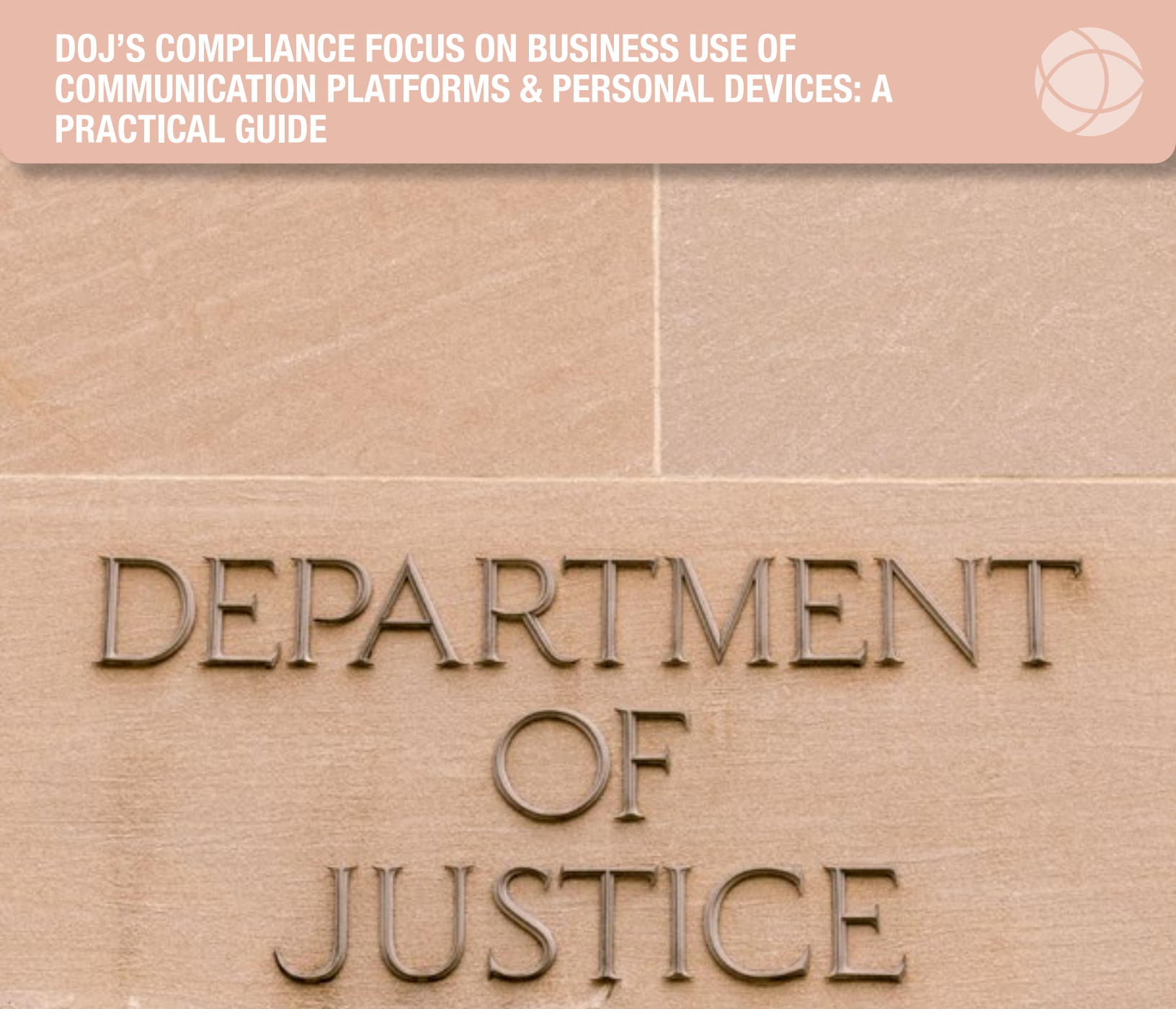
DOJ'S COMPLIANCE FOCUS ON BUSINESS USE OF COMMUNICATION PLATFORMS & PERSONAL DEVICES: A PRACTICAL GUIDE



BY JAMES W. ATTRIDGE, BROOKE J. OPPENHEIMER & HEATHER C. ZUCKERT[1]



1 Attridge is a partner at Axinn, Veltrop & Harkrider LLP, where Oppenheimer is Counsel, eDiscovery, Cyber & Data Protection and Zuckert is an associate.

CPI ANTITRUST CHRONICLE
September 2023

Visit www.competitionpolicyinternational.com for access to these articles and more!

