JONES DAY | One Firm Worldwide®

WHITE PAPER

October 2023

Considerations for Addressing DOJ's Corporate Compliance Guidance on Mobile Devices and Messaging Platforms

In light of the DOJ's most recent guidance on the use of personal devices and third-party messaging applications by corporate personnel, this *White Paper* addresses issues and challenges that companies are facing in this area and offers guidance on whether, and how, to update relevant corporate policies, procedures, and systems. The ubiquitous use of mobile devices and messaging applications to conduct company business, and the DOJ's heightened focus on the preservation of and access to data from these sources, make it important to consider, among other things, potential technological solutions for increasing control over corporate data generated by use of messaging platforms and stored on mobile devices, related training, and effective preparation for possible data collection.

TABLE OF CONTENTS

INTRODUCTION 1

DOJ GUIDANCE AND RELEVANT ENFORCEMENT ACTIONS 1

History of DOJ Guidance on Personal Devices and Third-Party Messaging Apps 1

Factors Used by DOJ to Assess Compliance Programs 2

Related SEC, CFTC, and FINRA Enforcement Actions 3

REALITIES OF BUSINESS COMMUNICATIONS 4

ASSESSING YOUR ELECTRONIC COMMUNICATION LANDSCAPE 5

Existing Policies, Procedures, and Acknowledgments 5

Communication Practices Among Employees 7

Technological Support for Policy Enforcement, Data Preservation, and Collection 7

Applicable Legal Framework and Data Protection/Privacy Regimes 7

UPDATING OR IMPLEMENTING RELEVANT POLICIES 8

General Policy Considerations 9

Company-Owned Devices vs. BYOD 10

Work-Related Communications 11

Retention of Electronic Data 12

Cooperation and Advance Consent 12

Exploring Technological Options for Increasing Control 12

TRAINING, MONITORING, AND CONTINUOUS IMPROVEMENT 13

Training and Communication 13

Attestations 13

Testing Policy Compliance 14

Disciplinary Action for Violations 14

Documentation 14

Continuous Assessment 14

PREPARING FOR POSSIBLE COLLECTION 15

CONCLUSION 16

AUTHORS 17

APPENDIX—Implementing DOJ Electronic Communication Guidance: Key Takeaways 20

ENDNOTES 21

INTRODUCTION

Earlier this year, the U.S. Department of Justice's Criminal Division ("DOJ") released updated corporate compliance program guidance,[1] including enhanced guidance on the use of personal mobile devices and third-party messaging platforms by employees to conduct company business. DOJ's updates in this area are, in many ways, an unsurprising reaction to what has become a pervasive use of mobile devices and messaging applications (or "apps") to conduct business in the United States and around the world. Because of the frequency and informality with which these communication channels are used, they are often one of the first areas of focus for companies, as well as for DOJ and other enforcement agencies, when conducting investigations into suspected misconduct.

DOJ recognizes that these communications are often critical to a company's internal investigations or compliance reviews and, of course, to DOJ's own investigations. Thus, the goal, from DOJ's perspective, is that companies have effective policies and procedures in place to "ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company,"[2] even when the data and communications reside on an employee's personal device or in a third-party messaging app.

Companies face practical challenges to ensuring the preservation of these electronic communications, both from a policy and technological perspective. Notably, DOJ does not provide prescriptive guidance nor does it advocate a one-size-fits-all approach; instead, DOJ counsels that policies "should be tailored to the corporation's risk profile and specific business needs."[3] As a result, companies implementing the DOJ guidance should not merely adopt an off-the-shelf, generic policy, but should instead assess their own needs and risks, depending on their business model and activities, the industries in which they operate, and the jurisdictions where they do business.

This *White Paper* considers the issues and challenges that companies are facing in determining how to address the pervasive use of personal mobile devices and third-party messaging platforms to conduct company business, and offers perspectives on deciding whether, and how, to make relevant changes, particularly in light of the DOJ guidance. Following a review of the guidance and tips for assessing a company's current electronic communication landscape, this *White Paper* addresses the considerations surrounding corporate policy updates; potential technological solutions for increasing control over corporate data generated by use of messaging platforms and stored on mobile devices; related training; and preparation for possible data collection and review.

DOJ GUIDANCE AND RELEVANT ENFORCEMENT ACTIONS

History of DOJ Guidance on Personal Devices and Third-Party Messaging Apps

Reflecting the ever-changing realities of technology and mobile device use in the modern workplace, DOJ's guidance related to personal devices and messaging apps has evolved significantly in recent years—from encouraging outright prohibition of ephemeral messaging apps to offering a more nuanced and risk-based approach.

In November 2017, DOJ announced a then-new FCPA Corporate Enforcement Policy requiring companies to prohibit their employees from "using software that generates but does not appropriately retain business records or communications" in order to obtain full remediation credit in FCPA matters.[4] But in March 2019, after pushback from the business community, DOJ modified the policy to remove the suggested ban on ephemeral communications. Instead, DOJ required companies seeking remediation credit to ensure the "[a]ppropriate retention of business records" and to implement "appropriate 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."[5]

In September 2022, DOJ extended its guidance addressing ephemeral messaging and electronic communications beyond the FCPA Corporate Enforcement Policy, announcing that "all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified."[6] DOJ also emphasized that whether a corporation

had instituted policies allowing it to collect and provide all relevant, non-privileged documents, including those stored on personal mobile devices used for business, would be an important factor in assessing a company's cooperation credit.[7]

Then, in March 2023, DOJ updated its Evaluation of Corporate Compliance Programs ("ECCP")[8] to include more detail regarding how prosecutors will evaluate whether a company has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms. DOJ emphasized that the policies and procedures should be tailored to the company's risk profile and outlined a number of factors to be considered, as detailed below.

Factors Used by DOJ to Assess Compliance Programs

Included in the ECCP[9] are the factors DOJ prosecutors are instructed to consider in assessing a company's compliance program in the context of any corporate investigation. Prosecutors are directed to use the ECCP in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (i) form of any resolution; (ii) monetary penalty, if any; and (iii) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).[10] Regarding electronic communications, the guidance directs prosecutors to consider "a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications" in determining whether to bring charges or in assessing an appropriate corporate resolution.[11] The guidance reflects DOJ's view that an effective compliance program is, in part, reliant on the corporation having mechanisms in place to allow for meaningful preservation, collection, and review of business communications for compliance-related purposes, regardless of whether those communications reside on company-owned devices or applications controlled by the company.

The factors that DOJ directs prosecutors to consider fall into three general categories—(i) the communication channels used by the company and its employees; (ii) the relevant policy environment; and (iii) risk-management considerations. In particular, the guidance suggests that a prosecutor's evaluation of these issues should include:

Communication Channels. What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?

Policy Environment. What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" ("BYOD") program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

Risk Management. What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's

compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization's affairs? Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?[12]

The overarching message is that DOJ expects companies to take steps to identify the communication channels their employees are using; to modify or adopt policies to permit the company to secure, monitor, control, and review business information in all relevant channels; and to evaluate and modify, if necessary, its practices to ensure relevant policies are communicated, followed, and enforced.

