Bloomberg Law

Corporate Law & Accountability Report™

IN-HOUSE COUNSEL

Data Issues Keeping Counsel Up at Night (and Concerns for 2018)

BY CHRIS ZOHLEN

While 2017 didn't introduce any ground-breaking or unforeseen headaches for legal professionals, what we did see was a steady stream of growing complexity and prevalence of existing challenges. Regulatory agencies have been increasingly diligent in their demands for data. Hacks and data breaches are constantly making headlines, with cyberattack tactics evolving daily. Technical diversity is creating chaos, with new applications appearing on the scene faster than packaged software to deal with them can be modified.

Additional factors, including workplace challenges stemming from mobile device usage and globalization, are putting new demands on data storage and access. Lines are blurring between professional data ''owned'' by a company or by an individual and many users do not know how to or do not want to maintain separate professional and personal electronic identities. Many organizations are grappling with how to set the highest bar for protecting data. Firewalls and other traditional safeguards have now been breached, so efforts must become more sophisticated. Largely, IT and legal departments don't know what's in their data universe and lack control over how users move, share and delete data. Mapping the enterprise's information, and understanding where data lives and how it flows continue to be difficult for legal teams to execute.

Chris Zohlen is a managing director in FTI Technology's Information Governance, Privacy & Security Services (IGP&S) practice, with more than 15 years of experience in information governance and legal technology. He helps legal, records, IT and information security departments identify, develop, evaluate and implement in-house e-discovery and data governance processes and programs.

In looking back at 2017, there are a handful of issues that led to sleepless nights for counsel. Below is an overview of the top concerns from last year, many of which are expected to continue bringing challenges in 2018.

- **GDPR and privacy-related issues:** The General Data Protection Regulation (GDPR) goes into effect in May 2018, yet many multinational companies are just now starting to prepare for compliance. This regulation requires organizations to meet stringent data protection requirements over personal data of EU citizens and may impact companies that are based outside of Europe. Many corporations are struggling with obtaining appropriate funding for the work that is required. Much like IG, GDPR preparedness requires involvement from stakeholders across legal, IT, line of business, and security. Companies are also challenged with contract renegotiation to comply with enhanced data processing standards, which require data controllers and data processors to review their data supply chain and ensure that commercial terms are compliant with the GDPR. Keeping track of and ensuring collaboration and compliance across these many moving parts is a complex ordeal and one that counsel must be prepared to address.

- **Hacks, data leaks and privacy violations:** Corporate IT and security departments face the pressure of getting security right every day, all of the time, in every scenario, while a hacker or an accident only has to happen once to wreak havoc. We saw this time and again last year, particularly with the global WannaCry incident, one of the most highly publicized cyberattacks and a wake-up call to the importance of ongoing and proactive cyber vigilance. While counsel may not be the primary owner of the many steps organizations must take—including encryption, anonymizing data, putting a wall around sensitive information—to protect the organization, legal is impacted and considered a responsible party when a breach occurs. Most effective cybersecurity measures require a lot of expense and effort to implement, and leaks can happen despite the best efforts. But security and data protection must be a high priority for every corporation. Legal has an opportunity and responsibility to take part in ensuring all possible protections are in place before a major attack.

- **Shadow IT:** With BYOD (Bring Your Own Device), Internet of Things (IoT) devices and data sharing apps now common factors in most workplaces, legal has a growing pool of data that lacks formal organizational structure or oversight. Shadow IT is risky because it can expose security vulnerabilities that IT is unware of, and can also cause issues if there is an obligation to preserve some of the data created by those sources for legal hold requirements or compliance inquiries. There are technology solutions that can help with limiting how data sharing sites such as Dropbox are used and how mobile data is managed across company-owned and employee-owned devices. Cloud Access Security Brokers (CASBs) are also maturing to help enable security between cloud-based and on-premise data usage. But the most important element of addressing Shadow IT is policy development followed by thorough employee training on the processes. Policies should also have some teeth to them that press the significance of compliance.

