Professional Perspective

# Employee Communications Practices and Investigations

**Alexander J. Willscher, Anthony J. Lewis, and John B. Sarlitto**
**Sullivan & Cromwell**

Bloomberg Law

# Employee Communications Practices and Investigations

*Contributed by Alexander J. Willscher, Anthony J. Lewis, and John B. Sarlitto, Sullivan & Cromwell*

Courts have long recognized that the methods employees use to communicate are constantly changing. See, e.g. *City of Ontario* v. *Quon*, 560 U.S. 746, 759 (2010). Over the course of the last year, however, Covid-19 turbocharged that evolution. Novel communications practices that, under ordinary circumstances, would have been rolled out with careful supervision over the course of months or years—or that might never have been permitted at all—became necessary business continuity measures overnight. A year into the pandemic, it is clear that many of these changes have staying power.

In the investigations space, the consequences of novel employee communications practices will surface in backward-looking criminal and enforcement inquiries that examine a company's historical records, and in forward-looking imperatives to understand and regulate employee habits as a matter of policy and compliance.

It is an appropriate time to take stock: In the context of responding to government investigations, and crafting sound compliance and legal discovery strategies to anticipate them, what should companies be thinking about with respect to employee communication practices during this transitional period? In concrete terms, how are companies treating employees' use of personal devices or communications systems as a matter of compliance and policy, and in scoping their review and collection of materials in response to an investigation? And, conversely, are there limits to where a company can look within its own communications systems?

## Business Communications on Personal Devices and Platforms

The extent to which Covid-related remote work policies and business continuity measures influenced employee communications practices has varied across companies, offices, and even teams. Nevertheless, general fact patterns stand out. In the aftermath of initial stay-at-home orders, for example, employees may have turned with greater frequency to messaging platforms and applications, whether on personal or business-issued devices, to keep in touch with colleagues and third parties. Any increase to the volume of work-related communication made via text message, WhatsApp, or so-called "ephemeral messaging" apps—marketed as more privacy sensitive in that they purport not to preserve a communication after it is sent—exacerbated an area of compliance risk many companies had identified even before the pandemic.

Similarly, although some companies had already phased in such technology, a broader set of employees may have found themselves using virtual conferencing software and their inbuilt chat functions on a daily basis, in some cases before company communications policies, or company-issued hardware, had a chance to catch up. Employees may even have resorted to more regular use of personal email accounts for reasons as mundane as making it easier to print on a home network.

These new habits will matter in the course of future internal or government investigations, particularly at the outset, as a company scopes its response to an initial request for information or subpoena. Courts in the civil context have at times compelled discovery of business records from employees' and directors' personal devices and communications facilities. See, e.g., *Schnatter* v. *Papa John's Int'l Inc.*, 2019 BL 12904 (Del. Ch. Jan. 15, 2019). Broadly, companies will need to ask themselves to what extent responsive business records are likely to be found on personal devices and whether such records could be deemed within their possession, custody, or control.

There is more than one aspect to formulating an effective approach. There is a corporate policy question: What communications media are employees authorized to use—or prohibited from using—for work purposes? Are the policies governing the use of personal devices ("bring your own device," or BYOD) versus employer-issued devices clear, practical, and well-publicized? See generally Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 Sedona Conference Journal 496 (2018).

There is also a technical dimension: What categories of communication is the company technically able to collect itself, using available technology, including resources such as a mobile device management or "MDM" system? Finally, there is an important behavioral component: How familiar is the company—including its internal counsel—with its employees' day-to-day communications practices, including how they have evolved during Covid-19, and what has it done as a practical matter to channel communications into appropriate media and respond to lapses?

 

Discovering, managing, and disclosing any one-off, pandemic-induced gaps in a company's set of potentially responsive communications can go a long way toward building trust with a government team early in an investigation. But remaining on top of how employees communicate is more than a logistical discovery challenge. It is an issue that has attracted the attention of major regulators, and some government authorities will take the strength and reach of a company's communications-related policies into account when evaluating its compliance program when making charging decisions or awarding cooperation credit.

The Department of Justice's FCPA Corporate Enforcement Policy explicitly takes into account corporate "guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

As companies determine what appropriate retention means for them under this U.S. guidance, they should also recognize that this is a cross-border concern. The UK Financial Conduct Authority, for example, sounded a note of caution on the more frequent use of alternative communications applications in a January 2021 newsletter cautioning that "risks from misconduct may be heightened or increased by homeworking," in part because firms "will be less able to effectively monitor communications" made on WhatsApp and similar platforms. U.K. Fin. Conduct Auth., Market Watch 66, Recording telephone conversations and electronic communications (Jan. 11, 2021).