In remarks coinciding with the release of the guidance, a senior DOJ official emphasized DOJ's expectation that companies will tailor relevant policies and procedures to their specific risk profile and business needs, while still ensuring "as appropriate, [that] business-related electronic data and communications can be preserved and accessed."[13] This official added that "prosecutors will also consider how companies communicate the policies to employees, and whether they enforce them on a consistent basis."[14]

Similarly, DOJ's FCPA Corporate Enforcement Policy provides that for a company to receive full credit for timely and appropriate remediation, it must have "appropriate 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."[15]

It is now clear that DOJ is not recommending that companies prohibit their employees from using personal devices or third-party messaging apps altogether. It is also clear that what is "appropriate" when it comes to related controls and efforts toward preservation should be rooted largely in a company's own assessment of its business needs and the associated risks. What is sensible for one company may not be for another, particularly if the companies have different risk profiles and/or geographic footprints. Indeed, as a senior DOJ official has explicitly acknowledged, the guidance is not meant to be "prescriptive," and "[t]here is no one-size-fits-all" approach.[16]

Related SEC, CFTC, and FINRA Enforcement Actions

While DOJ has been focused on refreshing its guidance on these topics, the U.S. Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission ("CFTC"), and the Financial Industry Regulatory Authority ("FINRA") have been cracking down on firms in the financial services industry for failing to comply with more stringent recordkeeping rules that explicitly require those firms and other industry participants to preserve business-related communications.[17]

In recent enforcement actions, the SEC and the CFTC have pointed to "pervasive," "egregious," and "widespread" instances in which employees at all levels, including senior executives and supervisory personnel responsible for ensuring compliance with the firms' policies and procedures, were communicating about business matters through "off-channel" messaging apps (including Signal, Telegram, WhatsApp, and text messages on personal devices) and then failing to preserve those messages in contravention of the applicable rules and the firms' own policies and procedures.[18] To date, the SEC and the CFTC have brought more than 50 enforcement actions and ordered financial institutions to pay more than $2.5 billion in penalties for use of unapproved methods of communication.[19]

In announcing the settlements, the SEC and the CFTC emphasized the importance of the applicable recordkeeping requirements, with SEC leadership calling the rules "sacrosanct," and warning firms with outstanding recordkeeping issues to "self-report, cooperate and remediate."[20] And indeed, the SEC has given every indication that it will continue to focus on recordkeeping moving forward, as the SEC's Division of Examinations' 2023 priorities include a focus on broker-dealer compliance and supervisory programs, including those related to electronic communications.[21] More recently, the SEC's Director of Enforcement stated that the agency will continue to aggressively pursue cases related to ephemeral messaging.[22] The CFTC has echoed this sentiment, with CFTC leadership stating that "[t]he Commission's message could not be more clear—recordkeeping and supervision requirements are fundamental,

and registrants that fail to comply with these core regulatory obligations do so at their own peril."[23]

The SEC and CFTC orders include admissions by the settling firms and note that the firms cooperated with the agencies' investigations[24] and undertook initial remedial steps.[25] As part of the settlements, the SEC also required each of the firms to retain a compliance consultant to review and assess aspects of the firm's compliance program, including conducting:

- A comprehensive review of the firms' policies and procedures designed to ensure that electronic business communications, including those on personal devices, are preserved in accordance with federal securities laws.
- A comprehensive review of training undertaken by the firms to ensure compliance with electronic communication and personal device policies.
- An assessment of the "surveillance program measures" implemented by the firms to ensure compliance with the requirements to preserve electronic communications, including those stored on personal devices.
- An assessment of technological solutions implemented by the firms to ensure preservation of electronic communications.
- An assessment of measures used by the firms to prevent employees from using unauthorized communication methods.
- A comprehensive review of the framework adopted by the firms to address instances of noncompliance in the past.[26]

Like the SEC and the CFTC, FINRA has also brought recent enforcement actions involving failure to supervise employees' business-related communications and to preserve business-related text messages.[27] FINRA's 2023 Report on its Examination and Risk Monitoring Program highlights that firms should ensure (i) that they have a digital communications policy addressing all permitted and prohibited digital communications channels; (ii) that employees are trained on that policy; and (iii) that they implement procedures to review for red flags that may indicate a registered representative is communicating through unapproved communication channels.[28]

While the SEC, CFTC, and FINRA actions against financial services firms are reflective of the potential importance of policies and procedures focused on electronic communications, their broader applicability is limited in light of the heightened recordkeeping requirements applicable to that highly regulated industry. Nevertheless, *all* companies regulated by the SEC—even those outside of the financial services industry—can expect that during an investigation, the SEC will raise questions about the company's policies, including preservation and access policies, related to text messages, chats, and ephemeral messages.[29] Additionally, DOJ continues to focus on these messages as a source of valuable evidence.[30] As such, companies outside of the financial services industry should be proactive in assessing their approach to these issues, while recognizing that the particular risk factors associated with their industries and business operations may well counsel in favor of less stringent recordkeeping practices, consistent with DOJ's most recent guidance.

REALITIES OF BUSINESS COMMUNICATIONS

The DOJ guidance comes at a time when the global workforce is increasingly using mobile devices—and in many cases, personal mobile devices—to communicate about business matters. This trend has only become more widespread in the wake of the COVID-19 pandemic, as more employees are working from home, either on a hybrid or fully remote basis.

In a number of jurisdictions across the globe, it is now common practice to conduct business over third-party messaging apps, such as WhatsApp, WeChat, Signal, and Telegram. Use of these communications channels, of course, does not itself indicate any nefarious intent; rather, as DOJ's move away from urging companies to prohibit ephemeral communications suggests, these channels are tools of ease and convenience that promise to become even more, not less, prevalent for both intra- and inter-company business communications going forward. Indeed, in some cases, employees may not independently choose to use messaging apps to communicate, but they may be driven to those channels based on customer preference or demand. In other cases, an employee may simply be responding to a message received directly from a supplier out of convenience and efficiency without stopping to consider whether that message is subject to—or should be preserved in accordance with—the company's retention policies.

Many times, communications on third-party messaging apps are conducted on an employee's personal device, whether or not that device is part of a corporate BYOD program. For security and data management reasons, companies often prevent employees from downloading these messaging apps on company-issued devices. While employees may routinely use their personal devices to conduct business in good faith, there are also instances in which employees shift communications "off-channel" intentionally to avoid corporate monitoring or preservation requirements. These employees often believe their communications are out of reach—from either their employer or regulatory authorities. And while data privacy laws and nascent corporate policies have, in many cases, made those communications difficult for companies to access, DOJ's guidance reflects a desire for companies to do more on the front end to be able to access data on an employee's personal device should the need arise.

Indeed, companies should expect that in the event they receive a subpoena or other request for documents from a regulatory agency, particularly one in the United States, they will be asked to produce not just policies and procedures addressing electronic communications and mobile devices, but also relevant business-related information on their employees' personal and company-issued devices and from third-party messaging apps. Standard language in subpoenas from U.S. regulatory agencies now specifies that—from the perspective of the relevant enforcement authority—"communications" include virtual conversations, text messages, instant messages, chat messages, and encrypted communications, in addition to emails, other traditional correspondence, and voicemails. Such subpoenas also typically indicate that responsive material should be produced regardless of its location, including from personal email accounts and personal electronic devices. In remarks earlier this year, a senior DOJ official explained that if, during a DOJ investigation, a company does not produce employee communications from "third-party messaging applications, our prosecutors will not accept that at face value[, and t]hey'll ask about the company's ability to access such communications, whether they are stored on corporate devices or servers, as well as applicable privacy and local laws, among other things."[31]

ASSESSING YOUR ELECTRONIC COMMUNICATION LANDSCAPE

For many companies, the first steps in determining whether to implement policy changes and update mobile device practices in response to DOJ's guidance will be to (i) identify and assess all existing relevant policies; (ii) understand the realities of how employees are communicating across the company and current methods of preservation; and (iii) analyze potential legal implications across the jurisdictions in which the company operates to determine whether a more nuanced approach is required in some areas. A fulsome risk assessment may also allow a company to consider whether specific jurisdictions or business functions require more attention—either through training, policy monitoring and enforcement, and internal audits, or through the use of technology that can assist in actively preserving communications on mobile devices.

Existing Policies, Procedures, and Acknowledgments

In the first instance, a company might think broadly about all existing policies and procedures that address how its employees are permitted to communicate about business matters, the situations in which the company can request or obtain access to data contained on an employee's corporate-issued and personal devices, retention of company data, cooperation with internal investigations and other compliance or HR matters, and collection or imaging of devices. Companies could have a number of policies, procedures, and user agreements in place that touch on one or more of these topics, so it is a helpful exercise to understand how those policies work together, whether there are any issues with consistency, and whether there are any gaps. Because some companies may have global policies or employee handbooks that apply regardless of location, as well as more targeted jurisdiction-based policies, the process of collecting and analyzing all potentially applicable policies may be time-consuming but is worth the effort.

