UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

**PRESENTED AT**

29th Annual Technology Law Conference

May 26-27, 2016
Austin, Texas

# Chapter 3
# Computer Usage Policies, Records Management, and Information Governance

**Jonathan Lass and Dustin S. Sachs**

Note: This paper was converted from a scanned image. The conversion has been reviewed for accuracy; however, minor spelling or text-conversion errors may still be present.

*CHAPTER* 3

# Computer Usage Policies, Records Management, and Information Governance

*Jonathan Lass and Dustin S. Sachs*[1]

## I. Introduction

Topics covered in this chapter include information governance management issues in the context of electronic discovery, including how document retention policies, records management, and computer usage policies affect a party's risk management position when dealing with electronic discovery issues. This chapter will conclude with recommendations concerning specific computer usage policies to assist in developing an effective information governance and document management and retention policy, to best protect a party from e-discovery issues that may arise during litigation, investigations, or audits.[2]

Companies involved in litigation are concerned with electronic discovery as a means to obtain information about the adverse party persuasive to a party's claims or defenses. To avoid sanctions for failing to preserve data relevant to the litigation or a presumption that deleted data was beneficial to the claims of the adverse party, companies have developed document retention policies (DRPs) aimed at regulating the destruction of data, including electronically stored information (ESI) that the company holds in its or its employees' possession. Companies have included DRPs that, if effective, reflexively respond to receipt of litigation hold letters from adverse parties in litigation, thereby avoiding failure-to-preserve-data claims (also known as spoliation claims) from requesting parties.

1. Special thanks to Eve Searls of Jackson Walker, LLP.

2. Additional helpful guidance may be found in The Sedona Conference, *The Sedona Conference Commentary on Information Governance* (2013), *available at* **https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentan%20on%20Information%20Governance,** and the Information Governance Reference Model (IGRM), **www.edrm.net/projects/igrm.**

## II. Computer Usage Policies

While the ability to save large amounts of data at lower and lower costs per gigabyte or terabyte is appealing to operating companies, it also means that these companies arc storing ever larger amounts of data. The risk of holding so much unnecessary data becomes apparent when a company is the subject of a litigation, investigation, or audit where large amounts of ESI will need to be preserved and later reviewed to determine whether it is within the scope of the subject litigation, investigation, or audit, and then whether the ESI is subject to a privilege, such as an attorney-client privileged communication or attorney work product. Information governance policies assist companies in regulating the placement and volume of stored data, including ESI. Computer usage policies, namely DRPs, address the problem of managing the accumulation of ESI and the systematic processes that purge unnecessary data on a regular basis.

An effective computer usage policy provides clear rules for storage of data (that is, proper places for storage and types of data to be stored), timing of deletion of such data, and suspension of deletion of data in the context of a legal hold or litigation hold that pertains to an actual or threatened litigation, audit, or investigation.

To be effective, computer usage policies clearly explain the rules for storage of electronically stored data and have systems that congruently act to initially deploy and then manage the computer usage policies. In the face of litigation hold letters or requests for production, having computer usage policies pays for itself several times over.

When companies have computer usage policies intended for employees to review and acknowledge upon date of employment, the terms generally cover the following areas:

1. **No Right of** Privacy. For company employees residing in the United States, it is standard for companies to place a disclaimer that any electronic communications and any documents stored on the company's servers or computers shall be the property of the company and subject to review and use by the company, and that the employee should not expect any right of privacy with respect to electronic communications.
2. **Use of Internet on Company Devices.** Internet usage policies typically request that employees refrain from inappropriate use of the Internet, including accessing Web sites that have inappropriate, harassing, sexually explicit, or illegal content. Compliance reduces a company's legal risk.
3. **Storage of Nonwork Documents on Company Devices.** Companies' computer usage policies typically include a restriction that company devices issued to employees should not be used for nonbusiness purposes. Further, more sophisticated **company** policies include a provision specifically restricting employees from storing nonwork documents or e-mails.

UT LAW CLE THE UNIVERSITY OF TEXAS TEXASLAW

Also available as part of the eCourse
2016 Technology Law eConference

First appeared as part of the conference materials for the
29th Annual Technology Law Conference session
"Technology Law from the Bench"