The investigations and enforcement ramifications of employees' communications practices are especially pronounced for entities subject to more robust recordkeeping requirements administered by the Commodity Futures Trading Commission, the Securities and Exchange Commission, and self-regulatory organizations. For regulated entities such as broker-dealers and futures commission merchants, a breakdown in employee communications processes or documentation around trading activity will not only complicate investigations into conduct that took place during the pandemic, a time of historic volatility in commodities and securities markets, but also could serve as the basis for a standalone enforcement action, even when the authorities are able to obtain communications on personal devices by directing a subpoena at the relevant individual.

Market regulators have expressly signaled that corporate supervision of employee communications practices is on their radar, and this attention will likely sharpen due to the pandemic's workplace disruption. Just prior to Covid-19's onset in the U.S., FINRA sanctioned a registered broker for his use of WhatsApp to communicate with overseas customers from late 2017 into 2019.

Because these communications were neither permitted by company policy nor captured by company systems, the FINRA staff found that the individual violated both the FINRA rule requiring the maintenance of books and records and FINRA's standards of commercial honor and principles of trade. The broker consented to FINRA imposing a suspension and fine in February 2020 to resolve the matter.

Later in the year, the SEC staff flagged the issue for broker-dealers and investment advisers in an August 2020 Risk Alert, which suggested that firms "may wish to modify" their supervisory and compliance procedures to address, among other things, "communications or transactions occurring outside of the Firms' systems due to personnel working from remote locations and using personal devices."

A September 2020 enforcement action against a broker-dealer for failing to preserve and produce text messages sent outside of authorized company channels illustrates the Enforcement Division's willingness to investigate and charge certain lapses. Not only were senior management and compliance leadership aware that employees texted both with others inside the company and with customers, each against company policy, the order found that they had even done so themselves.

As part of its remediation, the order notes that the company ultimately offered to provide all employees who wished to use their own mobile phones for work-related messaging with "a firm-sponsored software solution that preserves text messages sent or received for business purposes." The settlement illustrates that a corporate policy out of step with practice on the ground offers little protection from regulatory scrutiny, and that addressing electronic communications is not only a best practice, but a matter of enforcement.

## Personal Communications on Business Devices and Platforms

The persistent blurring of lines between home and work can complicate the converse scenario—employees' use of business systems and devices for personal communications that could become relevant to government investigations. In other words, even on the company's own systems, are there limits to where the company can look?

The most prominent example is the treatment of personal communications potentially subject to an individual employee's privilege, but made on company systems. This issue most frequently crops up in a civil litigation context, but this dynamic can also be treacherous for a company responding to a government investigation. In order to determine whether employees' expectation of confidentiality in such communications was reasonable, thereby preserving the privilege claim), courts regularly apply a test first articulated by the Bankruptcy Court in *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

The four factors courts look to are: does the corporation maintain a policy banning personal or other objectionable use, does the company monitor the use of the employee's computer or email, do third parties have a right of access to the computer or e-mails; and did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

The Delaware Chancery Court recently applied the *Asia Global* framework to require a company to produce what might otherwise have been considered privileged communications but for the fact that they occurred on another company's email system. *In re WeWork Litigation*, 2020 BL 498038 (Del. Ch. Dec. 22, 2020). Outcomes like this underscore the importance of policies and communications designed to reinforce employees' use of authorized systems for work-related communications.

Courts have also relied on this framework to uphold privilege claims over an employee's communications with his or her individual attorney, even when they occurred on an employer's own systems or devices. See, e.g., *U.S. v. Hatfield*, 2009 BL 246123 (E.D.N.Y. Nov. 13, 2009). Whatever the result, this inquiry is likely to be fact-intensive. See *Convertino* v. *U.S. Dep't of Justice*, 674 F. Supp 2d 97, 110 (D.D.C. Dec. 10, 2009).

Privileged communications, where the privilege belongs to an employee but not the company, on work networks and devices can be particularly thorny in an investigative context, potentially years down the line. It requires a thoughtful and potentially laborious procedure to identify and appropriately handle these communications in a manner that balances the equities and concerns of the government, current and former employees and their counsel, and the company.

It is a concern to keep in mind at the time employees are being provided individual counsel, as document collection and review progresses, and in scoping collection and production discussions with the government. And, of course, in crafting effective policies aimed at device use and document retention.

## Looking Forward

There is no universal playbook to managing the difficulties posed by shifting employee communications practices during a period when the very idea of a workplace has been redefined. There are, however, themes to aid companies and their legal advisors seeking to put themselves in the best possible position going forward to respond to and resolve government investigations:

- Companies, especially compliance and legal personnel, and the outside counsel that advise them, should strive to understand employees' communication practices and behavior, in particular in the current work-from-home environment, and be prepared for the possibility that those practices may endure once work returns to more normal conditions.

- Companies should consider how their policies and technical capabilities map onto what employees are actually doing, and proactively address any potential gaps that are discovered before they complicate or impede the company's ability to conduct a complete investigation and respond to a government inquiry.

- If an information request has already been received, consider the inquiries above at the outset to head off discovery surprises down the road.

- Finally, in addition to keeping their communications policies up to date, companies should ensure that they broadcast those policies widely to enhance employee awareness and compliance.