The following provides guidance on the types of policies that might be identified and the specific questions that can be considered as a part of this process:

What existing policies, procedures, or agreements might contain relevant guidance?

- Code of conduct
- BYOD or personal device policies
- User agreements
- Policies addressing data security and data privacy
- Policies addressing appropriate use of company information technology and company data
- Policies and procedures addressing electronic communications and/or social media
- Data/document retention policies and procedures
- Policies covering cooperation with investigations or compliance reviews
- Acknowledgments regarding a lack of expectation of privacy in company-owned or operated information technology and equipment
- Advance consents for access to and collection/review of business data on company or personal devices

What questions should be assessed in the course of a policy review?

- What is the universe of company policies relevant to the use of company-owned or BYOD devices and messaging apps?
- Do the company's policies clearly address the company's rights to access, image, transfer, and review all data on any company-owned or company-issued device?
- Is there an existing policy that addresses the situations in which the company can access, image, transfer, and review business-related data stored on personal devices or in personal applications contained on a BYOD device? If so, does the policy address situations in which the company may access personal data in the course of collecting and reviewing business-related data?
- Do the company's policies specifically address guidelines for business-related communications, including the channels that are permitted (or prohibited)?
- Do data retention policies address retention of all business-related data (including data stored on personal devices or in personal applications contained on a BYOD device)? How do policies and/or procedures address preservation of business-related information on devices that are replaced?
- Are there any inconsistencies or gaps among relevant policies that might lead to confusion among employees about the use of/access to personal devices and business data contained within third-party messaging apps?
- Would the company benefit from consolidating information regarding mobile device usage/access into a single policy?
- Have employees executed any acknowledgments or attestations in connection with any of the existing policies?
- How and when are the policies and procedures communicated to employees, and what training is offered?
- How often are the policies reviewed and updated to keep up with technological developments and legal changes?
- How does the company test compliance with the policies?
- How do relevant policies address consequences for violations?

Communication Practices Among Employees

In addition to understanding the nature and scope of any existing policies that address mobile devices and electronic communications, a company should seek to understand how its employees are actually communicating in the different jurisdictions in which the company operates and across different business functions. For some companies, information about communication practices among employees may be readily available in light of recent investigations, compliance reviews, or litigation. For others, there may be some level of uncertainty about how employees are communicating internally and externally for business purposes. Given the ubiquity of communication technology and the realities of human nature, companies may need to take steps to test the assumption that employees are communicating only via approved channels, even if corporate policy prohibits the use of personal devices or third-party messaging apps. The likelihood is that in some (or all) locations, employees are conducting at least some company business on their personal devices or by means of third-party messaging apps, regardless of any such prohibition.

To better understand actual employee communication practices, companies could audit company-issued devices, distribute anonymous surveys, or conduct targeted interviews for the explicit purpose of assessing potential policy improvements (rather than enforcing existing policies). Questions can be developed to elicit information not just on how the responding individuals personally communicate internally and externally for business purposes, but also about what those individuals understand regarding how others within the company communicate—particularly as it relates to personal devices or messaging apps. Companies can also ask employees why they choose to use particular methods of communication. Analysis of the responses can help inform a company's overall approach with respect to mobile devices and can also help identify jurisdictions or business units that may pose a more significant risk when it comes to the company's ability to preserve business-related communications.

Technological Support for Policy Enforcement, Data Preservation, and Collection

In assessing the need for policy and/or technological enhancements focused on mobile devices and electronic communications, companies can also work with their IT professionals to understand existing permissions and/or limitations on various communication channels on company-issued and/or BYOD-enrolled devices. For example, if there is an approved messaging app that employees can use on their mobile devices, the company should understand the current preservation settings and both the company's and the employee's ability to modify those settings. The company should also consider its internal capabilities for mobile device collection and preservation, as well as its ability to monitor employee communications on apps installed on company-issued and/or BYOD-enrolled devices. Companies can also use these discussions as an opportunity to confirm with their IT professionals that broader preservation and retention policies are being followed operationally.

Applicable Legal Framework and Data Protection/Privacy Regimes

Finally, for companies with employees dispersed across the globe, consideration should be given to the various laws and regulations that inform how a company can access, collect, transfer, and review data from personal devices, as well as communications containing personal information. The legal landscape in the United States differs, for example, from that which would inform the approach in the European Union ("EU") or China. In some jurisdictions, employees must explicitly consent to the collection of any data from company-issued or personal devices. In others, there are industry-specific laws that dictate how information must be collected and secured. So while a company may be able to adopt or maintain a single policy addressing mobile devices and third-party messaging applications (to be executed in accordance with applicable laws and regulations), it should also assess the need for any additional jurisdiction- or industry-based procedures or consents.

Example: Data Privacy and Data Security Considerations in China and the EU

For example, data privacy laws, including the Personal Information Protection Law ("PIPL"), applicable in China, and the General Data Protection Regulation, applicable in the EU, impose restrictions on the ways in which personal information can be collected and processed. Subject to limited exceptions, an employee's personal mobile device—or communications contained within personal apps on a device enrolled in a BYOD program—can be accessed only after acquiring informed, voluntary, and explicit consent from the relevant employee.[32] As such, policy language stating that the use of a personal device for business purposes will necessarily constitute advance consent for the company to access that device for internal investigations, compliance, or other enumerated purposes may, in certain cases, be insufficient.[33]

Under PIPL in particular, exceptions to consent requirements are vague and have not been the subject of meaningful judicial interpretation. But in practice, companies have relied on the necessity of fulfilling "human resources duties" and "statutory duties" to fill the gap in situations where obtaining an employee's consent is not practical or where any existing consent is limited in scope or has been withdrawn by the employee.[34] Companies may also negotiate with employees about selective or partial collection of information if an employee is unwilling to consent to a full image of a personal device.

Note that in both China and the EU, companies must also pay special attention to situations in which the cross-border transfer of Chinese or EU data may be involved.[35] Applicable data privacy laws restrict the ways in which certain types of data can be transferred outside of these jurisdictions and, in China, even provide for potential criminal penalties in the case of certain types of violations.[36]

UPDATING OR IMPLEMENTING RELEVANT POLICIES

Once a company understands how its current policies align with the communication practices of its employees and applicable data privacy laws, it should consider whether to update its policies to clarify use, preservation, and access issues, or whether to adopt an entirely new or supplemental mobile device and/or electronic communications policy. Although companies may be concerned about how policies authorizing the access, collection, and review of data originating from personal devices could motivate plaintiffs in civil discovery, that concern should be balanced against the company's need to access the information for compliance and other purposes.

General Policy Considerations

Although the details will vary depending on a company's risk profile and the jurisdictions and industries in which it operates, the following provides a high-level overview of the content that policies related to mobile devices and messaging apps should generally address:

Content of Policies Addressing Mobile Devices and Messaging

- **Purpose and Scope** of the company's policies should be set forth expressly.
- **Definitions**, including definitions of key terms, e.g., "company data" and "personal data."
- **Technical and Security Requirements** for company-owned devices or personal devices that are part of a BYOD program. These requirements may include:
  - Data encryption and password protection requirements;
  - Required device settings;
  - Preferred and/or prohibited applications for work-related communications;
  - "Blacklisted" applications that pose a security risk and cannot be downloaded onto the device; and
  - Any required mobile device management ("MDM") program.
- **Confidentiality and Acceptable Use Requirements**, which outline employee obligations with respect to maintaining the confidentiality of company data, as well as policies related to the acceptable uses of company-owned devices, systems, and networks.
- **Expectation of Privacy**: This will vary depending on whether the employee is using a personal or company-owned device, but generally employees should have no expectation of privacy as to company data, regardless of where that data is located.
- **Access to Data**, including identifying the circumstances under which the company may access company data and image company data from both company-issued and personal devices, and as well as when the company may review, process, and transfer that data. The policy should also address an employee's obligations in providing access to relevant devices when required, and whether, and in what circumstances, a company can remotely wipe a device.
- **Maintaining and Safeguarding**, including the employee's obligations for maintaining and safeguarding the device, including reporting obligations if the device is lost or stolen.
- **Data Retention and Back-Up**, whether for company-owned or BYOD devices, including data contained in third-party messaging apps.
- **Training and Disciplinary Actions**, including required employee training and consequences to employees for violations of the policies, up to and including termination of employment.
- **Device Replacement**, including procedures for preservation of company data on devices that are replaced in the normal course.
- **Termination of Employment**, which may include required procedures to be followed upon termination or separation of an employee, including returning any company-owned devices and returning or deleting company data stored on personal devices.
- **Acknowledgement**: Employees should be required to expressly accept the policies' conditions and periodically certify compliance with their requirements. In some jurisdictions, more specific consents may need to accompany an employee's acknowledgment of the mobile device policy in light of applicable data privacy laws.

