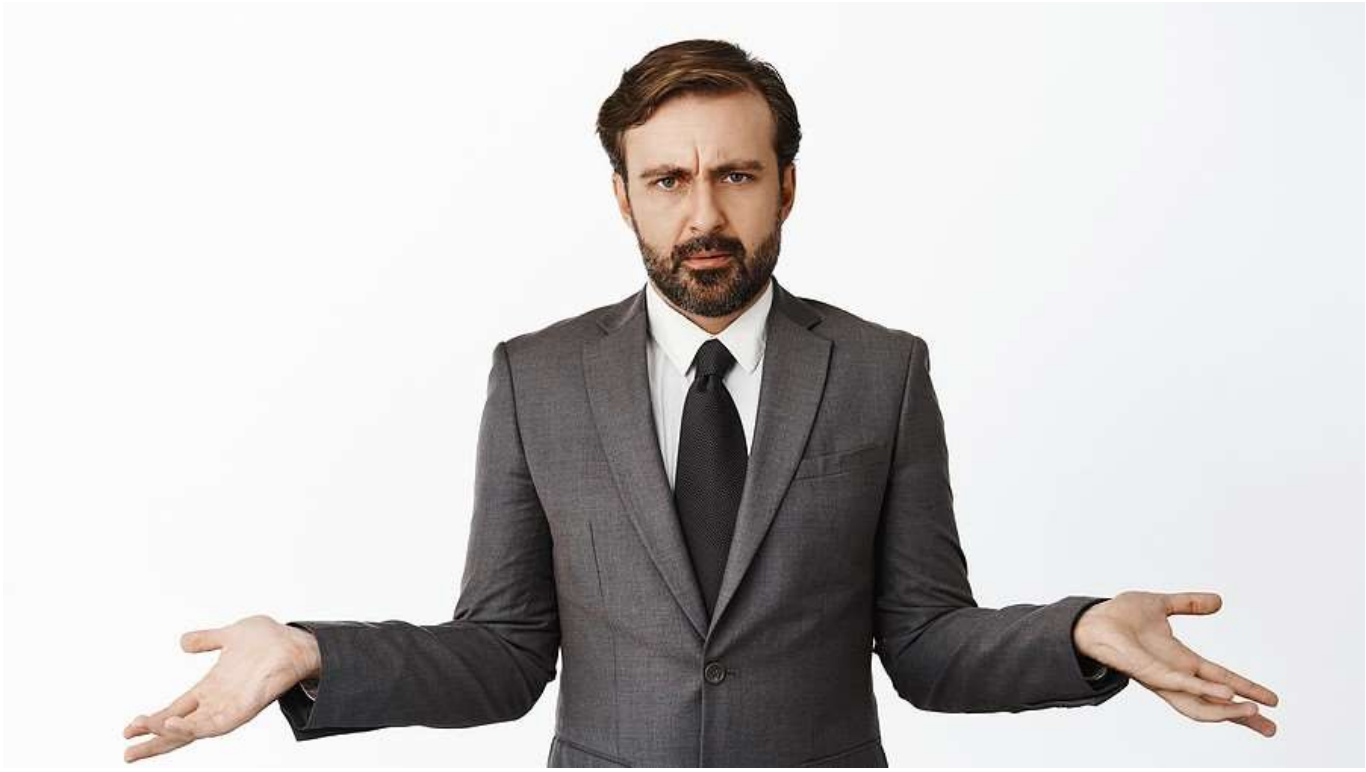
# Why Lawyers Need to Understand Shadow Data



Organizations gather massive quantities of data, using that data to inform decision-making and business strategy. However, while data plays a critical role in business success, it can also increase security and compliance risks. When advising their clients on cyber security, legal teams must take into account the dangers posed by shadow data.

In a digital environment dominated by cyber threats and privacy regulations, proactive organizations take great care to protect sensitive data. For instance, healthcare organizations bolster security around their EMR. But they may be neglecting shadow data, the sensitive data that lives outside the EMR, beneath the radar of the IT department.

