Deloitte.

5 insights into mobile messaging and chat surveillance

Focus on Five

5 insights into mobile messaging and chat surveillance

Easy-to-use and widely adopted messaging apps are a popular way for billions of people to stay in touch and share information with family, friends, colleagues, clients, vendors, and other people or organizations with whom they have relationships. The ubiquity and ease of the messaging applications used in personal interactions have quickly entered the business mainstream. Appealing as they may be, messaging and chat apps can create issues when used for business communications, including headaches for compliance and legal functions. Organizations that face or anticipate the use of these tools within their ranks can benefit from five insights into why they are popular, and potentially problematic.

#1—Mobile data is increasingly important in both litigation and regulatory matters

Companies in certain industries operate under regulatory requirements to archive, monitor, and surveil employee and customer communications. US Financial Industry Regulatory Authority (FINRA) rules dictate the handling of electronic communications involving securities broker-dealers and commodity traders. The Health Insurance Portability and Accountability Act (HIPAA) includes procedures to safeguard patient information and the types of messages that can be sent between providers and patients. These regulations challenge the client's or patient's desire to communicate with their providers with the same messaging platforms they use day to day for general purposes.

Organizations in industries without explicit message monitoring and surveillance regulations also have good reason to look at messaging implications. Two examples include a technology company that could face an antitrust issue and a business that wants to investigate allegations of employee misconduct.

In these circumstances, mobile messaging data could play a substantially larger role than just a few years ago, subjecting an organization to keen attention from regulators and the courts. Reasons for using messaging and chat in lieu of enterprise communications channels can range from the more-or-less innocent to the nefarious. An employee may opt to use an app simply for convenience. Or, the person could do so to circumvent organizational monitoring and surveillance of enterprise email, messaging, and other channels. In either case, the business may have an obligation and need to produce the mobile messages to comply with current regulations or a court order.

#2—Employees are using chat apps more often to perform their work

Ask information technology (IT) leaders whether messaging and chat are being used, and they may say in a confident tone that such apps are not part of the enterprise technology picture. Pose the same question to employees, though, and the response could be more . . . nuanced. Unless already controlled by policy or technological control, it is likely many organizations have some form of mobile messaging "shadow IT" used by some employees used in situations such as: "My UK client prefers to communicate on this app." Or, "We were on a tight deadline, so we used that app to collaborate."

Organizational concerns about the use of messaging and chat apps are not necessarily motivated by fear of bad actors. Instead, leadership can simply feel unprepared because they are not aware of the apps that are restricted or those that are in use. The organization wants to give employees the leeway to use apps they know and enjoy, helping keep them happy and productive. At the same time, many apps are not designed with enterprise monitoring in mind, leaving leaders to find novel ways to meet the associated compliance, discovery, and investigative requirements.

#3—Popular apps are designed for ease of use, not compliance and litigation

The term is not intended as a slight, but many mobile messaging and chat apps may aptly be described as "consumer grade." They are typically not built for enterprise communications and employee collaboration. They often lack controls essential to meeting compliance requirements and critical features such as legal-hold and surveillance functionality.

Given these deficiencies, organizations are challenged to balance the potential gains in productivity and employee engagement against the risks of deploying this technology. A major consideration is how to keep up with the app developers as they continuously improve and evolve the applications. Many chat applications are vying for market share and adapt quickly to meet consumer wants and needs. This creates an environment where volatile applications with features that have no litigation or regulatory precedent can proliferate.

#4—A plan for third-party applications is essential to legal and regulatory readiness and it may include white/blacklisting

An insightful and researched list of apps to use and apps to avoid, along with clear policies and direction for usage, are essential tools for organizations operating in regulated industries to guide employees. Either contractual terms or technical restrictions can be used as a framework for development and maintenance of a list. If an organization wants to provide functionality to certain employees, establishment of use policies can clarify access and restrictions, particularly when technology constraints limit monitoring capabilities.

It can also be wise to consider how the "self-destructing" or "vanishing" capabilities built into some messaging apps could affect the organization from a risk and compliance standpoint. Starting with early chat apps nearly a decade ago, most leading messaging platforms now offer the capability to compose and send messages that disappear immediately after viewing or after a specified time.

It is likely that regulations require monitoring of self-destructing messages in the same manner as any other communication. This could include real-time archiving in order to prevent the disappearance of messages with regulatory or legal import. In some cases, organization may be tasked to look for and identify recovered messages that may exist on devices.

Retrieval of deleted chat messages requires analysis and actions beyond those typically available with commercial tools. Analysis can include determining what remnants are left behind in the database. In addition, comparing the percentage of deleted messages to active messages can provide insight into what has previously happened on a device or identify patterns of activity and usage. For example, are there spikes or anomalies in activity that might relate to a specific matter, time period, or inquiry?

#5—Surveillance and collection methods exist for some messaging apps, but capabilities can change with updates

Monitoring of app capabilities is essential to help prevent a situation where an app that is used today becomes a potential problem with the introduction of a new feature, such as video chat. Along with policy and white/blacklisting, third-party monitoring applications can add support to strengthen surveillance capabilities and activities.

There may still be reasons, though, to hold off on introducing a monitoring app. First, employees may well balk at the idea of having one more tool to deal with. Second, while apps are now available to monitor popular messaging apps, the providers may not have partnerships with the messaging app makers. Because of this, if the messaging application is altered in some way, the monitoring solution is likely to require an update, or it could stop working all together. It may be detrimental to client relationships to suddenly discontinue use of an application that clients or patients have become accustomed to using, because an app update broke the selected monitoring solution.

When facing the need to comply with regulations or litigation, organizations may need to look beyond the collectable message application data and consider various analyses to better understand an employee's usage. Metrics to consider include:

Chat message deletion. A red flag goes up if someone has been put on notice to retain messages and a review finds no messages on the person's phone or in logs. Such a situation could trigger a process to identify whether deletion activity occurred in a period that might be relevant to a specific issue. Steps can include examination of deletion percentages and identification of anomalies and patterns using analytics tools and concepts.

Chat message pattern and gap analysis. Analysis of a lack of messages vs. intact messages can help identify communication patterns, in conjunction with monthly and daily message frequency analysis. Customized charts based on relevant dates can be used to identify spikes and anomalies.

Mobile communication frequency analysis. Analysis of custodian activity can flag spikes in communications and the appearance of additional, previously unidentified custodians. Frequency analysis can reveal heightened communication between parties around a relevant date or the recent addition of someone new to a communication string.

Mobile data mapping. Mobile device analysis can help identify additional data repositories, accounts, and locations. For example, a certain type of web storage repository could be uncovered that provides additional information and leads.

Our take

The spread of messaging and chat apps creates an imperative for organizations to understand and create appropriate polices for use of these applications. And, while they open doors to new methods of communications, apps also can create risks. Mitigating those risks through effective management of messaging and chat activity is complicated by the speed at which applications can change.

For regulated companies especially, but also for any company that allows its employees to use these apps, exploring the art of the possible—identifying effective risk management avenues—can equip organizations to better address the proliferation of messaging and chat.

Contacts:

Mike Weil
Managing Director
Deloitte Financial Advisory Services LLP
+1 312 486 0207
miweil@deloitte.com

Deloitte.