Company-Owned Devices vs. BYOD

Company-Owned Devices. A company's mobile device policies will necessarily be impacted by whether the company provides company-owned devices to its employees or implements a BYOD program where the devices are employee-owned (or some combination of the two). On the one hand, company-owned devices provide the company with more control over the device itself, such that the company can configure the device to mandate certain security and/or data retention settings, including those relating to data encryption, password protection requirements, application installation, and default data retention. It may also be easier for companies to configure company-owned devices so that they can be remotely wiped in the event that they are lost, stolen, or otherwise compromised. Company-owned devices also reduce ambiguities surrounding data ownership, making it easier for companies to access data in the event of an internal investigation, government subpoena, or other external request, and to control the disposition of data if the device is replaced or if an employee is terminated or leaves the company. On the other hand, company-owned devices can be an administrative burden. They may increase hardware and wireless services costs to the company, as well as IT costs associated with maintaining and supporting a fleet of company-owned devices. Additionally, the inconvenience associated with carrying two mobile devices may cause employees to be less accessible on a company-owned device or to use their personal device for company business, particularly if they previously communicated about business on an app that is blocked on the company-owned device.

When issuing devices to employees, companies should consider expressly stating in corresponding policies and/or acknowledgments that the company owns the device and, where consistent with applicable data privacy laws, that employees have no expectation of privacy when using the device. The policies may also provide clear guidance to employees regarding personal use of the device, including whether, and to what extent, personal use of the device is permitted. In some jurisdictions, policy language limiting or prohibiting personal use may facilitate accessing, imaging, and reviewing data on a device because, consistent with the policy, the device should not contain personal data.

BYOD Program. A BYOD program, which allows employees to use a personal device for company business, may bring with it a number of benefits, including reducing hardware costs to companies and increasing convenience to, and productivity of, employees. However, BYOD programs also can carry security and access risks. As such, companies with BYOD programs should ensure that they have appropriate technical solutions, policies, and procedures in place to mitigate these risks.[37]

In addition to the general considerations outlined above, companies drafting BYOD policies should aim to eliminate ambiguities regarding ownership of and access to data. To accomplish this objective, companies might expressly state that the company owns any and all company data sent, received, or stored on a personal device that is part of the BYOD program, including all business-related communications on the device, regardless of their location. In addition, companies should consider providing clear guidance on what applications are permitted to be used for conducting company business and storing company data. In making these determinations, companies should consider—among other things—security, how easily data can be preserved and accessed, and whether the application can be used to communicate with both other employees and third parties. BYOD policies should also include a detailed description of the circumstances in which the company may access the device (e.g., for certain specified compliance and HR purposes, investigations, or to respond to government requests/demands), including any necessary limitations on what portions of the device may be accessed by the company; the employee's obligations in permitting the company to access the device and company data stored on the device; and policies related to commingling company data and personal data. Finally, as discussed below, companies should also consider whether software or other technological measures can be used to facilitate control of company-owned data on BYOD devices.

With advances in technology, companies do not always need to make a binary selection between company-owned devices and BYOD programs. A third option, which operates as a hybrid between company-owned devices and BYOD, is to add a company-paid Voice over Internet Protocol ("VoIP") on an employee-owned phone. This solution allows an employee to use their own device, but to receive phone calls and text messages on a separate company-owned VoIP line, providing additional separation between company data and employee data.

Work-Related Communications

Considerations for Work-Related Communications. Regardless of whether a company provides employees with company-owned devices, institutes a BYOD policy, or takes some combination of both approaches, company policies should set clear guidelines for work-related communications. In addition to all of the issues discussed above related to company-owned devices and BYOD programs, companies should consider the following:

- Policies related to confidentiality of company data and information, including any restrictions on use of particular types of information (e.g., protected health information or material non-public information);
- Policies related to use of social media;
- Preferred platforms for work-related communications, such as company email or company-controlled applications with chat functions like Microsoft Teams, Slack, Skype, or Google Chat;
- Whether work-related communications are permitted on SMS text message or iMessage and, if so, any related usage and preservation guidelines;
- Whether work-related communications are permitted on third-party messaging apps, such as WhatsApp and WeChat, and, if so, any related usage and preservation guidelines;
- Whether work-related communications are permitted on third-party ephemeral messaging apps, such as Telegram and Signal, and, if so, any related usage and preservation guidelines;
- Any blacklisted or prohibited applications for work-related communications;
- Guidelines for employees if a third party (such as a customer or vendor) contacts the employee on a non-approved communication channel; and
- Policies related to retention of company-related communications and data.

Again, the particulars of policies related to business communications will depend on the company's unique risk profile, including risks associated with the nature of the company's business and the jurisdictions in which it operates.[38] Companies should also consider the reality on the ground—i.e., what applications their employees actually use for business communications, with whom these communications occur, and with what regularity. This assessment should be made in every jurisdiction where the company operates, as local business customs will vary. And depending on what that assessment shows, consideration should be given to whether a global policy or individual, jurisdiction-specific policies should govern.

Third-Party Messaging Apps. Consistent with DOJ's guidance, companies should also consider addressing specific issues related to the use of third-party messaging apps, including ephemeral messaging apps. Use of these apps has increased dramatically in the past several years, driven by increased "smart" mobile device use and adoption of BYOD policies, as well as the increase in "work from home" policies that accompanied the Covid-19 pandemic. However, such apps may be particularly challenging from a monitoring and preservation perspective, as they may allow an employee to send messages or otherwise communicate anonymously; may be "ephemeral," such that messages are automatically deleted or destroyed after they are read; and/or may encrypt messages in a way that prevents third-party viewing or back-up. Nevertheless, an outright ban on third-party messaging apps may not be appropriate or feasible for companies, particularly in certain jurisdictions. Indeed, as noted above, even DOJ has recognized that a ban on third-party messaging may not make sense for all companies—as one senior DOJ official observed, "We're not telling companies they can't use WhatsApp."[39] Instead, DOJ expects companies to be able to demonstrate that they have thought carefully about their ephemeral messaging policies in the context of the overall compliance program.[40]

A careful thought process should include consideration of how best to mitigate risk where banning a particular third-party app may be difficult (e.g., in a jurisdiction where, as a practical matter, most individuals—including employees, vendors, and customers of the company—communicate about business using that application). In this regard, companies should consider the security of the third-party application; what retention options are available—either as part of the app settings or as a separate obligation imposed on the employee; and what alternative apps are available for use.

After assessing potential risk, if a company determines it is critical (or even, on balance, advisable) that employees be able to use certain third-party messaging apps for business-related communication, companies should consider providing clear guidance regarding the preservation of those

communications. And even if a company decides to prohibit the use of third-party messaging apps in the normal course, it should still provide preservation-related guidance in the event a customer, vendor, or other third party contacts the employee regarding company business on a third-party app that does not typically allow for message retention. Companies should also consider policy language that makes clear that any business use of a third-party messaging application—even on a personal device—constitutes advance authorization for the company to access, collect, process, review, and transfer such data (consistent with applicable data privacy laws).

