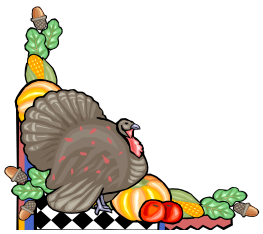
Mesmer & Deleault, PLLC
41 Brook Street, Manchester, NH 03104
*Seacoast Office: One New Hampshire Ave., Suite 125*
*Portsmouth, NH 03801*

*Happy Thanksgiving!*



# "Tip of the Month"

## The Digital Age: Privacy and Data Security Challenges for Companies

Everyone nowadays has heard of the issues surrounding privacy and data security. Some have experienced firsthand unauthorized disclosures of their own private data. Companies need to be sensitive to these issues of privacy and data security, especially those companies that provide employees with cell phones, tablets and/or laptop computers. What is the relationship between company rights and the employee's reasonable expectation of privacy?

Despite the importance of these issues, there is no comprehensive or consistent set of rules that currently govern privacy and data security in the U.S. What exists at present is a patchwork of federal and state statutes and cases that govern different industries, various types of conduct and different kinds of personal information. This can be complex and confusing.

Electronic communications privacy is a relatively new issue and, not surprisingly, the one with the least developed legal guidelines. The most significant rules arise out of the Electronic Communications Privacy Act (the "ECPA") and the Stored Communications Act (the "SCA"), both federal laws. The ECPA provides civil and criminal penalties for the interception of electronic communications and the use or disclosure of unlawfully intercepted electronic communications that are captured in transit. The SCA imposes civil and criminal penalties on any business that accesses a computer used to provide an electronic communications service without authorization or beyond the scope of authorization.

While it is well settled that a company can access email and other electronic communications created, sent, received, and stored in the company's own computer systems, the new digital age technology has created complicated and confusing questions for which there often are no clear answers. This new digital age technology includes text and instant messaging, webmail (Gmail, Yahoo!, Hotmail, etc.), social media (Facebook, MySpace, Flickr, LinkedIn, etc.), Twitter, and blogs. Although a company has the right to review its employees' text and instant messages stored on company-owned electronic devices, it may violate the SCA for a service provider to furnish the subscriber-company with copies of those texts or instant messages. Even though these issues remain unresolved, a company can create and implement information use policies that will shape the reasonable expectation of privacy of its employees.

More recently, there are several bills pending in Congress that would broadly govern privacy and data security. These include the Commercial Privacy Bill of Rights Act of 2011, the Consumer Privacy Protection Act of 2011, the Personal Data Privacy and Security Act of 2011, the Secure and Fortified Data Act, and the Data Accountability and Trust Act of 2011. Internet service providers and employers should pay attention to developments in Congress related to privacy and data security. These developmenst may simplify the complexity and confusion created by the patchwork of federal and state statutes relating to these issues but may also impose new procedures that a company must follow to be compliant.

If you need help understanding the complex interaction between privacy, data security, and reasonable expectation of privacy, the attorneys at Mesmer & Deleault are here to help. For more information, please do not hesitate to give us a call at 668-1971 or contact us by email at *mailbox @ biz-patlaw.com*.

Frank B. Mesmer, Jr.
Robert R. Deleault
Steven H. Slovenski
Ross K. Krutsinger
1111

(603) 668-1971
Fax (603) 622-1445
*E-mail:* mailbox@biz-patlaw.com
*Website:* www.biz-patlaw.com