

What the IRS reminds us about email privacy

John E. Anderson Sr. 11:04 a.m. CDT July 11, 2014



(Photo: Submitted)

A half-decade's worth of emails recently were summoned in the investigation surrounding former IRS employee Lois Lerner, who remains under scrutiny for allegations of abusing her power to fulfill a political agenda.

But it isn't just high-ranking federal employees who have to worry about who might be reading their emails. Most employees are unaware that their place of work may have the right to all information shared across their company email address, even information normally protected by attorney-client privilege.

In today's digital age, some of the most confidential conversations occur over email. And someone can never be entirely sure if information is really ever gone for good.

Take Lerner's case, for example. Although an unknown number of emails spanning two years may never be fully recovered, investigators were still able to trace back to more than 24,000 of them by accessing emails from other accounts. Additionally, more than 67,000 emails were handed over to investigators — all potentially revealing incriminating evidence.

Although the IRS case has shifted focus to whether a hard-drive crash resulting in the loss of two years' worth of emails was a matter of convenience or subpar technology, it serves as an important reminder to the average email user that one of our most used means of communication is hardly private.

It is important to realize that just because user names and passwords protect access to accounts, it does not necessarily mean that there is a reasonable expectation of privacy, particularly regarding emails sent from company accounts. An email scandal at Harvard University, during which it was revealed that 16 deans' email accounts had been searched to identify a media leak surrounding a cheating incident, revealed just how little privacy an employee has with information exchanged over a work account.

The Harvard scandal was yet another reminder that most employers have policies that allow them to monitor the online activity of their employees, often without an employee's knowledge. Such a situation could be disastrous for an employee involved in litigation against his or her own company, because even the attorney-client privilege may not hold up in court.

And it's not just work accounts that can fall under scrutiny. Personal email accounts aren't as private as you think.

The Stored Communications Act protects information sent over personal email, but it's not a cure-all. Last year, Google argued that its users have no reasonable expectation of privacy. They also argued that users sending emails from other providers to Gmail accounts similarly lack a reasonable expectation of privacy.

So is there any way to make certain that information is being sent securely across the Internet?

Emails between a client and their attorney, as with anything confidential, should never be sent from a company email account. In fact, employees should be wary of any communications from a company account.

One of the morals of the IRS case might just be that nothing sent over the Internet is safe or private — and it should never be assumed that it is. In the digital age, people are leaving a trail behind, and that trail could end up haunting them in ways they had never imagined.

John E. Anderson Sr. is a member attorney with the Nashville office of Dickinson Wright PLLC. His practice focuses on commercial and business litigation. Reach him at janderson@dickinsonwright.com (<mailto:janderson@dickinsonwright.com>).

Read or Share this story: <http://www.tennessean.com/story/opinion/2014/07/10/irs-reminds-us-email-privacy/12421397/>