- **Non-traditional data types:** Legal and e-discovery requirements are not a priority for public app developers, and most emerging apps are often missing critical features needed to collect data for legal and compliance purposes. Texting, collaboration platforms, and social media are all data sources that can and do come into play for e-discovery matters. Unfortunately, they can be complex to collect, search, and index. Moreover, rapid changes to apps may break tools used for legal management, creating further headaches for counsel. While app culture will continue to overwhelm many organizations, there is an opportunity to leverage all of the knowledge that resides within those repositories and begin to establish greater control.

- **Cloud migration:** As cloud solution adoption becomes increasingly widespread—Microsoft reports that 90 percent of the Fortune 1000 is using its cloud products—counsel are gaining increasing exposure to migration initiatives. Legal and compliance groups have a lot to gain from features within Office 365, but face equal or greater risk if the process is not conducted in the context of strong legal and regulatory guidelines. All too often, cloud migrations are spearheaded by other organizations, and legal considerations are not factored in until late in the process or after the transition is complete. This lack of early involvement can adversely impact legal hold, e-discovery needs, policy enforcement, and other issues that affect the legal department. Counsel must have a voice when it comes to cloud migration decisions and understand the opportunities these initiatives bring to meeting their needs. By ensuring involvement early on, or better yet, leading the initiative, counsel can optimize cloud solutions to help with common legal tech challenges.

- **Unchecked data volumes:** Historically, data volume concerns were based on cost considerations—the greater the volumes, the greater the storage and data center expenses. Cloud adoption has modified the economics, and now counsel are focused on the risks associated with large volumes of stored information not in the IT group's possession. This includes risk of lost or stolen data and the difficulty of wading through large pools of data to find potentially relevant documents for litigation.

- **Incomplete data preservation efforts:** There are two considerations around preservation with which counsel is concerned. The first is thorough scoping to preserve anything potentially relevant during active litigation. Given the issues identified above—expanding locations for corporate data and the number of data types—this is increasingly more difficult and presents new challenges. The second is more within the realm of information governance (IG) and ensuring comprehensive, defensible legal hold processes and streamlining workflows across the Electronic Discovery Reference Model (EDRM). Counsel must take the time and energy required to ensure that all data and custodians that are under legal hold have proper preservation guidelines in place around them, and enable straightforward procedures for turning those guidelines on quickly when new legal hold obligations arise.

In 2018

We are starting to see counsel become increasingly proactive on these issues, and will likely see more of that this year. This includes conversations around cybersecurity and the overall data health of the company spanning a wider group of concerned parties, including executive leadership and the board. The struggle is often prioritizing how to fix hundreds of issues and enable a trickle down of those solutions to the tens of thousands of employees that also have a role to play in maintaining security and policies. The good news is that people are generally becoming more aware and vigilant about cybersecurity in a non-professional setting, and are taking increasing caution in protecting their personal data from hackers. Because cybersecurity is now hitting closer to home, we'll likely see employees become more active in supporting security in the workplace as well. IG teams will still need to put change management and training front and center in their programs, but those efforts will begin to be more widely understood and adopted.

This year, counsel will also need to be prepared for a changing regulatory environment given the new administration and a changing global scene in light of Brexit, GDPR, etc. We're seeing the administration seek stronger cybersecurity efforts and funding to that end. Counsel must keep a close eye on these developments, and modify their policies and safeguards accordingly. Ensuring that company processes are robust enough that they can be changed frequently and easily is one basic way to establish readiness for any forthcoming changes.

Enabling a Healthier Organization (and Better Sleep)

The key to easing the burden of the concerns outlined above is for counsel to first start having the important conversations around these issues, and make sure those conversations include key stakeholders across teams. From there, counsel must get a solid grip on the data landscape of the organization. Knowing where and what the data is, how much there is, who manages it and how it is used is the necessary first step toward figuring out what programs and solutions are needed.

Identifying what data is sensitive and protecting the most critical data is effective in reducing risk. Routine and consistent data remediation and establishing enforceable policies that require employees to keep personal and company data separate are additional best practices to simultaneously improve security, navigate new data types, and lower e-discovery burdens. When counsel is aware of what data the organization has, where it is and what the value of it is, it is possible to make sound decisions as to how to approach cybersecurity, enable privacy, manage retention and deletion, and know where to look for key information in the event of litigation. This process of understanding data flows can serve as the baseline to get projects off the ground and begin easing the sea of concerns that will be on counsel's mind for the foreseeable future.