Retention of Electronic Data

Companies should also consider, more generally, DOJ's guidance that companies should design their policies and procedures to "ensure that business-related electronic data and communications are preserved."[41] In the context of its FCPA enforcement-related guidance, DOJ has further counseled that such retention should be "[a]ppropriate" and that companies should and "prohibit[] the improper destruction or deletion of business records, including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms."[42] DOJ has provided little clarity on what constitutes an "appropriate" retention of records, but that analysis will necessarily depend on a number of factors, including the company's risk profile and any applicable regulatory record-keeping requirements. Of course, companies in industries with stringent regulatory record-keeping requirements generally face greater enforcement risk for possible record-keeping violations, as evidenced by recent enforcement actions by the SEC and the CFTC. But all companies should have document and data retention policies that work in tandem with their mobile device and business communication policies. As they relate to mobile data and messaging, these policies should clearly describe employees' data preservation obligations, including what data must be preserved and for how long, as well as the preferred method of preservation. As with the other policies, employees should be expressly required to acknowledge that they have read, understand, and will comply with the policy.

Cooperation and Advance Consent

If not already in place, companies should also strongly consider adopting a policy (or revising an existing policy, such as the code of conduct) requiring employees to cooperate with internal investigations, compliance or human resources inquiries, and/or other litigation or enforcement matters or face discipline, up to and including termination. An express duty to cooperate can help facilitate an employee's participation in interviews and other fact-gathering processes, including the preservation and collection of relevant data. If not already included elsewhere, this type of policy can be a natural place to incorporate a provision explicitly requiring employees in certain circumstances, such as internal or regulatory investigations, to permit the company to access any devices (corporate-issued or personal) and apps containing business-related data or communications. For companies with a BYOD program, this provision would include allowing access to any personal apps on BYOD-enrolled devices that contain business-related data or communications.

In addition to adopting a clear policy, companies should also consider obtaining explicit advance consent from employees permitting access to, and collection of, all company-owned data, even (or especially) where the data is stored on a personal device. At the same time, companies should ensure they understand whether applicable data privacy laws in the jurisdictions in which they operate might require a different approach (e.g., require the employee to provide separate, informed, and written consent to collection for a particular matter).

Exploring Technological Options for Increasing Control

Although clear and comprehensive policies and procedures regarding the use of mobile devices and messaging apps can be critical, even the most carefully crafted policies can be ignored or circumvented by bad actors or well-meaning, but imprudent employees. As such, companies can explore technology-based options to increase visibility, prevent circumventions of company policy, and/or preserve relevant data, particularly if there are areas where the company's risk profile merits such increased control. Companies can implement mobile application management solutions, which allow companies to manage and secure certain corporate applications and data, without having control over the entire device. Depending on their security and management needs, companies may choose to implement MDM solutions, which allow for more centralized control over devices, including device configuration, security policies, device tracking for lost devices, and remote wiping if a device is lost or otherwise compromised. Companies adopting MDM solutions may also include application surveillance, by which companies can track the

applications installed on devices but cannot see the data stored on those applications. Application surveillance can be useful in the event of a subsequent investigation or regulatory inquiry insofar as it allows companies to have visibility into which applications a particular employee downloaded at a given point in time (providing insight into which applications the employee could have been using to communicate about business), as well as whether any of those applications were deleted prior to data collection.

In industries in which specified data preservation is mandatory (e.g., financial services), tools that facilitate the regular and routine archiving of communications from third-party messaging apps can be critical. Outside of those industries, companies should, on a continuous basis, weigh the security and visibility benefits of any technological solutions against their costs. For companies with employees in high-risk business units within high-risk jurisdictions that regularly use third-party messaging apps for key business discussions, an archiving tool could be worthwhile. In other lower-risk areas, a clear retention and cooperation policy may be sufficient even where the use of third-party messaging apps is likely. This risk-bound cost-benefit analysis may change over time as business practices evolve and available technological solutions become cheaper or more effective.

TRAINING, MONITORING, AND CONTINUOUS IMPROVEMENT

Following a review and appropriate modification of policies addressing the use of mobile devices, messaging apps, and related preservation and cooperation requirements, companies should consider how best to communicate and train employees on the policies, monitor compliance, address any policy violations, continuously assess policy effectiveness, and incorporate any lessons learned through these activities.

Training and Communication

Training related to the company's mobile device and messaging policies should be incorporated into the company's overall compliance training. At a minimum, mobile device and messaging policy training should be required for all employees who use a company-owned device, are enrolled in a BYOD program, or might otherwise communicate electronically about company business. Generally, training should be required when new employees are onboarded. For existing employees that have already been trained, companies should consider how frequently to require refresher training, particularly as the underlying policies, procedures, or training modules are updated. Companies should also consider whether to provide tailored or more extensive training to certain categories of employees (e.g., those in high-risk positions or who work in high-risk jurisdictions), and should assess whether to provide training to any third parties who might communicate electronically on their behalf.

As with all training, companies should consider the form and content of the training, including whether the training is effectively communicating the policies and procedures related to mobile devices and messaging. Companies should consider whether to offer training in non-U.S. jurisdictions in local languages and should provide ample opportunity for employee questions. Companies can also incorporate a process to assess the effectiveness of the training (e.g., requiring employees to take a quiz on the content of the training) and should make periodic updates to incorporate the latest regulatory guidance and lessons learned from prior compliance issues.

Particularly where policies have been updated, modified, or newly implemented, leadership should strongly consider prompt and clear communication of the policy updates or changes to all employees. And aside from formal training, companies should assess whether other periodic communications or reminders about the policies are warranted. Companies should also make sure that there are resources from which employees may seek guidance about the policies and that employees are aware of these resources.

Attestations

Companies may also require employees to sign attestations related to the mobile device and electronic messaging policies, either as a stand-alone process or as part of a broader compliance program, training, or code of conduct acknowledgement. Generally, such an attestation would require an employee to certify that the employee has read, understands, and will comply with the policies related to mobile devices and messaging. An attestation might also require an employee to certify that the employee completed the required compliance training related to mobile devices and messaging, understood the content of the training, had an opportunity to ask questions related to the training, and is aware of company

resources for reporting violations or seeking guidance on any future questions or concerns. Finally, after the initial attestation, companies might periodically require additional attestations through which an employee certifies his or her continued compliance with the policies. These periodic attestations can serve as reminders, reinforcing the compliance expectations and increasing employee engagement.

Based on the results of a risk assessment, a company might also consider customizing attestations for certain employees (e.g., requiring more frequent certifications from employees in high-risk positions or in high-risk jurisdictions).

Testing Policy Compliance

Potential wrongdoing or violations of the policies may be investigated through the company's normal internal investigation process. However, companies can also consider the availability of proactive, non-investigation mechanisms for testing the effectiveness of their policies related to mobile devices and messaging. Such mechanisms will necessarily vary depending on the nature of the devices used by employees (i.e., company-owned or BYOD) and the company's risk profile, but they might include periodic internal audits or monitoring the frequency of communications on company-owned apps for anomalies (e.g., an unusual decrease in the volume of communications on company-monitored channels may signal use of unauthorized devices or messaging apps). Auditing employee communications in the absence of any active investigation or inquiry is not required across the board and, in fact, may not be permitted under applicable law. Indeed, one senior DOJ official has said that DOJ does not expect companies to audit the personal devices of employees, particularly where doing so might violate applicable data privacy laws.[43] Nevertheless, regardless of how a company tests compliance with its policies, it should be able to demonstrate that employees are well-informed of the company's mobile device and messaging policies.[44]

Disciplinary Action for Violations

DOJ has made clear that, from its perspective, simply having policies on mobile devices and messaging is not sufficient; companies should also be able to demonstrate that the policies are being enforced. Consistent with this guidance, policies should typically include specific information regarding disciplinary action for violations of the policy. Violations in this context could include communicating about company business on non-approved apps, deleting or attempting to delete company data that the employee was required to preserve, or refusing to allow the company to access a device to review business-related communications or data (where allowing access is required under company policy and is consistent with applicable data privacy regulations). Depending on the nature of the violation, disciplinary action could range from a warning or reprimand, to additional training, to withholding or reducing bonuses, up to termination.

