SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

DECEMBER 2018

Roy Snell

former SCCE & HCCA
Chief Executive Officer
Edina, MN

by John Jacobs

Using electronic communications surveillance to strengthen compliance programs

- Proactive surveillance of employees' electronic communications is an effective compliance and risk management practice that can foster strong cultures of compliance and deter employee misconduct.
- Proactive surveillance can help reduce eDiscovery and legal costs, because early detection of messages evidencing possible fraud or unethical employee behavior can reduce litigation risk.
- Archival systems help facilitate efficient monitoring and allow for auto-flagging messages. Thoroughly research the right system for your organization.
- Establish a policy regarding employees' electronic communications as part of your company's compliance program, and consider including a surveillance provision as part of the policy.
- Before implementing an electronic communication surveillance policy, determine if there is a "legitimate business purpose" for the monitoring.

John Jacobs *(jjacobs@acacompliancegroup.com) is a Senior Principal Consultant for ACA Compliance Group in Pittsburgh, PA, USA.*
bit.ly/in-JohnJacobs

As Benjamin Franklin famously advised, "An ounce of prevention is worth a pound of cure." Proactive and thoughtful surveillance of employees' electronic communications is an effective compliance and risk management practice that can prevent potential problems. Yet, as employees' online behavior continues to pose serious compliance and reputational risks, and as eDiscovery costs resulting from misconduct skyrocket, many companies outside of the financial industry have not yet implemented this "ounce of prevention" that is effective to curtail unethical and damaging behavior.


Jacobs

Surveillance in the financial industry

Focused, risk-based surveillance of employees' electronic communications has become a standard practice in the financial industry. Surveillance of emails, chats, instant messages, and other electronic communications is not required by laws or regulations, but nevertheless has been implemented by investment advisers, investment companies, and broker-dealers. It's no longer merely a "best practice," but has become a standard practice to help prevent the dissemination of material nonpublic information and safeguard against other regulatory compliance violations.

The mutual fund scandal of 2003–2004 was an important factor in investment advisers' decisions to initiate proactive surveillance of employee emails. In one of the high-profile cases prosecuted during that era, the Securities and Exchange Commission (SEC) filed a complaint against Columbia Management Advisors (Columbia), alleging unlawful market-timing arrangements with third parties. As part of its case, the SEC relied on emails between Columbia employees and employees of the funds Columbia advised. In one of the emails from August 2000, a fund employee complained that the "active trading has increased and it has become unbearable. There will be long term damage to the fund. Let's understand that they really are not investors." Columbia settled for $220 million, and total industry settlements from similar charges totaled over $3 billion.[1]

In the wake of this scandal, SEC commissioners and staff began to discuss the importance of early detection of potential misconduct and the need for financial institutions to build strong cultures of compliance generally. Since that time, surveillance of employees' electronic communications has become standard practice within the financial industry, with 92.1% of firms in the financial sector participating in some form of employee surveillance.[2]

Notable cases where surveillance could have prevented harm

Outside of the financial industry, many firms do not yet conduct proactive email surveillance. However, the American Bar Association has acknowledged the role of email surveillance in the workplace, indicating that it can be "necessary to protect trade secrets, confidential business information, sexual harassment, fraud, theft, embezzlement, and data breaches."[3] Moreover, the Electronic Communications Privacy Act (ECPA) provides that an employer may monitor employees' electronic communications if the employer has a "legitimate business purpose" for the monitoring, or if the employer has obtained its employees' consent.

A review of some high-profile cases in other industries reveals that proactive surveillance could have mitigated future damages by detecting employee emails containing content that evidenced fraudulent or unethical behavior.

Merck

In September 2004, Merck & Company, Inc. (Merck), was forced to pull its blockbuster drug Vioxx from the market due to an increased risk of heart attack and stroke.[4] Internal emails by Merck executives indicate that they were aware of the cardiovascular risks presented by the drug well before it was released to the public. In 2000, an email from the company's research chief, Edward Scolnick, indicated that the "CV [cardiovascular] events are clearly there" and "there is always a hazard."[5,6] As these and other incriminating emails were made public, Merck defended more than 27,000 lawsuits, which were settled for $4.85 billion.[7,8]

Volkswagen

German automaker Volkswagen Group (Volkswagen) suffered public embarrassment, loss of public trust, fines, and penalties resulting from its diesel-emissions cheating scandal, which was uncovered in September 2015. The Environmental Protection Agency (EPA) filed a civil enforcement case against Volkswagen for violations of the Clean Air Act when it discovered that approximately 590,000 vehicles were equipped with "defeat devices" designed to cheat federal emissions tests.[9] Volkswagen officials claimed that they had no knowledge of the defeat devices, but internal emails indicated that the high-level executives were

aware of the unethical practice. An email from a Volkswagen compliance officer stated "It must first be decided whether we are honest. If we are not honest, everything stays as it is," referring to the defeat devices.[10,11]

