The Case Is Over: But Now What Do You Do With the Mass of Data Transmitted Throughout the Life of the Case?

by Anne Shea Gaza

Anne Shea Gaza is a partner with the law firm of Young, Conaway, Stargatt & Taylor LLP in Wilmington, Del., practicing in the area of intellectual property litigation and complex commercial litigation. She serves on the editorial board of The Federal Lawyer. *The author wishes to thank her colleague, Samantha Wilson, for her assistance in making this article possible. The views expressed in this article are those of the author and not necessarily those of her colleagues or firm. © 2017 Anne Shea Gaza. All rights reserved.*

With data breaches occurring from the highest level of government to corporations and even law firms, cyber-security is a concern not only for the owner of the data, but also for service providers as well.[1] For attorneys, this can mean balancing their discovery obligations to produce relevant information with their ethical obligations to protect confidential client information.[2] A confidentiality agreement or protective order is a traditional litigation tool for providing protection for confidential information. Ethical obligations to clients, however, necessarily require attorneys to have an understanding of the data that may be produced, and the technology underlying the data,[3] even under the protections afforded by a confidentiality agreement.

With electronically stored information (ESI) dominating the discovery landscape, merely having a confidentiality agreement is not enough. Counsel must have an understanding of what needs to be protected, how it needs to be protected, and what level of protection may be needed. Producing ESI is the rule rather than the exception in most litigation,[4] but counsel may inadvertently produce confidential client information if they do not have an understanding of both the easily reviewable data and the behind-the-scenes data. For example, if electronic data will be produced, then the attorney may need to understand what metadata is associated with any electronic files being produced to ensure adequate safeguards are taken depending on the level of security needed.[5] If source code will be produced, then the attorney may need to know what programs are needed to review the source code and whether extra precautions are needed, such as limitations on accessing, copying, or printing the source code.[6]

While many states and the American Bar Association (ABA) have taken steps to educate lawyers about their ethical obligations when it comes to technology, nearly half of the lawyers that responded to a recent ABA poll remain unclear on their technology-related duties.[7] This is particularly concerning when it comes to adequately protecting confidential client information once a case has ended. While confidentiality agreements provide protections for the parties, and often third parties, during the life of the case, provisions addressing the return or destruction of confidential information after a case ends are often brief and the express obligations directed primarily to the law firms involved in the case. If the parties did not have a confidentiality agreement, or relied on a default confidentiality order or local rule protecting confidential information, then there may be no provisions for how to handle confidential information once the case ends.

In jurisdictions following the ABA Model Rules of Professional Conduct (MRPC), an attorney's duty to make reasonable efforts to prevent inadvertent or unauthorized disclosure of a client's information continues not only after a case has ended, but after the lawyer-client relationship has terminated as well.[8,9] This also applies to third-party vendors that may have been retained to assist with the representation, such as e-discovery vendors.[10] Numerous states have issued similar ethics rules and guidance specifically requiring a minimum level of competence with technology.[11] Accordingly, it is incumbent upon a lawyer to be as involved and protective during the wrap-up process as during the litigation itself.

What follows are a few items to keep in mind while handling the final administrative details before closing a case.

Start Early

While protective orders or agreements between the parties may allow for the return or destruction of confidential information over a prolonged time period, early planning and investigation will prevent otherwise avoidable delays in completing the process. For example, if a law firm has archival data systems and software that take a long time to fully purge of the confidential information, delaying the initiation of the process may mean an attorney cannot certify to a client or opposing counsel that the confidential information was destroyed in a timely manner.

Know the Requirements

Was there a confidentiality agreement or protective order providing for the return or destruction of confidential information at the conclusion of the case? If not, then confer with opposing counsel, your client, and any third parties (if appropriate) to establish agreed-upon protocols for the return or destruction of the confidential information exchanged during the case. If the parties agree to permit retention of certain confidential information or categories of data (e.g., correspondence, pleadings, transcripts), then determine what ongoing protections will be accorded the retained data.

If there is an agreement that provides for how confidential information will be handled upon the conclusion of the case, what does it say? The specific terms that may have been agreed to vary widely from case to case so it is important to review the language in the case-specific agreement. Generally, confidentiality agreements will provide for a set time period for compliance with any return or destruction obligations. Counsel will often be permitted to retain at least one copy of certain categories of documents that remain subject to the confidentiality agreement even after the conclusion of the case. The key is determining what obligations the parties may have or may agree to for handling and protecting confidential information once the case is over so that compliance may begin.

Indeed, it is as important to know what can be retained as it is to know what must be returned or destroyed in order to account for all of the confidential information exchanged during the case. From a data security standpoint, appropriate protections should continue to be provided for confidential client information. Alternatively, a client may require that its confidential information be returned or destroyed by its counsel once the representation is over so appropriate steps may need to be taken in order to certify compliance with client requirements.

Know Where Everything is Stored (or Hiding)

Paper copies of confidential information are generally easy to find and collect. Electronic documents may appear equally as easy to find, such as in personal drives, email folders, personal mobile devices and/or laptops, shared drives, and production databases, but there are other repositories that should be considered. For example, some other locations to consider are cloud-based storage or file sharing sites, physical media (such as flash drives, CDs, DVDs, etc.), intranet/internet files, and voicemail boxes.