DOJ'S COMPLIANCE FOCUS ON BUSINESS USE OF COMMUNICATION PLATFORMS & PERSONAL DEVICES: A PRACTICAL GUIDE

By James W. Attridge, Brooke J. Oppenheimer & Heather C. Zuckert

The Department of Justice and the Antitrust Division have been increasingly focused on combatting corporate crime by prosecuting individual wrongdoers. To further that goal, the Department redoubled its commitment to incentivizing corporate compliance and raised its expectations of cooperating companies. Among the factors prosecutors consider when evaluating corporate compliance and cooperation are the company's document and data retention policies. In a series of speeches and policy changes culminating in March 2023 updates to the Justice Manual and the Criminal Division's Corporate Compliance Guidance, the Department outlined its expectation that companies have effective policies and procedures governing the use of personal devices and communication platforms – and provide training on and enforce those policies – so that business-related electronic data and communications are preserved. In practice, companies looking to regulate and preserve employee communications face increasing challenges in light of the predominance of "bring your own device" ("BYOD") programs and wide-ranging messaging and communications channels. This article outlines the Department's and the Division's compliance and preservation guidance and practical steps companies can take to ensure they are implementing best practices around: (i) how and what to collect in BYOD programs; (ii) collection and use policies; and (iii) how to enforce those policies.

The Department of Justice ("DOJ"), including the Antitrust Division, recently amplified its focus on corporate compliance programs in a series of speeches and policy changes, culminating in updates to the Justice Manual and Criminal Division's Compliance Guidance issued in March of this year. The Department outlined its expectation that companies have effective policies and procedures to govern the use of personal devices and communication platforms – and provide training on and enforce those policies – so that business-related electronic data and communications are preserved.

In practice, companies looking to regulate and preserve employee communications face increasing challenges in light of the predominance of "bring your own device" ("BYOD") programs and wide-ranging messaging and communications channels. Below we outline the Department's and the Division's compliance and preservation guidance and practical steps companies can take to ensure they are implementing the best practices around:

- How and what to collect in BYOD programs;
- Documenting collection and use policies; and
- The need for enforcement mechanisms

I. BACKGROUND ON DOJ'S GUIDANCE

For the Antitrust Division, whose criminal cases primarily involve allegations of collusion, the focus on business communications – particularly among competitors – isn't new. As the Antitrust Division's 2019 Compliance Guidance asked: "as employees use new methods of electronic communication, what is the company doing to evaluate and manage antitrust risk associated with these new forms of communication?"[2] Core to any cartel investigation – and resulting prosecution – for an agreement to limit competition are communications between competitors that evidence that agreement, implement it, or even take issue when it isn't abided by.

Like the rest of the DOJ, the Antitrust Division applies the Justice Manual's Principles of Federal Prosecution and Principles of Federal Prosecution of Business Organizations when enforcing the antitrust laws in the criminal context. The Manual lists eleven factors to consider in determining whether to charge a corporation, including "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one."[3]

In March 2023, the Department updated the Justice Manual's assessment of corporate compliance programs to include consideration of policies and procedures governing the business use of personal devices and communications platforms, "to ensure that business-related electronic data and communications are preserved."[4] At the same time, the DOJ's Criminal Division released updated guidance that further expands upon its expectations for corporate compliance and preservation efforts under the updated Justice Manual.[5] In evaluating corporate compliance efforts, the Criminal Division notes that "prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications."[6] In particular, it focuses on three considerations:

- Communication channels – What channels do the companies and employees use, and what mechanisms are in place regarding how information is preserved;
- Policy environment – What data retention policies are in place and how are they enforced, in particular with respect to "BYOD" programs; and
- Risk management – What are the consequences for failing to comply with company policies, in particular with respect to internal investigations.

Although the Antitrust Division has not updated its own compliance guidance following the March 2023 updates to the Justice Manual and the

2 U.S. Department of Justice, Antitrust Division, E*valuation of Corporate Compliance Programs in Criminal Antitrust Investigations* (July 2019), https://www.justice.gov/atr/page/file/1182001/download.

3 U.S. Department of Justice, "9.28.300 - Factors to Be Considered," *Justice Manual*, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations (emphasis added).

4 U.S. Department of Justice, "9.28.800 - Corporate Compliance Programs, *Justice Manual*, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.800.