Additional emails suggested that Volkswagen executives knew of the defeat devices and conspired to conceal them. The aforementioned compliance officer emailed a colleague discussing how the company could explain the difference in emissions between EPA testing and street-level testing. In the email, he appears to have been aware of the ongoing unethical activity. He wrote, "Difference between street and test standard must be explained (Intent = penalty!)"[12] As a result of the "Dieselgate" scandal, several key Volkswagen employees were incarcerated, the company incurred more than $30 billion in costs, and it also suffered a loss of trust and consumer backlash.[13,14]

Takata

A decade ago, auto manufacturers began to recall vehicles containing Takata Corporation (Takata) airbags due to safety concerns. Under certain conditions, the propellant causing the airbag to inflate would explode when deployed, causing serious and sometimes fatal injuries.[15] In 2005, a Takata airbag production engineer voiced concerns in a memorandum to another employee that the testing data was being manipulated and was not being accurately reported to the end customer. He added, "the data presented…to the customer is a clear misrepresentation of the facts."[16] By 2006, the same engineer wrote "Happy Manipulating!!!" in an email referencing the results of an airbag test.[17] As of December 2017, 20 people had died as a result of injuries caused by the defective Takata airbags, and approximately 37 million vehicles have been recalled, making it the largest automobile recall in US history.[18,19] In the resulting litigation, the corporation was fined $70 million by the National Highway Traffic Safety Administration (NHTSA), paid a $650 million settlement for various state lawsuits, and as part of a criminal plea with the Department of Justice, agreed to pay victims $125 million and to pay $850 million in restitution to automakers.[20,21] As a result, Takata filed for Chapter 11 bankruptcy protection.

Monsanto

Monsanto, maker of the weed killer Roundup, has been embroiled in litigation resulting from the alleged failure to adequately warn plaintiffs that certain chemicals in Roundup were carcinogenic to humans. In a 2015 internal email, Monsanto employees suggested "ghostwriting" scientific articles on the safety of Roundup, wherein Monsanto employees would write articles and have scientists merely sign their names to the research papers.[22] The email also suggested that the company had ghostwritten an April 2000 research article.[23] The consolidated case in federal court is subject to ongoing litigation, but in a California state court case stemming from similar alleged circumstances, a jury recently awarded the plaintiff $289 million in damages.[24]

In each of the four cases discussed above, proactive surveillance of electronic communications could have revealed that employees were possibly engaging in fraudulent or unethical behaviors. Early detection of such activity could have allowed the respective companies to take corrective actions before significant harm was done, and to mitigate damages.

eDiscovery costs are an additional consideration

Surveillance can help companies foster strong cultures of compliance, and act as a deterrent to employee misconduct. In the financial industry, proactive surveillance has helped to detect problematic employee behaviors that could have otherwise resulted in costly

litigation, business loss and reputational harm, and criminal liability. Email surveillance should be an essential component of any company's risk management and compliance program, but companies in most industries only review employees' email communications as a corrective measure after an adverse event occurs, usually during the discovery process of litigation.

In addition to fines, penalties, and other damages, companies have also incurred substantial legal costs in defending claims that can result from employee misconduct through electronic communications. Email and other electronic correspondence has overwhelmingly become the preferred medium for business communications. As Judge Shira Scheindlin of the U.S. District Court for the Southern District of New York noted, "as individuals and corporations increasingly do business electronically—using computers to create and store documents, make deals, and exchange e-mails—the universe of discoverable material has expanded exponentially.[25] Not surprisingly, the cost of eDiscovery has ballooned. By one estimate, the amount spent by US corporations on eDiscovery is $40 billion annually.[26] According to the RAND Institute for Civil Justice, a study of 32 cases found that the total cost per gigabyte reviewed was approximately $18,000.[27]

Conclusion

Unfortunately, as demonstrated by the high-profile cases reviewed above, employees' problematic emails can become strong evidence used against their respective companies in the resulting lawsuits. The "ounce of prevention" provided by proactive surveillance of communications could help prevent litigation by allowing early detection of unethical and problematic behaviors, such as employee discrimination, harassment, theft of intellectual property, fraud and financial crimes, and other types of employee misconduct. Left unchecked, such employee actions can ultimately result in significant damages. In such cases, a "pound of cure" will be exacted in the form of eDiscovery costs, legal fees, fines, settlements and verdicts, and reputational harm. ✳

