LAWYER
MONTHLY

What Are The Legal Pitfalls Of Online File Sharing?

We all know Google Docs, Share Points and other workplace collaboration tools are convenient. The problem is that employees start saving personal information in places that aren't governed blurs the lines of data and puts the entire organization at risk.

While all of these all methodologies definitely make employees' day to day jobs much easier, it can cause many long-term security or even legal challenges. Here Lawyer Monthly speaks to Kon Leong, CEO of ZL Technologies to learn more.

DO YOU THINK A SIGNIFICANT AMOUNT OF MID-SIZE TO LARGE ENTERPRISES ARE USING GOOGLE DOCS AND SHARE POINT, OR DO LARGER COMPANIES HAVE MORE SOPHISTICATED PLATFORMS? DO YOU BELIEVE THAT EMPLOYEES ARE USING NON-MANDATED FILE SHARING TOOLS?

While more sophisticated file sharing tools exist, it is a near inevitability that company information will make its way onto free file sharing services. Therefore, if your organization is not prepared to integrate Google Documents into your information governance, a new silo will be born.

WE KNOW THESE TYPES OF WORKPLACE COLLABORATION TOOLS ARE CONVENIENT, BUT WHAT ARE SOME OF THE LEGAL OR SECURITY RISKS ASSOCIATED WITH USING THEM?

New silos further fracture organizational control over data creating legal and security issues for any enterprise. From a security perspective, a free online file share service can only be as safe as the weakest security link. Commonly used passwords, failure to set up two-step verification, or simply forgetting to logout in a public location can all compromise document security. From a legal perspective one has to ask if these files would be readily discoverable by a legal team.

IS THE DATA THAT LIVES IN THESE TYPES OF DOCUMENTS GDPR COMPLIANT? IF NOT, WHAT CAN ORGANIZATIONS DO TO ENSURE COMPLIANCE WITH DATA REGULATIONS?

GDPR respects no silos. If an organization wishes to ensure GDPR compliance in any type of file share environment, they must have an iron grip over all their data. That means bringing together every silo so that all data is readily searchable and manageable via holistic information management. Currently, organizations aren’t even aware of all the repositories that requirement management, let alone are they actually able to apply policies across them. This means there is a lot of dark data out there that could be creating unidentified risk.

YOU MAY ALSO BE INTERESTED IN:

Staying on the Right Side of the Law in a Digital World

Was the FTC’s $5 Billion Facebook Fine Enough?

HOW DOES THE PROLIFERATION OF FILE SHARING AND COLLABORATION CHANNELS IMPACT EDISCOVERY EFFORTS? IS IT PUTTING COMPANIES AT RISK?

The risk created by silos of unmanaged file shares on eDiscovery efforts cannot be understated. Imagine trying to perform an e-discovery search when data lies across various siloes, each with its own search engine, each with its own limitations. Thus, in order to successfully complete comprehensive eDiscovery, one needs to be able to search across all these silos, also known as unified data management.

WHAT ARE THE DANGERS AND LEGAL IMPLICATIONS OF BLURRING TH LINES BETWEEN PERSONAL AND COMPANY DATA?

When enterprises perform analytics on company data from emails, instant messages, and various file shares, there will almost inevitably be personal information that coexists within the data. For instance, employee analytics done on company IMs and emails can reveal who works frequently together in an organization, but it may also reveal personal conversations, opinions and other sensitive data that opens the company up to risk—cybersecurity, legal, regulatory, and otherwise. Or to provide an extreme example, what happens when the CEO's emails end up in the wrong hands due to an analytics initiative?

WHAT CAN ENTERPRISES DO TO PREVENT CHALLENGES ASSOCIATED WITH EMPLOYEE INTRODUCED VULNERABILITIES?

Organizations have made efforts to protect from the outside (i.e. perimeter security) but there is still much to be done to protect it from the insider threat. Employees create valuable and sensitive data every day, and this internal data is vastly powerful because it reveals human intent. However, employees are also often the biggest threat to protecting that data, unfortunately. With regards to its protection, organizations are often too preoccupied with the 0s and 1s of data to think about the ABCs—in other words, looking into the actual *content* of documents in order to classify and apply governance.

By **Kon Leong** Last updated **Oct 7, 2019** 🗨 0 PUBLIC & REGULATORY COMMERCIAL CORPORATE LEGAL TECH