Deloitte.

Business Collateral

Managing Emerging Data Types for Corporate Investigations, Litigation or Regulatory Matters

Within most organisations, typically the CIO, IT teams or specific business functions will make the decisions about the adoption of any new technology products. However, the introduction of tools such as messaging applications or collaboration and productivity solutions can often have wide reaching implications for legal counsel and compliance teams too. Specifically, how accessible is the data and logs produced from these systems if it is needed for future litigation, investigation, or regulatory matters?

Historically, finding relevant information has involved the collection of emails, office documents and occasionally corporate mobile devices. Today, that picture is a lot more complex, and the sources of relevant information is far broader given the rapid adoption of these social and collaboration apps.

Driven by the rise in hybrid working models, which has accelerated since COVID-19, platforms such as Teams, Zoom and Slack have recorded substantial growth in their user base. As organisations adapt to these new ways of working, centered on flexible working and online collaboration, the impact of this shift can already be anticipated across the legal and compliance landscape.

The Challenge

How do legal counsel and compliance officers ensure they can still respond to issues as they arise, all the while allowing their organisations to harness the full power of these tools? How can they have comfort that they know where their data is stored and it is accessible when needed? What processes need to be in place to enable the analysis of this data so potential events of interest can be identified? These are some of the questions which arise for corporate legal and compliance teams when considering common scenarios such as:

- Members of staff who allege to have been subjected to **aggressive and abusive behaviours** by their colleagues over **Teams chats or Zoom calls**
- An IP dispute which arises after suggestions that **sensitive information** pertaining to a new technology solution **was misappropriated** by an external third-party contractor who had access to the data through a shared project **Confluence page.**
- **Market sensitive information** regarding an M&A transaction having been shared on a **personal WhatsApp chat** and being made public prior to any official market announcement.

Below are five insights to consider and five actions which in-house counsel can action today to help in their preparations for their next investigation or litigation matter:

Insights to consider

1. **The accelerating growth in discoverable content can represent an opportunity as well as a challenge:** As the scope of discoverable content continues to increase, understanding how these tools and technologies are being adopted within the organisation plays a key first step in the discovery process. These new systems/tools can reveal valuable information if harnessed in the right way.
2. **Communications and collaboration data comes in varied forms and formats:** The diverse nature of these collaboration tools and messaging platforms means that data stored on corporate systems takes an increasingly wide range of formats, structures and even locations. This can challenge the traditional concepts of custodian collections, linear review and document productions. For example: What is a document in the context of a business slack channel which spans days, months or even years?
3. **Piecing together data from disparate systems can often be the only way to reveal the truth behind a series of disparate events:** As we adapt our behaviours around the usage of these new tools, it's common for conversations or business activities to also span across multiple channels or devices. This multi-modal approach to communication increases the challenge in piecing this information back together. Only in reviewing or producing relevant content in a single stream or chronology can you often tell the real story behind a series of events.
4. **Tools and technologies are often developed at pace with limited consideration to legal or compliance requirements:** As the rate of development and adoption of these tools has increased, it is important to recognise that many of these have not been designed with future discovery requirements in mind. The capture of this data in a forensically sound manner can often be a challenge unless approaches are considered in advance of their deployment.
5. **Defensible deletion protocols are as important as secure retention policies:** The types of tools discussed through this document are often cloud based, hosted by third parties and setup to retain data on the service provider's servers. As such it's important to understand legal and regulatory implications of any retention policies, rights of access and any SLA's which you may have to call upon, as well as any defensible deletion policies you may need to consider. Afterall retaining too much data can be as problematic as not retaining enough.

Here are 5 actions you can take now

1. **Understand the systems in use within the Organisation:**
Create a map of all applications used within your organisation and the types of data stored within them. This can become a building block within your records management process and a key scoping document for each new matter you embark upon – Providing a useful foundation to evaluate what you need and where you need to get it from.

2. **Conduct a regular review of your systems and your technology onboarding process:**
No longer can you rely on a 'set and forget' approach to records management. Conduct a review of systems currently deployed within the organisation and actively participate in activities leading up to the onboarding of any new technology products. This will support alignment between technology teams, the legal and compliance functions and the wider organisation. For regulated organisations this may involve the periodic validation of any capture controls by external parties to provide you with the confidence that you're fulfilling regulatory expectations.

3. **Capture the data in its native form to derive the most value:**
Establish protocols to defensibly capture the data in a form as close to the original source as possible. Connectors which allow you to tap in to the source systems through automation (i.e. using API's) can deliver great value as they allow for the richness of the data to be exploited and enable this valuable source of information to be leveraged as evidence, confident that it is complete, accurate and admissible.

4. **Be deliberate about what you're keeping and deleting, where it's stored and how you can retrieve it:**
Develop a comprehensive strategy around the data retention and disposition of cloud hosted or third-party licensed collaboration and chat platforms. Beyond this, consider what corporate data may be stored within personal devices, such as mobiles, or on private messaging applications such as WeChat and WhatsApp, and what steps you may need to take to interrogate this data if required.

5. **Have your response plan mapped out:**
Whether conducting an internal investigation, preparing a regulatory response or producing data to opposing parties, consider what resources, both internal and external, you will need to support you through this journey. Developing a strategy or playbook to enable you to quickly and effectively review this material, and respond to issues as they arise, can deliver substantial cost and time savings and minimize any day-to-day business disruption.

To discuss any of these important actions above, please reach out to:

Alex Comyn
alcomyn@deloitte.com.au
+61 (3) 8486 1835

Sam Lamble
slamble@deloitte.com.au
+61 (0) 3 9671 8786