Meeting the data governance challenge of ephemeral messaging

By Albert Barsocchini, Director of Client Advisory Services, NightOwl Discovery

Ephemeral messaging, typified by Snapchat or WhatsApp's time-limited messaging features, may at first glance appear to have no place in Chambers. This type of encrypted self-destruct messaging, however, is in increasing use within the legal world for sharing confidential information.

The attraction of ephemeral messaging is that the content of the messages automatically disappears from the recipient's device within a short time of receipt. It is very difficult to capture and store information sent in this way, or send it on to third parties. As a result, organisations are turning to this channel of communications when they need to conduct a confidential investigation or to prevent leaks of sensitive information.

The issue is that information shared through self-destruct messaging is kept off corporate systems and is not available later on, should a process of litigation or legal discovery begin. This is set to cause major headaches for barristers. As the use of the technology in the corporate environment is relatively new, legal precedents are yet to be set. Uber employees' use of ephemeral messaging app Wickr came under legal scrutiny at a pre-trial hearing of a trade secrets case. Timothy Heaphy, a lawyer at Hunton & Williams and a former U.S. Attorney in Virginia, was reported as commenting that although there is nothing inherently unlawful about instructing employees to use disappearing messaging apps, companies do have an obligation to preserve records that may be reasonably seen as relevant to litigation or that fall under data retention rules set by industry regulators1.

Information governance to self-destruct messaging

Ephemeral messaging holds undeniable appeal when it comes to sensitive negotiations or confidential communications. But barristers need to be realistic about how this will look when it comes to compliance or future litigation. The existence of secret, recorded conversations taking place in the context of Chambers is at the very least likely to ring warning bells. If the technology is to be used at all it is vital to have strong policies and controls that recognise Chambers' obligation to preserve data.

Best practice in information governance is to set controls even before document are created and certainly before they are shared. Normally, controls would include labelling the document by category and content, setting time limits for the storage of documents, known as time-to-live or TTL, and restricting access permissions by job role or geographical location. None of these requirements goes away simply because barristers are using ephemeral messaging but all of this is achievable on a single corporate ephemeral messaging technology platform like Wickr.

Chambers should assume that barristers are or will be using ephemeral messaging and put steps in place to address that:

1. **Bring secret messaging out into the open.** Let barristers and clerks know that the Chamber understands there will be circumstances in which ephemeral messaging makes sense. Create a culture of transparency around its use that will enable a meaningful audit of the Chamber's usage of ephemeral messaging and creation (and deletion) of ephemeral data.

Which platforms and features are barristers using? Track any changes to keep policies and controls updated. Currently, it would appear that where the corporate document retention policy provides for the routine deletion of data and there was no existing duty to preserve at the time the information was destroyed, no legal issue of spoliation arises. But that could change in relation to ephemeral data, as case law is created.

2. **Create a multidisciplinary team to set acceptable use definitions and access permissions.** Heads of Chamber, Silks, barristers and clerks should be represented. This team should meet regularly to review how the Chamber is currently using ephemeral messaging and what data is involved. The next step would be to consider all possible scenarios where documents and data subject to regulatory requirements may end up being transmitted and destroyed by time-limited encrypted messaging apps. This should be a constructive approach that aims to determine acceptable uses of the technology and log them in a centralised and accessible acceptable use policy manual. This team should also determine permissions for individuals or groups of employees to use ephemeral messaging, similar to access control permissions applied to Chamber computer networks.

3. **Communicate regularly with barristers about how they should and shouldn't use ephemeral messaging in real life scenarios.** Individual barristers and clerks may be given access to relevant data and documents held on the formal in-house intranet through a system of access controls that works in the background. In the case of ephemeral messaging it may be more a matter of making it clear to them what they are allowed to share and clarify exactly when it could become an issue if important data is encrypted or deleted by ephemeral messaging systems. Communications might extend as far as mandating training modules so that there is consistent understanding of the acceptable use of and issues around ephemeral messaging throughout the Chamber. Completion of training also provides clear evidence that the Chamber has a clear view of its data governance responsibilities on every possible platform.

The growing number of high profile data breaches and the recent tightening of data protection legislation is having a positive impact in driving awareness of everyone's role in keeping data safe. The danger is that this heightened awareness will drive barristers into the arms of ephemeral messaging apps – with the resulting potential for loss of crucial data and a resulting catastrophic impact on the reputation and business of the Chamber.

It is crucial to act now and address the risk of misuse and non-compliance that comes with this new technology by first getting clear picture of how it is used and how it might be used in future within the Chamber. In the light of these findings, Chambers should be looking to develop their data governance policies to reflect new realities around ephemeral data. A strong usage policy helps demonstrate that barristers within the Chamber are using self-destruct technology responsibly and in good faith for legitimate reasons and is key to compliance.

About the author
Albert Barsocchini is Director of Client Advisory Services, NightOwl Discovery.

Reference
1 https://www.reuters.com/article/us-uber-waymo-evidence/ubers-use-of-encrypted-messaging-may-set-legal-precedents-idUSKBN1DU099