NEW CASE CHALLENGES PUBLIC EMPLOYER'S MONITORING OF WHISTLE-BLOWERS' PERSONAL EMAIL MESSAGES

Paul D. Godec, Esq.
Kissinger & Fellman, P.C.
3773 Cherry Creek North Drive, Suite 900
Denver, Colorado 80209
Main: 303-320-6100
paul@kandf.com

Can government employers monitor the personal email accounts of suspected whistleblowers? Can governmental employers monitor and seize private email messages from private email accounts only because employees viewed those messages through government-issued computers on government networks? A potential bellwether lawsuit claims that federal agencies violated employees' rights and retaliated against them for whistle-blowing by monitoring their private and personal email messages.

Factual Background. The lawsuit alleges that the United States Food and Drug Administration (FDA) began monitoring certain employees after discovering congressional authorities had information about purported FDA missteps. The lawsuit alleges that the FDA knew about reports from FDA employees to the House Energy and Commerce Committee. The reports from FDA employees alleged that senior FDA managers had ordered, intimidated, and coerced FDA scientists into modifying their scientific reviews, conclusions, and recommendations in violation of federal law. *See Hardy v. Shuren*, No. 1:2011cv01739 (U.S. District Court, District of Columbia, filed Sept. 28, 2011).

Specifically, FDA scientists had concluded that computer-aided-detection devices designed to enhance breast mammograms were neither safe nor effective. Yet, the scientists alleged that the FDA approved the devices for use anyway through a flawed process that ignored science.

Legal Allegations. The lawsuit describes the FDA's alleged secret email monitoring and search-and-seizure operations in retaliation against the protected speech of the whistle-blowers. The lawsuit alleges that the FDA intercepted private communications created on government-issued computers and sent to congressional representatives through government computer networks. The FDA employees allege that their email messages enjoyed privacy protection because they disclosed corruption within the FDA's device review process; managerial misconduct; and dangers to public health, welfare and safety. The lawsuit also alleges that the targeted monitoring of the FDA employees' email messages constitutes unlawful retaliation against the whistleblowers.

The lawsuit alleges that federal employees, acting as whistle-blowers, have rights to free speech and to privacy under the First Amendment. The lawsuit alleges that the FDA violated rights

under the Fourth Amendment by illegal searching and seizing private email communications in which employees had a reasonable expectation of privacy. The lawsuit alleges that the FDA violated rights to freedom of association with whistle-blowers and to petition the government for redress of grievances. The lawsuit also alleges violations of statutory rights of the public employees. The lawsuit alleges a distinction between lawful routine computer system monitoring, and the unlawful targeting of a protected class of whistle-blowers for individualized monitoring.

The FDA apparently admits some targeted-monitoring of the email content of certain employees. The FDA apparently justifies initiating the monitoring after a private company alerted the FDA about leaks of confidential and proprietary information to Congress and to the public. The FDA apparently believed that the leaks occurred from within the FDA and took steps to identify the sources of the leaks. The FDA reportedly designed its heightened internal monitoring to determine whether FDA employees inappropriately disclosed confidential information.

The lawsuit raises questions with respect to email monitoring and potential claims for discrimination or retaliation by public-sector whistleblowers. If employers may institute heightened monitoring against suspected whistle-blowers, then the monitoring could have a potential chilling effect on these employees' rights to free speech and association.

Practical Implications. These allegations should remind all employees that, when done properly, employers may lawfully subject employer-owned computers to monitoring. Current federal law generally allows employers to monitor all computer activity including any content transmitted, created, stored, viewed, uploaded, or downloaded on the company's computer or network.

Likewise, these allegations generally should dispel employees' common misperception that privacy expectations remain after employees open personal email accounts on company-provided computers. In most instances, employers may properly monitor any content on company-issued computers for the purpose of protecting business interests; preserving the integrity and operation of computer systems; protecting proprietary information and trade secrets; ensuring compliance with regulatory requirements; and preventing outside content from creating employment claims for harassment or discrimination.

These allegations should remind employees that, under certain circumstances, employers have legal obligations to disclose information to law enforcement authorities about suspected unlawful activities occurring through company-issued computers. Those reporting obligations may arise under the Patriot Act for content or activities implicating terrorism. The reporting requirements might also arise under various other federal or state laws.