When a company discovers violations of the policy, whether during a routine internal audit or an investigation, it is important to consider what disciplinary action is appropriate, consistent with the policy and the surrounding facts and circumstances. A company's history of enforcing its policies by imposing appropriate disciplinary action for violations on a reasonably consistent basis will be a key step in demonstrating the effective operation of this aspect of the corporate compliance program.

Documentation

Companies should also have procedures in place to document all relevant consents, attestations, trainings, remediation efforts, and disciplinary action. While documentation can be critical for demonstrating a company's diligence in any future regulatory inquiry, it can also serve as an important internal tool. For example, in an investigation, documentation of prior consent or attestations might be critical in gaining access to an employee's device. Documentation can also be enormously beneficial for continuous evaluation and assessment of whether the policies are being implemented and enforced appropriately. A pattern of similar unintentional violations by employees may indicate a gap in training that should be addressed. Documentation of initial disciplinary actions may also be crucial in the case of repeat offenders, where more serious action may be warranted for subsequent violations.

Continuous Assessment

Finally, as with all aspects of a corporate compliance program, companies should consider mechanisms to routinely assess whether the policies are effective and to incorporate any lessons learned. Such routine assessment is particularly critical here, as technology is rapidly evolving, both with respect to the messaging apps themselves and the technology available to companies to preserve and monitor communications.

Companies should consider reviewing the results of investigations, internal audits, and any ongoing monitoring or data analysis to identify areas where policies need to be clarified or updated, as well as areas where employees may need additional training. Further, given the swiftly evolving technological landscape, companies should regularly work with their IT teams to identify new applications, threats, or other technological advances that should be incorporated into policies and training materials. Any policy updates should be promptly and clearly communicated to all employees and other stakeholders.

PREPARING FOR POSSIBLE COLLECTION

Even where company policies clearly set forth expectations and procedures regarding access to company data on mobile devices and where employees expressly agree in advance to provide such access, employees faced with imminent collection may have questions and concerns when asked to provide devices for data collection and review. To alleviate these concerns, companies should, to the extent possible, clearly communicate to affected employees the purpose, scope, and details of the data collection, including any encryption and security measures for storage of the collected data. Companies should also remind employees of their rights and obligations (e.g., any company policies requiring employees to cooperate in investigations or inquiries), as well as any prior consent to access given by the employee.

In many cases, employees are not concerned about the collection of company data from their device; instead, they are principally concerned about the possibility that the collection will also include personal data. Recognizing and acknowledging those concerns in conversation with relevant employees can be helpful in facilitating a less contentious and more successful collection. In jurisdictions with more stringent data privacy laws, however, an employee may arguably have a right to refuse to provide their device for data collection and review if they are concerned that the collection will include personal information. This may be true even if the employee previously signed an advance consent to collection. As a result, companies should be prepared to engage with any such employees on the applicable policies, the importance of cooperation, the safeguards that will be applied to protect or filter out personal data, and in some cases, alternatives to making a complete image of the employee's device.

From a technical standpoint, even where company data and personal data are not entirely commingled, it may be difficult to filter out personal data at the collection stage. Depending on the model of the device, the scope of the collection, and the apps installed on the device, a data vendor or IT personnel may need to collect the entire device and filter out irrelevant data after the data is processed. In other instances, filtering may be possible at the time of collection, such that only certain apps, date ranges, or even specific conversations are collected. Prior to initiating collection, companies should determine what pre-collection and post-collection filtering is available for the device at issue, so that those requesting access to data from employees are armed with details on the process.

Depending on the purpose of the collection and any applicable data privacy laws, companies may also need to be prepared with matter-specific consent forms at the time of collection that indicate an employee's specific and informed consent to the imaging of their device. In some cases, companies might consider including on the consent form that the employee agrees to any necessary transfer of information to third parties acting on the company's behalf or to regulatory authorities or judicial bodies within or outside of the country in which the employee is located. Matter- and jurisdiction-specific considerations will dictate whether a company is better served, from a risk perspective, by trying to seek specific consent for the collection of a device or by relying on potentially applicable exceptions to any consent requirement.

Despite a company's best efforts in assessing risks, implementing and communicating effective policies, and otherwise preparing for possible collection of mobile device data in the future, there will undoubtedly be challenges that arise in the process of collecting employee data. When those challenges arise, companies should use them as an opportunity to reassess and improve their processes. And where policy violations occur or are otherwise identified in the course of a collection, companies should take steps to ensure that the issues are addressed and, where appropriate, disciplinary action is

taken. Should a company ever be in a position of needing to explain its compliance efforts in this space, the company's steps toward continuous improvement will be an important part of the story.

CONCLUSION

With the ubiquitous use of mobile devices to conduct company business and DOJ's heightened focus on the preservation of and access to mobile device and messaging app data, companies should at the very least reassess their relevant policies and consider whether there is any need for related compliance and technological enhancements. Given the complexities associated with jurisdiction-specific data privacy and labor laws, companies will likely need to involve a multidisciplinary team in considering how best to address relevant electronic communication risks. And while sensible data policies contribute to good corporate governance and efficient operations, and attention to these issues is unquestionably warranted in any event, companies should also remember that DOJ's guidance in this regard is not prescriptive, nor does it have the force of law. Put simply, there is no universal approach that will be effective or advisable for every company. Steps taken by financial institutions in the wake of the recent SEC, CFTC, and FINRA enforcement actions can be a helpful reference point, but companies should also keep in mind the unique aspects of those highly regulated industries whose participants are bound by specific recordkeeping requirements. For participants of other industries, there is likely to be considerably greater room for discretionary judgments in addressing employee use of personal devices and third-party messaging apps—judgments that should be informed by regulatory guidance and grounded in the companies' unique and carefully assessed risk profiles.

AUTHORS

Theodore T. Chung
Chicago
+1.312.269.4234
ttchung@jonesday.com

Henry Klehm III
New York
+1.212.326.3706
hklehm@jonesday.com

Heather M. O'Shea
Chicago
+1.312.269.4009
hoshea@jonesday.com

Lisa M. Ropple
Boston
+1.617.449.6955
lropple@jonesday.com

Bethany K. Biesenthal
Chicago
+1.312.269.4303
bbiesenthal@jonesday.com

Jennifer C. Everett
Washington
+1.202.879.5494
jeverett@jonesday.com

Lillian He
Shanghai
+86.21.2201.8034
lhe@jonesday.com

Justin E. Herdman
Cleveland
+1.216.586.7113
jherdman@jonesday.com

Karen P. Hewitt
San Diego
+1.858.314.1119
kphewitt@jonesday.com

Samir Kaushik
Dallas
+1.214.969.5092
skaushik@jonesday.com

Leigh A. Krahenbuhl
Chicago
+1.312.269.1524
lkrahenbuhl@jonesday.com

Jerry C. Ling
San Francisco
+1.415.875.5890
jling@jonesday.com

Sidney Smith McClung
Dallas
+1.214.969.5219
smcclung@jonesday.com

David Peavler
Dallas/Washington
+1.214.969.5092/+1.202.879.3499
dpeavler@jonesday.com

Brian C. Rabbitt
Washington
+1.202.879.3866
brabbitt@jonesday.com

Evan P. Singer
Dallas
+1.214.969.5021
epsinger@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Paloma Valor
Madrid
+34.91.520.3903
pvalor@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

Alexander J. Wilson
New York
+1.212.326.8390
alexanderwilson@jonesday.com

ADDITIONAL CONTACTS

Artur L. Badra
São Paulo/Madrid
+55.11.3018.3920/+34.91.520.3939
abadra@jonesday.com

Adam R. Brown
London
+44.20.7039.5292
abrown@jonesday.com

Yvonne W. Chan
Boston
+1.617.449.6914
ychan@jonesday.com

Terri L. Chase
Miami/New York
+1.305.714.9722/+1.212.326.8386
tlchase@jonesday.com

