Commentary

Avoiding the Next 'Spygate': Critical Records Management Advice For Your Company In The Wake Of The Destruction Of The NFL And CIA Tapes

By
Danette R. Edwards

[Editor's Note: Danette Edwards is a member of Venable LLP's SEC and White Collar Defense Practice Group. Her practice is particularly focused on white collar criminal defense, complex civil cases, and corporate compliance and internal control issues, including records management policies and a range of Sarbanes-Oxley related matters. She also focuses on environmental criminal defense and internal investigations. Copyright 2008, the author. Replies to this commentary are welcome.]

Senator Arlen Specter's inquiry into the National Football League's destruction of six videotapes taken from the New England Patriots last September — dubbed "Spygate" by certain media outlets — has not surprisingly evoked some comparisons to the Congressional investigation of the Central Intelligence Agency's destruction of videotapes of interrogations of two terrorist suspects. Besides provoking Congressional ire and being the source of word plays related to spying, the destruction of the NFL and CIA tapes reinforces some valuable lessons about records management obligations affecting all of us in the age of electronically stored information.

When most people think of electronically stored information ("ESI"), they think of email, word documents, and Excel spreadsheets. As the NFL and CIA cases illustrate, this focus on the more traditional types of ESI is too narrow. ESI, as the name suggests, actually encompasses an entire array of media that goes beyond traditional forms. Relatively recent amendments to the Federal Rules of Civil Procedure ("FRCP") encourage litigants to request multiple types of ESI from their adversaries. The drafters of the FRCP intentionally failed to define ESI in order to give the term more breadth and longevity. An advisory committee note to the FRCP recognizes that current technology might lead a litigant to have to produce different image or sound files. Thus, under the FRCP's broad approach, stored videoconferences, videotapes, and digitized voicemail are just some of the myriad types of electronic information that might be subject to discovery in federal cases. The types of requests and production formats authorized by the FRCP will inevitably become more prevalent in contexts where the FRCP do not control — such as in state cases, enforcement actions, and criminal investigations.

It is important to remember that the failure to produce ESI in response to an appropriately tailored demand can lead to a potential sanction, substantial fine, or other penalty imposed by a court. There is a rapidly growing body of cases in which companies have been severely punished for their e-discovery failures. The case of *Qualcomm, Inc. v. Broadcom Corp.*, 2008 U.S. Dist. LEXIS 911 (S.D. Cal. Jan. 7, 2008) presents a particularly harsh example. As a sanction for intentionally failing to produce more than 46,000 emails and documents, the court ordered Qualcomm to pay Broadcom's attorneys' fees and litigation costs in the amount of $8.6 million. The court also referred six of Qualcomm's outside attorneys to the California Bar Association for possible ethics violations and ordered those attorneys plus Qualcomm and five of its in-house attorneys to participate in a "Case Review

and Enforcement of Discovery Obligations" program in order to create a case management/e-discovery protocol for future cases.

Stakes are even higher when there is an ongoing or potential government investigation and a company or individual has been accused of withholding, destroying, or altering ESI. An amendment to the federal criminal obstruction of justice statutes included in the Sarbanes-Oxley Act makes it a crime to knowingly destroy, alter or modify any document with the intention of obstructing a matter within the jurisdiction of an agency of the federal government, where such matter is pending, imminent or contemplated.

Viewing the NFL and CIA tape situations against the backdrop of the obstruction laws drives home the importance of taking proper measures to guard against the destruction of ESI when it might be relevant to an investigation. The NFL case raises a question about when precisely a matter within the government's jurisdiction is "contemplated." The NFL tapes were destroyed *before* Senator Specter launched his inquiry, and in fact, the inquiry appears to have been prompted by reports that the NFL destroyed the tapes. Questions about the NFL's integrity bear upon its continued entitlement to exemptions that it currently has under antitrust laws. Congress arguably has an *ongoing* concern in the effectiveness and proper administration of the antitrust laws. While all of this may not necessarily lead to the conclusion that there was a relevant antitrust matter within the contemplation of the government when the NFL tapes were destroyed, the more fundamental point is that the extension of the obstruction laws to matters where the government's jurisdiction is contemplated makes determining the boundaries of proper corporate conduct involving the destruction of ESI quite challenging. The CIA case stands at the opposite end of the spectrum from that of the NFL. Press reports indicate that the CIA took pains not to destroy the tapes until November 2005, nearly four years *after* the 9/11 Commission was no longer active. Press reports also indicate, however, that the CIA failed to provide the tapes to the 9/11 Commission, a failure that has been decried by the members of the Commission and Congress since the existence of the tapes was first reported. Likewise, although the CIA properly preserved the tapes for some time, the destruction of the tapes, coming at a time when Congress and others in government were expressing an interest in investigating the issue of "enhanced" interrogation techniques, has itself prompted a probe by the United States Department of Justice into whether any criminal statutes were violated. These events stand as a timely reminder not to destroy ESI when it might be relevant to an investigation.

Practically speaking, the best way to ensure that your company embraces the lessons from the NFL and CIA tape cases is by adopting a robust corporate records and electronic information management policy tailored to its specific needs. In the landmark case of *Arthur Andersen v. United States*, 125 S. Ct. 2129, 2135 (2005), the United States Supreme Court acknowledged the prevalence of such policies and the legitimacy, under ordinary circumstances, of using them to ensure the destruction of certain information. A well-crafted policy will allow your company to destroy information that no longer serves a business purpose and that relates to transactions or matters for which the relevant statutes of limitations have passed. At the same time, through inclusion of "litigation hold" provisions designed to address how records and other ESI are generated, used, and stored at your company, a robust policy will prevent regularly scheduled destruction of certain records and ESI when litigation or a matter within the government's jurisdiction is pending, imminent, or contemplated. In serving these functions, a corporate records and electronic information management policy can limit an organization's legal exposure for actions or conduct during the time period beyond the record retention period specified in its policy, while protecting against the risk of sanction for failure to have the records sought by prosecutors or regulators, or in litigation. ■