5 U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

6 *Id.*

Criminal Division's compliance guidance, we expect its compliance assessment will continue to take cues from and track the Criminal Division's. Indeed, in a keynote last year, then Deputy Assistant Attorney General of the DOJ Antitrust Division Richard A. Powers remarked on the future of effective antitrust enforcement and the need for companies to be proactive in their compliance programs.[7] He similarly alluded to BYOD programs and emphasized "[c]ompanies should consider whether permitting their employees to use personal devices with encrypted apps to conduct business is consistent with a culture of compliance."[8] And as Powers noted, encrypted and ephemeral messaging applications have featured in a number of recent Division investigations and prosecutions.[9]

Accordingly, the Division has tasked companies with creating corporate compliance programs that "account for and undertake measures to prevent collusion in a way that reflects the realities of how their businesses operate"[10] – in other words, companies should evaluate what types of devices, platforms, and applications are actually used within the company and adjust their compliance and preservation policies accordingly.

II. WHAT HAPPENS IF A COMPANY DOES NOT DO THIS?

The Division takes into account the "adequacy and effectiveness" of a corporation's compliance program when assessing whether to charge a corporation and in both the form and terms of a corporate criminal resolution. As outlined above, the Division considers "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision," and part of that assessment is "whether the corporation has implemented effective policies and procedures governing the use of personal devices and communication platforms, including third-party applications, to ensure that business-related electronic data and communications are preserved."[11] And as emphasized in the Criminal Division's recent guidance, this includes a particular focus on "messaging applications, including ephemeral messaging applications."[12]

Failure to implement appropriate policies to preserve data will therefore be detrimental to not only the perceived effectiveness of a company's compliance program, but also to the company's ability to get credit for cooperation in the Division's investigation, which includes timely "preservation, collection, and disclosure of relevant documents and information" and an assessment of whether the company "enforced effective document and data retention policies," "including as to third-party messaging data."[13] It could also undermine a company's own ability to detect potentially problematic communications via internal investigation. Such a review is critical in the leniency context, where the Division requires companies to self-report violations promptly upon discovery and to improve its compliance program to mitigate the risk of engaging in future illegal activity.[14]

III. IMPLEMENTATION CONSIDERATIONS

In light of the Department's and the Division's increased focus on the use of personal devices and communication platforms, companies should consider evaluating – and if needed, updating – their current policies relating to preservation of business-related communications. Companies often are experienced in monitoring, preserving, and deleting communications through company-provided devices, such as laptops or phones, and achieve this through established IT policies and litigation holds. Moreover, companies have insight into, if not control over, the types of applications that employees can use on company-provided devices.

7 Deputy Assistant Attorney General Richard A. Powers, Keynote at the University of Southern California Global Competition Thought Leadership Conference: Effective Antitrust Enforcement: The Future Is Now (June 3, 2022), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-powers-delivers-keynote-university-southern.

8 *Id.*

9 *Id.*

10 *Id.*

11 U.S. Department of Justice, "9.28.800 - Corporate Compliance Programs," *Justice Manual*, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

12 U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

13 Id. at 9.28.700 - The Value of Cooperation, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.700.

14 See e.g. U.S. Department of Justice, Antitrust Division, *Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations* (July 2019), https://www.justice.gov/atr/page/file/1182001/download ('[E]arly detection and self-policing are hallmarks of an effective compliance program and frequently will enable a company to be the first applicant for leniency under the Division's Corporate Leniency Policy.").

This is changing with the increasing popularity of BYOD programs among companies and employees, which can reduce costs to the company and increase productivity.[15] In 2022, estimates indicate that more than 87 percent of companies rely on their employees' use of their personal devices for work in some capacity, with more than 50 percent of companies requiring such use.[16]

BYOD programs traditionally apply to mobile devices (e.g. phones and tablets) and laptops. While companies have realized the security risks associated with using personal devices for work and implemented technology to protect business data on mobile devices, this technology does not solve two problems that the Division is focused on: *monitoring* and *preservation*. Most mobile device management solutions today are geared instead toward protection and deletion – for instance, they allow companies to remotely delete information from employees' personal devices that are used for work, such as wiping email from their phones after they have left the company. But these solutions are not designed to preserve their communications for purposes of a litigation hold or collection. Nor do they monitor other means of communications on the employees' devices, such as social networks (e.g. Facebook, LinkedIn) or group chatting platforms.

As outlined above, the Antitrust Division expects robust compliance programs whose preservation efforts take into account all communication channels employees are using. Accordingly, companies should consider additional methods of preserving information and a proactive approach to ensure that employees are following corporate policies on all their devices when engaging in business-related communications.

