NORTON ROSE FULBRIGHT

The Obligation to Secure Your Opponent's Data in the Age of Hacking

David J. Kessler and Susana Medeiros, *New York Law Journal – June 3, 2019*

Data security concerns have increased in the past several years, as hacking, corporate espionage, and data breaches are on the rise around the globe. Third-party attacks are becoming not only more sophisticated but also larger in scale. Law firms, legal matters, litigation and produced data remain high-profile targets for cyber-attacks. As discussed in a previous article, producing parties remain vulnerable to the risk that even if they adequately protect data in their own systems, third parties may steal data from the requesting parties' systems.

Parties and counsel who receive data in litigation have an obligation to take reasonable steps to protect that data. See The Sedona Principles, *Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, 179 (2018); see also William LaRosa, Note, *New Legal Problems, Old Legal Solutions: Bailment Theory As A Baseline Data Security Standard of Care Owed to Opponent's Data In E-Discovery*, 167 U. Pa. L. Rev. 1 (2019). Moreover, "[a] requesting party inherits the data privacy and protection obligations that come with the ESI it receives, including the responsibilities that arise from the loss of that information." The Sedona Principles at 179, n. 147.

Thus, the question is not whether a receiving party has a duty to take reasonable steps to protect data, but what is reasonable and proportionate in the context of the matters. While a receiving party could attempt to address security concerns unilaterally without reaching an agreement with opposing parties, this is a risky strategy. First, they may not know the value of the data they are receiving and, therefore, not know whether their efforts to secure the data are sufficient. Second, reaching agreements with the opposing party in advance of production provides greater certainty as to what is reasonable and prevents the parties from imposing security standards after the fact. Third, and finally, producing parties may not be able to actually produce information without having certain data security and breach notice requirements in place.

Minimize Data Production

Parties should continue to focus on relevance and proportionality to minimize the production of unnecessary data by all sides. Data that is not produced cannot be stolen and obviously does not need to be secured by the receiving party.

Where very sensitive data (e.g., extremely valuable trade secrets like source code or genetic or other very sensitive personal information) is relevant and must be produced, additional safeguards are appropriate. For instance, a war room or secure review site with such features as watermarking and technical blocks on copying, pasting or printing controlled by the producing party may be the appropriate solution. Alternatively, the parties may negotiate a redaction protocol to remove irrelevant personal information and irrelevant trade secrets from relevant documents. See *In re:*

David Kessler is head of data and information risk, United States, based in Norton Rose Fulbright's New York office.
Susana Medeiros is an associate in the firm's commercial litigation team also based in New York.

Takata Airbag Prod. Liab. Litig., 2016 WL 1460143 (S.D. Fla. March 1, 2016). Because this option can be extremely expensive and time-consuming, however, the parties should consider phasing the production of such documents so that the most critically relevant documents are redacted and produced first, with the remainder re-evaluated as necessary.

The Duty to Secure

The following are some recommended measures for receiving parties complying with the duty to secure:

Access and downloading controls. Access to the producing party's documents can be limited physically and electronically. Physical measures may include key card access to offices and departments, which is implemented in some form at most work places, or restricting information to a single terminal. Electronic measures may include implementing multi-factor authentication, using strong password standards coupled with periodic forced password changes, limiting transmission of passwords (i.e., passwords provided orally via phone, not email), and similar measures.

A requesting party should limit access rights to the producing party's data on a need to know basis. This includes the litigation team, but may also include relevant experts, or key client employees.

Limit the number of copies. Limiting the number of copies of the data makes them easier to secure. The requesting party can prohibit making copies of data on external media (USBs; CDs; hard drives; and laptops). If such devices are used, they should be encrypted. Parties should be compelled to retain all branding and watermarking with any printed copies.

Sharing and storing of such information should be done in a secure manner. Encryption is essential to sharing information. This can include sharing encrypted files, sharing data on an encrypted Wi-Fi, and restricting the use of unencrypted external media. In addition, the parties should utilize secure file transfer protocols (FTPs) where possible to share data.