1. Todd Houge and Jay Wellman, "Fallout from the Mutual Fund Trading Scandal," *Journal of Business Ethics*, no. 62 (2005): 130-131, 134, Note 12, http://bit.ly/2zP1beK.
2. Romy Ribitzky, "Active Monitoring of Employees Rises to 78%," *ABC News*, April 18, 2001, https://abcn.ws/2O09WLT.
3. V. John Ella, "Employee Monitoring and Workplace Privacy Law," *American Bar Association*, Section of Labor and Employment Law, National Symposium on Technology in Labor & Employment Law (April 2016): 2.
4. Barbara Martinez, et al., "Merck Pulls Vioxx From Market After Link to Heart Problems: Drug's Demise Raises Concerns About Company's Future; Loss of $2.5 Billion in Sales," *The Wall Street Journal*, October 1, 2004, https://on.wsj.com/2Rnr640.
5. Edward M. Scolnick, "Vigor," Industry Documents Library, University of California, San Francisco, March 9, 2000, http://bit.ly/2IAqhkp.
6. Joseph S. Ross, MD, MHS, et al., "Pooled Analysis of Rofecoxib Placebo-Controlled Clinical Trial Data: Lessons for Postmarket Pharmaceutical Safety Surveillance," *Journal of American Medical Association Internal Medicine 169,* no. 21, November 23, 2009, http://bit.ly/2RjgGCq.
7. Alex Berenson, "Merck Agrees to Settle Vioxx Suits for $4.85 Billion," *The New York Times*, November 9, 2007, https://nyti.ms/2xWkK3k.
8. "Vioxx Settlement Agreement," November 9, 2007, http://bit.ly/2OyQlSf.
9. "Learn About Volkswagen Violations," United States Environmental Protection Agency, last modified on August 11, 2017, http://bit.ly/2xZVNUM.
10. William Boston, "VW's Emissions Scandal: How It Unfolded," *The Wall Street Journal*, January 11, 2017, https://on.wsj.com/2IzySUk.
11. *Complaint at 11-12, United States v. Schmidt*, No. 16-MJ-30588 (D. Mich. 2015), http://bit.ly/2NlyHgn.
12. *Id*. at 12.
13. "Learn About Volkswagen Violations," United States Environmental Protection Agency, http://bit.ly/2xZVNUM.
14. Alastair Jamieson, "Audi CEO Rupert Stadler arrested in Volkswagen diesel emissions probe," *NBC News*, June 18, 2018, https://nbcnews.to/2ybcxaZ.
15. "Takata Recall Spotlight," National Highway Traffic Safety Administration, accessed September 8, 2018, http://bit.ly/2zPvvWx.
16. Senate Committee on Commerce, Science, and Transportation, "Total Recall: Internal Documents Detail Takata's Broken Safety Culture and the Need for a More Effective Recall Process ADDENDUM to Danger Behind the Wheel: The Takata Airbag Crisis and How to Fix Our Broken Auto Recall Process," 114th Cong. (2015) (Exhibit B), http://bit.ly/2xVGIUe.
17. Danielle Ivory and Hiroko Tabuchi, "Takata Emails Show Brash Exchanges About Data Tampering," *The New York Times*, January 4, 2016, https://nyti.ms/2IyXuwx.
18. "20th Death from Faulty Takata Air Bags Reported by Honda," *The Associated Press*, December 20, 2017, https://cbsn.ws/2Qt11iB.
19. "Takata Recall Spotlight," National Highway Traffic Safety Administration, http://bit.ly/2zPvvWx.
20. Michael Laris, "Takata Fined $70 Million for Deadly Air Bags, Subjected to Outside Overseer," *The Washington Post*, November 3, 2015, https://wapo.st/2Ro0ks8.
21. "Takata Agrees to $650-Million Settlement Over Air Bags but Will Pay Only a Fraction of It," *The Associated Press*, February 22, 2018, https://lat.ms/2yf9ezM.
22. Plaintiffs' Submission in Response to Pretrial Order No. 8 at 14 n. 31, In re Roundup Prod. Liab. Litig., No. 16-MD-02741-VC (N.D. Cal. July 10, 2018).
23. Id.
24. *Johnson v. Monsanto*, No. CGC-16-550128 (Cal. Super. Ct. 2018).
25. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 311 (S.D.N.Y. 2003)
26. "The Bottom Line: Evaluating and Controlling eDiscovery Costs," *Corporate Ediscovery*, May 22, 2018, http://bit.ly/2yafl8r.
27. Nicholas M. Pace and Laura Zakaras, "Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery," Santa Monica, CA: RAND Corporation, 2012, http://bit.ly/2OBvii0.