A. How to Collect: The Forensic Collection Process

Generally, when collecting material from devices, a company can either do a (i) full forensic image of the device or (ii) targeted collection of device data. Because BYOD programs create a mix of personal and business information on employees' devices, some companies may prefer a targeted collection in order to avoid employees' personal data. A full forensic image, on the other hand, captures both business and personal information, which could include photographs of children, text messages with family members, downloaded videos, etc. As might be expected, employees are often not pleased that companies are capturing this unrelated information in the course of an investigation. However, the Division will often expect companies to capture a full forensic image of a device in order to capture any potentially relevant text messages, GPS coordinates, phone calls, system logs, photos, videos, and other information contained on the device, whereas selective collection may only capture specific items that a producing party deems relevant at a given point in time. This can prompt questions from regulators about what information was actually searched, considered, and produced.

That said, doing a full forensic image can provide benefits to companies as well, including:

(1) Sufficient Metadata/ Defensibility: The current forensic tools available for selective collection (e.g. collection of certain messages) may not be considered forensically sound. Taking a full forensic image of the device means that the company, and agency or opposing party if in a litigation, have access to an exact copy of the physical device. This includes capturing deleted space, files, or other deleted or encrypted data. In high stakes matters, such as criminal investigations, this can prove an important means to disprove the Division's theories, particularly related to alleged communications with competitors or collusive activity. Selective collection, on the other hand, only captures a tailored set of files or folders considered relevant and so could be perceived to provide an incomplete picture.

(2) Selective Collection is Burdensome: It is often difficult to clearly delineate between communications and other data that is business-related and that which is personal. And even when companies or employees can separate the two, such distinctions are often not easily identifiable without looking at the underlying data – for instance, each text message exchange or system coordinates – which can make the collection process extremely time-consuming and expensive. Though there is a larger up-front cost in generating a full forensic image, the downstream costs and time commitments often significantly outweigh the initial expense.

(3) Changing Needs: When engaging in selective collection, a company, in connection with counsel, identifies what information is relevant to a given subpoena, discovery request, or internal investigation, and copies that information from the device. However, certain messages or other data might not be needed at the start of an investigation but could become critical as the investigation proceeds. For example, messages might be the primary focus today, but in five years, whether an individual can be tracked to a certain location via GPS coordinates might be the priority. At that stage, such information would likely no longer be on the device and be nearly impossible to recover. Accordingly, while full forensic image collections may be overbroad initially, they prevent companies from needing to go back to a collection

15 See e.g. Powers, John, 7 key benefits of enacting a BYOD policy, *TechTarget (May 30, 2023)* https://www.techtarget.com/searchmobilecomputing/feature/Key-benefits-of-enacting-a-BYOD-policy.

16 Shields, Corey, *Bring Your Own Device (BYOD) Policy Tips and Best Practices for 2022*, Ntiva (May 12, 2022), https://www.ntiva.com/blog/bring-your-own-device-byod-policy.

source down the road if additional data is needed or if it was not in the original targeted collection, and they ensure such information is not lost or deleted in the meantime.

In addition to a full collection of a mobile device, the recent guidance suggests the Division may expect collections include third-party applications that might contain potentially relevant communications, such as:

(1) Social Media Accounts: Collection of social media accounts requires the sharing of the account owner's username and password. Even if using temporary credentials, employees are often not comfortable providing access to forensic technicians who will have complete control and access to their account, and the capture is likely to include a composite of personal information. But, depending on the nature of the investigation, social media might be a prime source of relevant information.

(2) Chat Rooms: Similar to the collection of social media, personal chat rooms have the added complexity of capturing personal communications of group members that are potentially outside the scope of the investigation. However, chat rooms have come up in several cartel cases in recent years and are likely to continue to be a focus for antitrust investigators.[17]

B. How to Document: Scope & Use Policies

To meet DOJ's evolving expectations, companies should consider policies that provide the ability to access, monitor, preserve, and collect relevant information transmitted on personal devices and through personal accounts, regardless of the intermingling of personal information. This requires strong, clear policies covering the following areas: (1) scope and access, (2) permissible use of data and systems for business related material, (3) technical protocols for encryption, and (4) departing employees.

(1) Scope and Access. Companies should consider ensuring that in their policies, they are allowed to undertake the type of complete forensic collection described above, including for any personal devices used for business purposes. Owners of devices that contain both personal and business information are typically very sensitive to the comprehensive collection of a device, and for obvious reasons as the collection could capture personal photos and communications, app use, and even account credentials. Unfortunately, most collection methodologies today used for full forensic imaging cannot themselves selectively exclude certain devices – the filtering and narrowing is conducted post collection. Therefore, companies should consider clear policies that make BYOD users understand that the use of the device for work might not limit the collection to only such work materials.