Many law firms routinely back up their servers and/or have secondary email servers. If this is the case, then compliance with return/destruction obligations may require that an attorney not only ensure that confidential information of the other party has been returned/deleted from email servers, desktops, and shared drives, but also from any backup tapes or secondary servers. Similarly, an attorney should ensure that the same level of detail is undertaken by the opposing side in order to adequately safeguard the confidential information of the attorney's client.

Advances in data security and technology management may mean there are servers or archives that are not readily accessible or even known by the attorney. As such, it behooves the attorney to solicit input early on from within the infrastructure of the law firm, such as a records manager or information technology (IT) specialist, to make sure that all possible locations for data are identified. To that end, just as the e-discovery process may have required review of client backup tapes or archives, confidential information could be hiding on a firm's backup tapes or archives and may require a records manager or IT specialist to delete or extract the data.

Remember the Experts and the Vendors

The case is over, the experts and vendors have long since been dismissed, but what about their data? Confidential information from either or both sides may have found its way to a document management company or an e-discovery vendor,[12] to a jury analyst, to experts, and/or consultants. If there was a confidentiality agreement in the case, then the experts and vendors may already be aware of its terms and may even have executed an undertaking to comply with it.

Some confidentiality agreements specifically impose affirmative obligations on the parties to request the return or destruction of confidential information from any experts, advisers, and/or vendors before certifying compliance. Regardless of whether such obligations exist, however, a best practice for counsel is to send a notice that the case is over to any experts and/or vendors that provided assistance during the case. Along with the notice, a reminder can be provided regarding the terms of the confidentiality agreement or instructions for how to treat the confidential information now that the case is over. This notice should be provided regardless of the source of the confidential information, particularly given ethical rules such as Rules 1.6(c) and 5.3 of the ABA MRPC.

In conclusion, there is no "one size fits all" approach to handling confidential information and no set guideline for ensuring compliance with ABA or state ethics rules. Just as an attorney must know and protect his or her client's data during the life of the case, the attorney should continue to ensure any confidential client data is accounted for and protected once the case is over. ⊙

Endnotes

[1] Based on data from the 2016 ABA tech survey, as reported in the ABA Legal Technology Resource Center's 2016 Legal Technology Survey Report, 14 percent of the survey respondents reported that their firm had experienced a security breach at some point in their firm's history. Responses to the 2016 ABA tech survey also indicated that 26 percent of law firms with more than 500 attorneys had experienced a security breach at some point. David Ries, *Security*, A.B.A. TechReport 2016, *available at* http://www.americanbar.org/publications/techreport/2016/security.html (last visited Jan. 27, 2017).

[2] *See, e.g.,* Jess Krochtengel, *Texas Lawyers Must Mind Metadata, Ethics Committee Says*, Law360 (Dec. 16, 2016, 8:41 PM), *available at* https://www.law360.com/articles/874054/texas-lawyers-must-mind-metadata-ethics-committee-says (last visited Jan. 27, 2017).

[3] *See* A.B.A. TechReport 2016, A.B.A., *available at* http://www.americanbar.org/publications/techreport/2016.html (last visited Jan. 27, 2017).

[4] Responses to the 2016 ABA tech survey indicate that 64 percent of the respondents receive requests for e-discovery while only 37 percent of the respondents indicated they never make e-discovery requests. Stephen Embry, *Litigation and T.A.R.*, A.B.A. TechReport 2016, *available at* http://www.americanbar.org/publications/techreport/2016/litigation_tar.html (last visited Jan. 27, 2017).

[5] *See, e.g.,* Commission on Law and Technology, *Understanding E-Discovery*, Del. Cts., *available at* http://www.courts.delaware.gov/declt/blogspot/understanding-ediscovery.aspx (last visited Jan. 27, 2017).

[6] *See, e.g., Default Standard for Access to Source Code*, Dist. Ct.

Del., *available at* http://www.ded.uscourts.gov/sites/default/files/pages/Default%20Standard%20for%20Access%20to%20Source%20Code.pdf (last visited Jan. 27, 2017).

[7] According to the 2016 ABA tech survey, "[n]early half of lawyers either don't think they're ethically required to stay up on legal technology developments or don't know what the rules are" that govern tech competency. Andrew Strickler, *Nearly Half of Lawyers Unclear on Tech Duties: ABA Report*, Law360 (Dec. 15, 2016, 7:31 PM), *available at* http://www.law360.com/articles/872719 (last visited Jan. 27, 2017) (referencing findings published in the ABA TechReport 2016).

[8] *See* Confidentiality of Information, A.B.A. MRPC 1.6(c), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html (last visited Jan. 27, 2017) ("A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.").

[9] A.B.A. MRPC 1.6, cmt. 20, *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html (last visited Jan. 27, 2017) (regarding former clients: "The duty of confidentiality continues after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(2). *See* Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.")

[10] Responsibilities Regarding Nonlawyer Assistance, A.B.A. MRPC 5.3, *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html (last visited Jan. 27, 2017). Rule 5.3 states:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

> (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> > (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
> >
> > (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

[11] "Following the ABA's adoption in 2012 of an amended competency rule that includes technology as a basic ethical duty, more than two dozen jurisdictions—they include New York, Pennsylvania, Massachusetts, and Illinois—have adopted in whole or in part a call for lawyers to keep up on legal tech or moved toward stronger regulation." Strickler, *supra* n.7.

[12] Responses to the 2016 ABA tech survey indicate that 52 percent of larger firms use outside litigation support bureaus and e-discovery consultants. Embry, *supra* n.4.