Data Retention: Evolving Best Practices in a World of Data Proliferation

Daniel P. Levison, Partner at law firm Morrison & Foerster in Singapore, is an expert in compliance issues concerning electronic discovery, including data preservation, and is well positioned to discuss the latest concerns and best practices for parties involved in the wealth management sector. He addressed the audience at the Hubbis Compliance in Asian Wealth Management Forum to explain the most recent regulatory expectations and to demystify some of the increasingly complex rules of engagement.

Link to Content Summary page
Link to Article on website
Link to Presentation
Link to Event Homepage

LEVISON BEGAN BY EXPLAINING THAT HE the heads Morrison & Foerster's Singapore-based disputes and compliance practice for the region, "Although this is a topic that is vast in its scope, I am today focusing specifically on data retention obligations for compliance, and in particular concerning how expectations have been articulated by the US Department of Justice ("DOJ"). Although the DOJ has not prescribed

DANIEL LEVISON
Morrison & Foerster

specific actions, their statements give us a clear idea of not only the US regulators' views but also some insight into the likely perspectives of regulators across the globe as we all grapple with the proliferation of data."

Apps and 'traditional' modes of communication

He first zoomed in on the communication apps that so many people today use for their daily messaging and voice calls. With the explosion of new and different modes communication and data thus generated, he remarked that enforcement authorities are having difficulty in obtaining evidence in their investigations through traditional means like reviewing email because people are using so many ways to communicate.

Levison then focused on the US Foreign Corrupt Practices Act ("FCPA") and its enforcement, noting that the DOJ has provided guidance on what it considers timely and appropriate remediation in the context of its FCPA Corporate Enforcement Policy that was issued in November of 2017.

"The DOJ," he elaborated, "therefore makes it clear that it will consider full credit for timely and appropriate remediation dependent on appropriate retention of business records and prohibiting the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records for communications."

Business records – very broadly defined

Unfortunately, he explained that the guidance is limited as there is no uniform definition of what constitutes a business record. "However," he commented, "as a general guiding principle, business records are considered to include any hard copy or digital document generated in the regular course of business. The critical question is not where the document is stored or created, the cloud, apps, or on other software, but more properly the nature of the document."

He extended his line of thought by noting that although the DOJ does not explicitly prescribe how to store business records, companies often have document retention policies that provide for specific categories of documents to be stored for a reasonable amount of time after which they are automatically subject to destruction to comply with other regulatory regimes to which they may be subject.

"But where there is an investigation or litigation is anticipated you must make sure that business records are properly retained, for example, through the issuance of a notice to employees to prevent automatic deletion of certain documents."

Additionally, if such a notice is issued, a determination should be made whether there are sufficient automatic preservation capabilities in place, or whether additional ad hoc forensic imaging needs to be used to adequately preserve relevant data.

Case by case, but general rules show through

"Again, although the DOJ is not prescriptive about this, the determination of how data should be retained should be risk-based and depends on the facts and circumstances of a particular case and the company's IT environment," he elucidated.

"Accordingly, data for different employees may require additional preservation efforts, and as such, it depends on the employee's role in the exact matter that is being reviewed."

Together with the proliferation of applications, devices, working remotely, and shared workspace environments, as well as other factors, all mean that data retention obligations are increasingly complex and dynamic.

Levison then mined further down into issues surrounding apps such as 'Line', 'WhatsApp', and 'WeChat' and others. "The DOJ has specifically mentioned ephemeral modes of communication," he noted, "but there is no prescriptive policy or guidance on exactly how these apps and the data generated by them should be retained."

Challenges for the regulators & the providers

Levison commented that the enforcement agencies have seemingly been challenged in their ability to obtain and collect important evidence through gathering traditional media such as email, again because people are frequently communicating in real time using messaging apps and because a significant amount of that data is not stored centrally in a company's enterprise systems.

Levison advised that there are several ways to mitigate risk when dealing with mobile devices and with messaging apps. "For example," he said, "you could implement a policy that requires employees to use company-owned devices for company business, or one that explicitly gives the company rights to monitor any personal devices that are used for company business."

Additionally, companies can implement policies that require employees to back up their company-owned device to a company-controlled enterprise archive, for example, a company-controlled enterprise cloud account.

"Further," he advised, "it is possible to implement policies that prohibit employees from using messaging apps for business purposes. Although this does, of course, rely to a certain degree on an individual employee's compliance with the policy."

Policy and technology combine

Another approach is to implement policies that permit employees to use messaging apps for business purposes, but that also ensure that the data generated by this application is regularly backed up and retained in a company-controlled cloud, or that the apps are not used for substantive business communications. That said, companies should be wary that even seemingly non-substantive communications such as "I will meet you by the Starbucks down the street" could also be viewed in some circumstances as critical evidence.

He then advised the audience that there is a variety of techniques that those in the wealth management industry can consider in putting together an effective policy. "One size does not fit all," he remarked, "You need to make your own informed and appropriate assessment of the risk."

Assess your risks

Levison closed his talk with a brief introduction to best practices, and in particular implementing policies based on a robust risk assessment. "These are the key to satisfying the regulators," he explained,

"Regulators have stated explicitly that while they may not in hindsight agree with the decision that a company reaches, if that decision is based on an appropriate risk assessment, then it will be difficult for the enforcement agency to challenge it.

And remember that best practices will likely continue to include some combination of clear, consistent, and well-documented policy and technology based solutions."