## Where Shadow Data Comes From

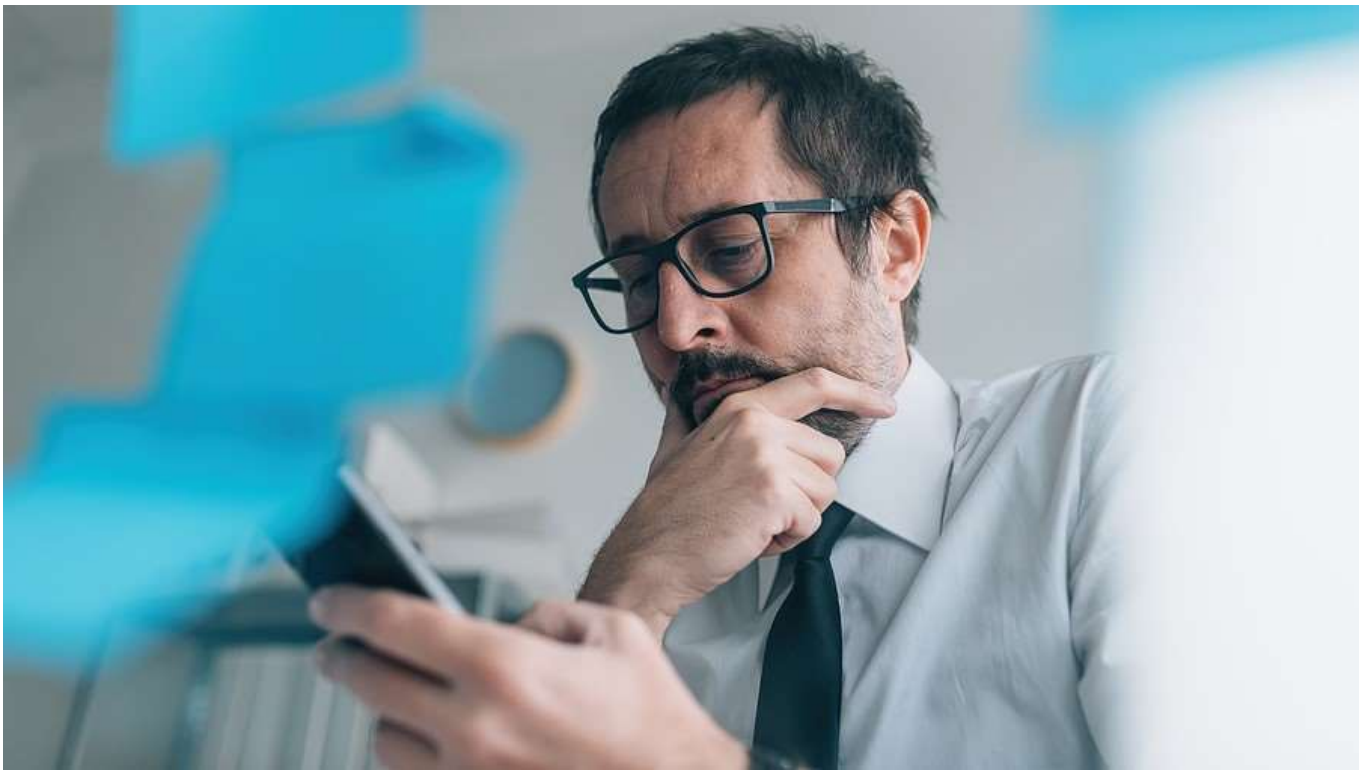
In simple terms, shadow data refers to data that remains invisible to the tools used by IT and security teams to monitor and secure information. This data can come from a variety of processes and live in various places.

For instance, in a constant drive to increase productivity, employees often turn to shadow IT to work more efficiently. For instance, they may use unsanctioned tools and services to share documents or message colleagues. Data present in those tools, outside the view of IT, becomes shadow data.

Multi-cloud environments also contribute to the growth of shadow data. With so many cloud locations, data slips through the cracks. As an example, many organizations keep backups in the cloud. While a wise protection strategy, these backups live in the background with little oversight, despite containing a wealth of valuable data.

Even the process of migrating to the cloud can create shadow data. Organizations that move from a legacy system to the cloud may leave unused and forgotten copies of data in the legacy system.

Additional examples of shadow data include test data used by developers and never deleted, as well as data left behind by former employees. Various applications generate hard-to-find local data stores, as well. For instance, GroupWise personal archives can exist wherever the user chooses to place them.



## Ignoring Shadow Data Can Prove Dangerous

Legal and IT teams may not be aware of the existence of shadow data in their organizations. However, hackers fully understand the value of that data, and they have sophisticated methods to find it. That makes ignoring the shadow data problem potentially very costly.

For instance, while healthcare organizations take great care to secure their EMRs, most data breaches occur outside the EMR. Care providers may share sensitive information through email or unsanctioned messaging apps, for instance. However, HIPAA requires that organizations safeguard sensitive patient data no matter where it lives.

Because shadow data poses significant risk, organizations need to find ways to gain visibility into that data. They then need to classify and monitor sensitive data, wherever it resides. And they need to tighten the security controls that govern access to that data.

## Find and Classify Data

To take control of shadow data, organizations need to gain visibility into all data storage locations and tag sensitive data. Creating an initial data map can prove challenging, as the security team will need to

shine a light into all possible data environments. Fortunately, the information governance industry makes tools and automation available to ease the process.

For instance, Microsoft Purview provides tools to classify data both manually and automatically, thus creating an "elastic data map." Using pattern matching, the system can apply classification tags automatically, labeling information such as credit card numbers. Additionally, trainable classifiers use machine learning to identify specific types of content based on examples.

With sensitive data tagged, organizations can follow that data across environments with continuous, automated monitoring. They can also ensure encryption and appropriate retention of sensitive data and guard against improper sharing.

## Control Access to Data

In addition to identifying sensitive data, organizations need to control access to that data, ensuring that users have just the access they need. For instance, security teams may implement role-based access. Tools like Microsoft Entra help organizations right-size permissions and monitor for permissions risks.

## Minimize the Risk of Shadow Data with Information Governance

No tool or policy will completely eliminate shadow data. However, by implementing consistent information governance strategies across all environments, organizations can mitigate the risks posed by shadow data. The information governance consultants at Messaging Architects can help you get started, with tools to help you locate, secure, and monitor data wherever it lives.