training employees to appropriately handle sensitive data and pointed to examples of what can happen when employee databases are breached.

As economists who conduct data analysis in the context of labor and employment litigation, we would like to supplement Caresani's discussion. While proper in-house data security processes and mechanisms are essential, it is equally important for businesses to understand how their sensitive data are treated when they are sent to third-party data processors. This is particularly true given the number of parties that may touch a business' sensitive data in the course of a litigation (e.g., in-house counsel, outside counsel, outside consultants and experts, as well as any number of parties on the opposing side of a case).

We have compiled a list of 10 questions businesses should ask when retaining experts that will receive the firm's sensitive information, including applicant tracking data, human resource information system personnel data, payroll data and time-keeping records. We have organized the questions around three main steps in the process: data transmission, data use and ongoing data management. For each step, we provide questions to highlight key issues and concerns to discuss with those receiving your firm's sensitive data.

Data Transmission

Although it is necessary to send data to parties outside the company (such as outside counsel, opposing counsel, and data experts), the data can be vulnerable during transmission. As such, you want to be aware of the precautions that are being taken to ensure it remains secure en route. Below are some useful questions to ask.

1. What Information Is Really Needed?

While it is important to produce the information necessary to appropriately analyze the claims at issue, as well as to be responsive to the opposing side's requests, from a security standpoint, focusing the set

of transmitted information can mitigate exposure to security risk. Custodians of sensitive data within companies should work closely with counsel and the expert team to understand the types of information to be provided, as well as the universe of employees for whom that information is needed. They should also discuss with the expert team options for anonymizing sensitive data that is not essential to the expert analysis (e.g., replacing Social Security numbers with unique employee IDs prior to transmission).

2. How Can We Send the Data?

Sensitive data should never be sent via email. Almost always — unless the size of the data is prohibitive — file sharing sites that encrypt data during transmission can be used. Uploading files to a secure site allows the data custodian to restrict access to just the relevant recipients and to track downloads. Additionally, it minimizes the "in transmission" portion of the process to a direct download, and data files can be deleted from the site once they have been downloaded. If the data files are too large to upload, encrypted data can be stored on external media such as a hard drive and sent to the appropriate parties. In such cases, instructions on how to decrypt and access the data should be sent separately from the hard drive itself.

3. What Will Happen to the Original Data After the Expert Takes Possession?

Sensitive data should be stored securely after the expert team takes possession of them. The data custodian should designate a concrete amount of time that the data will remain on the file sharing site prior to removal, as well as confirm who will be responsible for their removal after that time. With respect to external media, it should be made clear how the hard drive will be stored for the duration of the expert engagement (or whether it will be returned once the expert team has transferred the data from the drive). Note that this is an issue in both the initial data transfer as well as for any subsequent data updates or supplements.

Data Use

Once the data are safely in the possession of a third-party, you want to be sure they will stay secure. Questions to ensure proper handling by your expert team include the following below.

4. Where Will the Data Be Stored While It Is Being Processed and How Is It Secured?

While the expert team may be working with a company's sensitive data day in and day out, it is nonetheless important that security protocols continue to be followed. In this case — much like an in-house review — the company's data custodian will want to know whether the data are kept on an on-site server or an off-site data warehouse, as well as verify that the physical server is in a secure area.

5. How Is Access Controlled and Managed?

Access controls provide an important security mechanism, as minimizing sensitive data access to just the relevant expert team members reduces the risk of unintended leaks and disclosure. The company's data custodian should be aware of who is authorized to access the data, and request that they be notified of any major changes in access that may occur as the expert team evolves through the duration of the litigation. It is also important to understand how the data will be used by multiple individuals on the case and be aware that data are most secure when they remain on the server instead of being downloaded to individual work stations, especially laptops.

6. Are Social Security Numbers Retained in the Data?

As mentioned above, it is best if Social Security numbers can be removed from the data by the company's data custodian prior to production to outside parties. However, because multiple systems may use different employee IDs and/or IDs may be reused, the Social Security number may be the only unique identifier available. If that information is required to prepare the data for expert analysis, it is still best if, once the data are properly constructed using a Social Security number, the number is then replaced with a unique identifier and stripped from the working data sets. Any party providing such data should inquire if this kind of de-identification is possible.

7. How Will Data Be Exchanged Between the Expert and Counsel (Both In-House and Outside)?

Experts generate analyses and data samples for use by in-house and outside counsel, so the same data (either "raw" or processed) may be transmitted *back* from the expert team. It is important that the data custodian be aware of the transmission mechanisms the expert team intends to use (e.g., that just as with the initial file transmission, a secure site or encrypted hardware should be used, and that files containing sensitive data would not be sent via email).

Ongoing Data Management

Even when a litigation or investigation concludes, a company's sensitive data remains "out in the world." These data may still be at-risk, even when they are not in active use. Although it is often necessary for the expert team to retain data for some period of time following the close of litigation, it is important to understand the third-party's data retention policy. A few questions to ask about that policy are below.

8. How Long Is Data Retained After the Close of Litigation?

Because occasional follow-up questions or issues can arise, data are typically retained for some period after a litigation concludes. However, the company's data custodian should be aware of the expert team's plan for when the likelihood of such need diminishes. For example, the expert team should articulate whether the data will be archived, returned to the company or deleted altogether. As with the initial transmission, return of the data should follow secure transmission protocols.

9. Where Is Inactive Data Stored and in What Format?

It is likely that, at the conclusion of the litigation, the data relied upon for expert analyses are archived. (This may also be the case during the course of the litigation if, for example, a case is stayed for an extended period of time.) At this stage, the company's data custodian should be aware of how the data are stored, who has access and what is required to restore the data again should the need arise.

10. How Often Are Data Security Policies Reviewed and Revised?

Litigation and related data analysis projects can continue for years, so it is important to ensure the expert team regularly reviews and updates data security policies in response to ever-evolving security threats. For example, as new technologies or security threats emerge over time, the company's data custodian should be aware of the expert team's approach to implementing those technologies and mitigating those threats.

While data security questions like those above should be asked of experts and their teams at the outset of the engagement, it is important to remember that data security is an ongoing process. As the business' priorities evolve, or the course of the litigation changes, experts and their teams may need to adapt their processes for working with their clients' sensitive data. Moreover, as companies consider their internal data security protocols, they should continue to keep in mind third-party access to sensitive data are part of that process.

—By Michael Kheyfets, Deborah K. Foster and Nathan D. Woods, Edgeworth Economics LLC

Michael Kheyfets, Deborah Foster and Nathan Woods are partners in Edgeworth Economics' Washington, D.C., office.

[1] Ann M. Caresani, *The Greatest Cybersecurity Risk Comes From Within*, Law360, Sept. 1, 2015. Available at https://www.law360.com/articles/697280/.
