Departing Employees and the Stored Communications Act: Employers Beware

Insights
12.10.10

Departing employees sometimes access workplace computer systems to obtain information for purposes of using it in competition with their employer. Sometimes they use the internet at work to send emails concerning their post-employment plans. And while employers have many tools and tactics at their disposal to investigate their computers and related systems, these investigations are fraught with pitfalls for the incautious employer.

One of the issues employers need to be aware of in conducting such investigations is the unauthorized interception or monitoring of electronic communications – which includes e-mails – by an employee pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2510 ("ECPA"). The ECPA was passed by the United States Congress to update government restrictions on wire taps from telephone calls in order to protect transmissions of electronic data through computers. In fact, the ECPA was passed by way of an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which was intended to curb unauthorized government access and monitoring of private electronic communications. Through the ECPA, Congress prohibited the acquisition of a communication through the use of any electronic, mechanical or other device by criminalizing unauthorized acquisitions and creating a civil cause of action for victims of unauthorized acquisitions. Title II of the ECPA, the Stored Communications Act, 18 U.S.C. §§ 2701-12 ("SCA"), protects certain electronically stored communications.

The intersection of the ECPA, the SCA and an employer's investigation of a departing employee can become fertile ground for mistakes by the investigating employer. When investigating an employee's use of workplace computer systems, employers typically review corporate e-mails, corporate servers, and the computer assigned to the employee suspected of disloyal acts. Such investigations can uncover personal information, like the passwords used by the employee for his or her personal, internet-based e-mail accounts, and this is where investigating employers need to be careful. Some federal courts have held that improperly using these passwords to open and monitor the employee's personal, internet based e-mail or social media accounts may give rise to a claim for unauthorized access under the ECPA and SPA. See, for example, Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2009 U.S. Dist. LEXIS 88702, at *10-11 (D.N.J., Sept. 25, 2009). (A copy of the Pietrylo opinion is available in pdf format below.)

But the ECPA and SCA are not one-way streets running only in favor of departing employees. These statutes apply with equal force to allegations of misconduct by disloyal employees, as demonstrated

statutes apply with equal force to allegations of misconduct by disloyal employees, as demonstrated by the recent case of United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010). Szymuszkiewicz was employed as a revenue officer by the IRS, and he was convicted by a jury of violating the ECPA. In an appellate opinion affirming the conviction, Chief Judge Frank Easterbrook described Szymuszkiewicz's conduct as:

"monitor[ing] email messages sent to his supervisor, Nella Infusino. She found out by accident when being trained to use Microsoft Outlook, her email client. She discovered a "rule" that directed Outlook to forward to Szymuszkiewicz all messages she received. Szymuszkiewicz was convicted under the Wiretap Act for intentionally intercepting an electronic communication ... agents found emails to Infusino stored in a personal folder of Szymuszkiewicz's Outlook client -- in other words, Szymuszkiewicz not only received the emails but also moved them from his inbox to a separate folder for retention--which is not what would have happened had all of Szymuszkiewicz's access been legitimate....The jury could have chosen to believe Szymuszkiewicz's contention that he received Infusino's emails legitimately, or by mistake, but the evidence supported the more sinister inference that he obtained them intentionally and without her knowledge."

622 F.3d at 703-4 (internal citations omitted). (A copy of the Szymuszkiewicz opinion is available in pdf format below.)

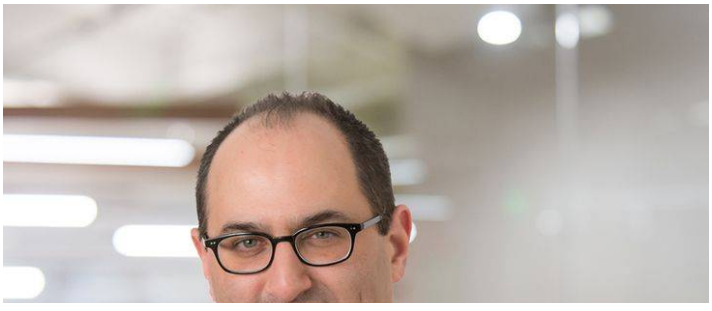
The takeaway from Szymuszkiewicz for employers is the importance of exercising extreme caution when conducting investigations of an employee's use of corporate computer systems, as mistakes committed during these investigations could possibly give rise to independent civil, and potentially criminal, liability. In addition to consulting with counsel and forensic computer specialists, employers should keep their eyes on the ECPA and SCA, under which one of the touchstone inquiries is whether there is authorization to access the electronic communications.

US v Szymuszkiewicz.pdf (112.39 kb)

Pietrylo v Hillstone Restaurant.pdf (95.40 kb)

Brent Cossrow is a member of Fisher Phillips' Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below.

Related People



Brent A. Cossrow
Regional Managing Partner
610.230.2135
Email