If using a third-party service provider such as a discovery vendor to store the producing party's data, ensure the vendor has adequate security and privacy protections in place. It may be appropriate to require that the data be stored in facilities that comply, either by certification or by attestation of compliance, to one or more of the data security standards (e.g., NIST; ISO) as applicable to the case or data. Additionally, old standbys like personnel background checks should not be overlooked.

Negotiating Obligations in a Protective Order

Discussing what data security measures are "reasonable" and "proportionate" and implementing them in the parties' protective order can minimize conflicts once data is produced. In some instances, measures above and beyond the duty to secure will need to be negotiated.

Below are some key provisions the parties should address in such a protective order:

Reasonable and Proportional Steps to Secure. At a *minimum*, parties should agree to use reasonable and proportionate steps to protect their opponent's data and, at least, protect their opponent's data with the same care and steps as they protect comparable data of their own.

Levels of Security. The parties should also consider instituting levels of security for information that requires additional protection such as limiting physical or electronic access to trade secret information.

Security in Pleadings and Trial. Parties may disclaim addressing secure use of documents in pleadings and trial, as only a tiny fraction of materials are used in either and fewer cases are going to trial. Securing discovery will address a significant amount of risk.

Deletion. It is standard, but crucial, that parties agree to delete the data of their opponent's once the litigation is completed. It may be important to provide specificity in the protective order on this issue to cover items like overwrites of data, destruction of keys that allow access to encrypted volumes, or aging out of backup material.

Notification obligations. Also, *at a minimum*, protective orders should have an obligation to promptly notify an opponent in the event of a cyber incident. Such a provision could read as follows:

> If the Receiving Party discovers a breach of security relating to the Protected Information of another Party, the Receiving Party shall: (1) provide written notice to Designating Party of such breach within twenty-four (24) hours of Receiving Party's discovery/notice of the breach; (2) investigate and remediate the effects of the breach, and provide Designating Party with assurance reasonably satisfactory to Designating Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Designating Party can reasonably ascertain the size and scope of the breach. If required by any judicial or governmental request, requirement or order to disclose such information, the Receiving Party shall take all reasonable steps to give the Designating Party sufficient prior notice in order to contest such request, requirement or order through legal means. The Receiving Party agrees to provide reasonable cooperation to the Designating Party or law enforcement in investigating any such security incident. In any event, the Receiving Party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access as it deems appropriate in its good faith and reasonable judgment.

Disclosure of Vendors. It may be appropriate for the parties to exchange the names of the vendors or places where the data is being hosted so they can assess the protections at issue (using publicly available information) and raise any objections. Parties may need to require that data does not leave certain jurisdictions, which can restrict the use of the cloud.

Auditing. Rarely is it appropriate for a producing party to "audit" the security processes of the requesting party's hosting location. Like discovery on discovery, this only should be done where there is good cause to believe that the security is not reasonable or there has been a data leak or incident.

Costs of Security. Under the American Rule, the costs of securing data should be borne by the party hosting the data. This will increase the costs of discovery, particularly for receiving parties in asymmetric cases, but that is the burden of e-discovery and is a fraction of a producing party's costs in discovery.

If certain vendors and law firms refuse to implement appropriate discovery in accordance with the recommendations above, then they may be excluded from engaging in discovery in certain cases, just as law firms and vendors that refused to adapt to the change in e-discovery were excluded (and or sanctioned) from engaging in discovery in complex litigation.

NORTON ROSE FULBRIGHT

Contacts

If you would like further information please contact:

David J. Kessler
Head of Data and Information Risk, United States
Tel: +1 212 318 3382
david.kessler@nortonrosefulbright.com

Susana Medeiros
Associate
Tel: +1 212 318 3044
susana.medeiros@nortonrosefulbright.com

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.