(2) Permissible Use Policies. Policies also should clearly state what an employee can do with business information and what specific systems an employee can use for handling company information. For instance, if a company does not have a BYOD program, but rather has and enforces a strict policy that any information related to the company cannot be created, shared, communicated, or stored on non-company devices, it will be more difficult for the DOJ to justify or obtain access to personal devices/accounts through the client. If, on the other hand, a company fails to implement such policies or permits employees to use their personal devices for business purposes, the company will have a harder time resisting such requests for access. The company will instead need to balance the requirements of the DOJ to obtain that data (or be liable for the consequences) or balance the issues with collecting their employees' personal devices and accounts.

(3) Technical Protocols. Companies should also consider establishing and documenting technical processes to permit the forensic collection of BYOD devices, including means of bypassing security protocols. Phones and laptops have various security protocols that limit unfettered access to their user's personal data. These protocols – such as iPhone passcodes – have made headlines when creating challenges for law enforcement agencies seeking to access certain data, and corporate entities can face the same issues when seeking to access necessary data during the collection process. For example, mobile devices with local backup encryption cannot be readily collected without (1) being provided the backup password by the device owner, or (2) without being reset to bypass the encryption. The local encryption password is often set on prior iterations of a users' device and is often not recalled by the end users. Therefore, companies permitting BYOD should establish protocols to manage encryption settings prior to permitting the device to be used for business purposes.

(4) Departing Employees. Companies with BYOD devices should also consider establishing protocols for preserving information on devices when an employee leaves the company. Unlike with company-provided devices, BYOD devices previously containing business-related communications leave with the employee. Will these devices be automatically imaged? Can devices be clawed back post-employment? How is

17 For example, the Antitrust Division charged five companies and six individuals in its investigation of collusion in the FX spot market and noted the currency traders had "engaged in near-daily communications with [their] co-conspirators by phone, text and through an exclusive electronic chat room to coordinate their trades." Dep't of Justice Press Release, "Former Trader for Major Multinational Bank Convicted for Price Fixing and Bid Rigging in FX Market," (Nov. 20, 2019), https://www.justice.gov/opa/pr/former-trader-major-multinational-bank-convicted-price-fixing-and-bid-rigging-fx-market.

the data being stored offline? Though there are many ways a company manages the data on BYOD devices, a clear and defined plan should be established.

Having these various collection and use policies well documented is an important first step. In the context of an investigation or eventual litigation, companies may need to explain what data they have – or have not – been able to produce in response to the Division's requests. It is therefore helpful to have documented, consistent, and followed processes so that this information is readily available. Ad hoc processes can be difficult for companies to reconstruct, particularly years after the fact, and so can risk complications with admissibility or defensibility in trial. Standard, well-documented policies, on the other hand, can typically be spoken to by one witness who oversees the implementation of those standardized collection processes.

C. How to Enforce

Finally, the Division also expects companies to monitor and enforce their scope and use policies. As previewed by the Deputy Attorney General in her September 2022 memorandum, it's not enough to have clear policies governing the use of personal devices and third-party messaging platforms, employees should be trained on those policies, and companies should "enforce those policies when violations are identified."[18] Likewise, enforcement is a primary focus of the Criminal Division's updated guidance from March 2023. With respect to communications platforms, messaging applications, and personal devices specifically, it calls prosecutors to consider:[19]

- How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications?
- 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, it is being followed in practice, and how is it enforced?
- What are the consequences for employees who refuse the company access to company communications?
- Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications?

Given the existence of disciplinary measures – and the frequency disciplinary measures are employed – will likely be another factor that the Division considers when assessing compliance and preservation programs, companies should carefully monitor any policies that they put in place around where and how employees can engage in business communications, for instance what an employee can do on business vs. personal devices and what specific systems or applications can be used. If employees violate such policies, the Division expects companies to (i) track this data and (ii) when appropriate, take disciplinary action. This will allow companies down the road to be better prepared to respond to investigation requests and meet the Division's cooperation and compliance expectations.

IV. KEY TAKEAWAYS

1. Preservation policies around business-related communications, including those done on personal devices, will play a role in the Antitrust Division's evaluation of corporate compliance programs;
2. As part of good compliance practices, companies should consider erring on the side of full collection of devices, even companies with BYOD programs;
3. Companies should ensure that they have the policies in place to (i) allow them to do such collections even if personal information may be implicated and (ii) enforce their policies related to business-related communications.

18 Deputy Att'y Gen., Lisa O. Monaco, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group"), Further Revisions to Corporate Criminal Enforcement Policies, September 15, 2022 (justice.gov).

19 U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.