Toni-Ann Citera
New York
+1.212.326.3454
tcitera@jonesday.com

Kevin M. Comeau
Washington
+1.202.879.3909
kmcomeau@jonesday.com

Roman E. Darmer
Irvine
+1.949.553.7581
rdarmer@jonesday.com

Richard H. Deane Jr.
Atlanta
+1.404.581.8502
rhdeane@jonesday.com

John Emmerig
Sydney
+61.2.8272.0506
jemmerig@jonesday.com

Steven W. Fleming
Sydney
+61.2.8272.0538
sfleming@jonesday.com

Anders Folk
Minneapolis
+1.612.217.8923
afolk@jonesday.com

Shirlethia V. Franklin
Washington
+1.202.879.3892
sfranklin@jonesday.com

Louis P. Gabel
Detroit
+1.313.230.7955
lpgabel@jonesday.com

Rasha Gerges Shields
Los Angeles
+1.213.243.2719
rgergesshields@jonesday.com

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Kevin B. Hart
Washington
+1.202.879.5403
khart@jonesday.com

Jill Keller Hengen
Atlanta
+1.404.581.8956
jkellerhengen@jonesday.com

Brian Hershman
Los Angeles
+1.213.243.2445
bhershman@jonesday.com

Adam Hollingsworth
Cleveland
+1.216.586.7235
ahollingsworth@jonesday.com

James T. Kitchen
Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

Tim L'Estrange
Melbourne/Sydney
+61.3.9101.6820/+61.2.8272.0561
tlestrange@jonesday.com

Guillermo E. Larrea
Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Andrew E. Lelling
Boston
+1.617.449.6856
alelling@jonesday.com

James P. Loonam
New York
+1.212.326.3808
jloonam@jonesday.com

Heather Martin
Dubai
+971.4.709.8484
hmartin@jonesday.com

Rebecca C. Martin
New York
+1.212.326.3410
rcmartin@jonesday.com

Kendra L. Marvel
Los Angeles
+1.213.243.2366
kmarvel@jonesday.com

Jordan M. Matthews
Chicago
+1.312.269.4169
jmatthews@jonesday.com

Shireen Matthews
San Diego
+1.858.314.1184
shireenmatthews@jonesday.com

Yvette McGee Brown
Columbus/Cleveland
+1.614.281.3867/+1.216.586.7055
ymcgeebrown@jonesday.com

Joan E. McKown
Washington
+1.202.879.3647
jemckown@jonesday.com

Daniel Moloney
Melbourne
+61.3.9101.6828
dmoloney@jonesday.com

David E. Nahmias
Atlanta/Washington
+1.404.581.8241/+1.202.879.3493
dnahmias@jonesday.com

Cheryl L. O'Connor
Irvine
+1.949.553.7505
coconnor@jonesday.com

Fernando F. Pastore
São Paulo
+55.11.3018.3941
fpastore@jonesday.com

Cristina Pérez Soto
Miami / New York
+1.305.714.9733 / +1.212.326.3939
cperezsoto@jonesday.com

Glyn S. Powell
London
+44.20.7039.5212
gpowell@jonesday.com

Mary Ellen Powers
Washington
+1.202.879.3870
mepowers@jonesday.com

Thomas Preute
Düsseldorf
+49.211.5406.5569
tpreute@jonesday.com

Jeff Rabkin
San Francisco / Silicon Valley
+1.415.875.5850 / +1.650.739.3954
jrabkin@jonesday.com

Ansgar C. Rempp
Düsseldorf / Frankfurt / Munich
+49.211.5406.5500 / +49.69.9726.3939 /
+49.89.20.60.42.200
arempp@jonesday.com

Sion Richards
London
+44.20.7039.5139
srichards@jonesday.com

Yaakov M. Roth
Washington
+1.202.879.7658
yroth@jonesday.com

Holly Sara
Sydney
+61.2.8272.0549
hsara@jonesday.com

Jeffrey B. Schenk
Silicon Valley
+1.650.687.4130
jbschenk@jonesday.com

Sheila L. Shadmand
Dubai
+971.4.709.8408
slshadmand@jonesday.com

Ronald W. Sharpe
Washington
+1.202.879.3618
rsharpe@jonesday.com

Zachary Sharpe
Singapore
+65.6233.5506
zsharpe@jonesday.com

Erin Sindberg Porter
Minneapolis
+1.612.217.8926
esindbergporter@jonesday.com

Stephen G. Sozio
Cleveland
+1.216.586.7201
sgsozio@jonesday.com

Edward Patrick Swan Jr.
San Diego
+1.858.703.3132
pswan@jonesday.com

John C. Tang
San Francisco
+1.415.875.5892
jctang@jonesday.com

Rick van 't Hullenaar
Amsterdam
+31.20.305.4223
rvanthullenaar@jonesday.com

Jason S. Varnado
Houston
+1.832.239.3694
jvarnado@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Simon M. Yu
Taipei
+886.2.7712.3230
siyu@jonesday.com

Kristin K. Zinsmaster
Minneapolis
+1.612.217.8861
kzinsmaster@jonesday.com

Associates Jacqueline A. DeJournett, Evelyn Ni, and Darya Vakulenko contributed to this White Paper.

APPENDIX—Implementing DOJ Electronic Communication Guidance: Key Takeaways

The DOJ Guidance

- In evaluating a corporate compliance program, DOJ Criminal Division prosecutors are directed to assess the company's policies and procedures addressing the use of personal devices, communications platforms, and messaging applications (including ephemeral messaging applications) by company personnel.
- According to DOJ's guidance, these policies and procedures should:
  - "Be tailored to the corporation's risk profile and specific business needs"; and
  - "Ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company."
- Prosecutors are instructed to consider a number of factors in their evaluation of the compliance program, including:
  - Mechanisms for managing and preserving information within the company's communication channels;
  - Application and enforcement of the company's data retention and business conduct policies regarding personal devices and messaging apps;
  - Policies regarding company review of data on personal devices and messaging apps and whether the company has exercised its rights to review such data; and
  - Consequences for employees who refuse to allow the company access to business communications and whether the company has implemented those consequences.

The Practical Effect

- Unlike the rules governing preservation of communications that apply to financial institutions, DOJ's guidance relating to personal devices and messaging apps does not have the force of law; the guidance does, however, indicate how prosecutors will determine whether this aspect of a company's compliance program is effective.
- DOJ is not recommending that companies prohibit employees from using personal devices or messaging apps altogether.
- Further, DOJ recognizes that there is no one-size-fits-all approach to personal devices and messaging apps that will be effective or advisable for every company—the appropriateness of a company's approach should be tied to its own assessment of its business needs and associated risks.

Assessing the Need for Change to Corporate Policies and Procedures

- Initial steps:
  - Identify and consider all existing relevant policies, procedures, and user agreements;
  - Understand the realities of how employees are communicating regarding company business and current methods of preservation; and
  - Analyze potential legal implications in all jurisdictions in which the company operates (e.g., applicable data privacy laws).
- Determine whether existing corporate policies:
  - Clearly address the need to preserve business-related data regardless of its location (including on personal devices) in accordance with applicable retention policies;
  - Provide direction on whether and how employees may appropriately engage in business-related communications via third-party messaging apps, such as WhatsApp, WeChat, and third-party ephemeral apps, such as Signal;
  - Address the company's ability to access, collect, and review business data regardless of its location (consistent with any applicable data privacy or data security laws), including on personal devices; and
  - Are inconsistent with one another or leave gaps that could lead to confusion among employees about the use of/access to personal devices and business data contained within personal devices or third-party messaging apps.

Preparation for Future Data Collections

- Consider obtaining advance consent from employees (in jurisdictions where it is legally permissible) permitting access to, and collection of, all company data, regardless of where it is located; and
- Ensure employees are aware of the company's policies addressing electronic communications; consider requiring employees to sign periodic attestations confirming compliance; and be prepared to institute discipline for noncompliance.

ENDNOTES

1 Jones Day, *DOJ Updates Corporate Compliance Program Guidance and Announces New Policy Initiatives and Enforcement Resources* (March 2023); U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (March 2023).

2 U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, 17 (March 2023).

3 *Id.*

4 U.S. Dep't of Justice, United States Attorneys' Manual § 9-47.120(3)(c) (2017).

5 U.S. Dep't of Justice, Justice Manual § 9-47.120(3)(c) (March 2019).

6 Lisa Monaco, U.S. Dep't of Justice, Memorandum, 11 (Sept. 15, 2022) [hereinafter "Monaco Memorandum"].

7 *See* Monaco Memorandum at 11; Marshall Miller, Principal Associate Deputy Attorney General, U.S. Dep't of Justice, *Keynote Address at Global Investigations Review* (Sept. 20, 2022).

8 U.S. Dep't of Justice, *Evaluation of Corporate Compliance Programs*, *supra* note 2.

9 *Id.*

10 *Id.* at 1.

11 *Id.* at 17.

12 *Id.* at 17-18.

13 Kenneth A. Polite, Assistant Attorney General, U.S. Dep't of Justice, *Keynote Address at the ABA's 38th Annual National Institute on White Collar Crime* (Mar. 3, 2023).

14 *Id.*

15 U.S. Dep't of Justice, Justice Manual § 9-47.120(3)(c) (Nov. 2019).

16 Gaspard Le Dem, *DOJ Fraud Chief Says Compliance Isn't "One Size Fits All"*, Global Investigations Review (May 19, 2023).

17 *See* U.S. Securities and Exchange Act of 1934, 17 C.F.R. § 240.17a-4 (2023); Financial Industry Regulatory Authority, *SEA Rule 17a-4 and Related Interpretations* (Feb. 23, 2023) (requiring a broker-dealer to maintain and preserve electronic records exclusively in a non-rewritable, non-erasable format); Financial Industry Regulatory Authority, *Disciplinary and Other FINRA Actions*, 3 (August 2022).

18 U.S. Securities and Exchange Commission, *SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures* (Sept. 27, 2022); Commodity Futures Trading Commission, *Statement of Commissioner Kristin N. Johnson Regarding CFTC Orders for $700 Million Penalty Against Bank-Affiliated Entities for Offline Communications* (Sept. 27, 2022).

19 *See* U.S. Securities and Exchange Commission, *SEC Charges 10 Firms with Widespread Recordkeeping Failures* (Sept. 29, 2023); *SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures* (Aug. 8, 2023); Commodity Futures Trading Commission, *CFTC Orders Four Financial Institutions to Pay Total of $260 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods* (Aug. 8, 2023).

20 *See* U.S. Securities and Exchange Commission, *supra* note 18; U.S. Securities and Exchange Commission, *supra* note 17.

21 U.S. Securities and Exchange Commission, 2023 Examination Priorities. Division of Examinations at 17.

22 Anna Bianca Roach, *SEC to prioritise ephemeral messaging and ESG misstatements, enforcement director says*, GLOBAL INVESTIGATIONS REVIEW (Sept. 22, 2023).

23 *See* Commodity Futures Trading Commission, *supra* note 18.

24 Some companies admitted only some of the facts set forth in an enforcement order, neither admitting nor denying other allegations. For example, one company did not admit that their employee deleted business-related communications and requested a third party to do the same and the second company did not admit that its traders impeded the CFTC's investigation. *See In re Bank of America*, CFTC No. 22-38 (Sept. 27, 2022); *In re Nomura Global Financial Products Inc, et al.*, CFTC No. 22-41, (Sept. 27, 2022).

25 *See, e.g.,* Barclays Capital Inc., Securities Exchange Act Release No. 95919, ¶27-28 (Sept. 27, 2022); see also BNP Paribas Securities Corp., Securities Exchange Act Release No. 98079, ¶26-27 (Aug. 8, 2023).

26 *See, e.g.,* BNP Paribas Securities Corp., Securities Exchange Act Release No. 98079, ¶28 (Aug. 8, 2023).

27 *See* H.C. Wainwright & Co., LLC, FINRA Case No. 2017055977301 (Sept. 23, 2022).

28 Financial Industry Regulatory Authority, *2023 Report on FINRA's Examination and Risk Monitoring Program* (Jan. 2023).

29 Gurbir S. Grewal, Director, Division of Enforcement, U.S. Securities and Exchange Commission, *Remarks at SEC Speaks 2021* (Oct. 13, 2021) ("[I]f we learn that, while litigation is anticipated or pending, corporations or individuals have not followed the rules and maintained required communications, have ignored subpoenas or litigation hold notices, or have deliberately used the sort of ephemeral technology that allows messages to disappear, we may well conclude that spoliation of evidence has occurred and ask the court for adverse inferences or other appropriate relief. These rules are not just 'check the box' exercises for compliance departments . . . .").

30 *See, e.g.*, *United States v. Google LLC*, No. 1:20-cv-03010, Mem. at 4 (D.D.C. Feb. 23, 2023) (seeking sanctions related to chats that were allegedly auto-deleted and arguing that the company's employees "held substantive and sensitive business discussions over chat, even when (or because) the history was set to 'off'"). While serving as another example of DOJ's continued focus on electronic messages as a source of evidence, note that the sanctions dispute in this antitrust matter relates to preservation *after* DOJ alleges that the company should have reasonably anticipated litigation, rather than proactive preservation prior to anticipation of litigation or a regulatory inquiry. *Id.* at 2-3.

31 *See supra* note 12.

32 Personal Information Protection Law ("PIPL") of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2010), arts. 13-14, 2021 (China).

33 Separate consent must be obtained if the purpose, manner, and category of information of the processing changes. *See id.*, Article 14.

34 The PIPL provides that consent is not required for the processing of personal information: (i) where the processing is necessary for the conclusion or performance of a contract to which the individual is a contracting party or to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts; and (ii) where the processing is necessary to fulfill statutory duties and responsibilities or statutory obligations. *Id.*, Article 14.

35 For a personal information processor to transfer personal information outside the territory of PRC, it must (i) pass a security assessment organized by the state administration; (ii) receive a personal protection certification conducted by a specialized organization; (iii) enter into a standard contract with the foreign receiving party; or (iv) comply with other laws and regulations. *Id.*, Article 38. Notice must be given to the individual and separate consent must be obtained for processor to transfer personal information outside of PRC. *Id.*, Article 39. The Data Security Laws of the PRC ("DSL") and PIPL both require pre-approval by a Chinese competent authority when companies intend to transfer any data stored in China to a foreign judicial or law enforcement authority. DSL, Article 36; PIPL, Article 41.

36 Public security administration penalties and criminal liability may be imposed for a violation of the PIPL. PIPL, Article 71. Criminal liability may be imposed for violation of the DSL when national core data management rules have been abridged and the violation endangers the national sovereignty, security, or development interests of the state. DSL, Article 45.

37 In addition to assessing its ability to access all business-related data on a BYOD device, companies deploying a BYOD program should also consider how best to address a number of data security considerations, including access controls, network security, and data encryption, and should also be prepared with a robust incident response plan to handle data breaches or security incidents involving BYOD devices.

38 *Supra* note 2 at 17 ("Policies governing [ephemeral messaging] applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company.").

39 Gaspard Le Dem, *DOJ Fraud Chief Says Compliance Isn't "One Size Fits All,"* GLOBAL INVESTIGATIONS REVIEW (May 19, 2023) ("Asked whether the DOJ thinks employees should be allowed to communicate using ephemeral messaging platforms like WhatsApp, [Glenn] Leon demurred. 'We're not telling companies they can't use WhatsApp,' he said. Leon said companies that operate in countries where WhatsApp is ubiquitous may decide against banning the platform, but should be able to demonstrate they have put careful thought into ephemeral messaging policies.").

40 *Id.*

41 *See* Monaco Memorandum, 11.

42 U.S. Dep't of Justice, Justice Manual § 9-47.120 FCPA Corporate Enforcement Policy (Nov. 2019).

43 Gaspard Le Dem, *DOJ Fraud Chief Says Compliance Isn't "One Size Fits All,"* GLOBAL INVESTIGATIONS REVIEW (May 19, 2023).

44 *Id.*