

Beyond Data Collecting: How to Protect and Leverage Big Data

Technology, Privacy, and eCommerce



Big data is a top-of-mind priority for in-house counsel. In fact, the *ACC Chief Legal Officers 2018 Survey* found that data breaches and the protection of corporate data keeps 70 percent of respondents up at night.

Despite this concern, many in-house counsel state that they don't use technology to leverage their data. Only 65 percent of in-house lawyers have considered using automated services to process data and reduce risk, according to the ACC Law Department Management Report.

For those technophobic lawyers, the *ACC Docket*'s March 2018 cover story, "Big Data, Big Business: Leveraging Analytics to Strengthen Your Legal Department," presents the benefits of using automated processes to increase efficiency in legal departments.

We followed up with Allison Trimble, one of the article's authors, for more insight on maximizing corporate data. She discussed information governance best practices and how they apply to working with big data, information security best practices (including having a breach response plan), and how to find the best contract management system for your legal department — even if you have to do more with less.

ACC: In your article, you stress that the first step to leverage big data is to collect it. What are some common security risks that GCs and in-house counsel face when they gather data?

Allison Trimble: Any data collection, including collection for the purposes of analytics, should follow information governance practices established by the corporation as well as any other applicable laws and guidelines in order to mitigate legal risk. Typical information governance practices that would apply for purposes of data analytics include: limiting the information collected to that which you

actually need, providing notice and obtaining consent when necessary, avoiding collecting sensitive information, and de-identifying data sets when possible.

When collecting data for purposes of evaluating past legal claims or evaluating trends in legal settlements, there is an additional layer of reputational risk and harm to current legal strategy that may occur if such information is not adequately protected. Proper steps should be taken to ensure outside counsel have reasonable information security programs in place and expectations should be clarified regarding to whom, if any third parties, those firms are permitted to disclose your confidential information. For example, you might prohibit a firm's disclosure to a third party artificial intelligence vendor.

ACC: You also discuss "leverag[ing] big data for purposes of identifying patterns that could be indicative of future security risks." What are some of the most common areas that in-house counsel forget to review or protect?

Trimble: I don't think there are specific areas that are "forgotten," per se, but the continued challenge that all organizations face is managing an information security program that is agile and responsive to changes within the organization itself as well as the legal requirements of the industry in which it operates. As an example, the definitions of "personal information" and "sensitive personal information" are a moving target these days.

It takes a concerted effort between members of legal, IT, and privacy/risk groups to monitor changes in privacy and cybersecurity laws, determine the applicability of those laws to your organization, and then facilitate measures to operationalize those changes in order to remain compliant. The ability to execute this process well and in a quick manner is the challenge we all face over the course of the next few years.

ACC: Companies should undoubtedly be less reactive and proactive when it comes to data privacy. But what should in-house counsel do if they find themselves breached?

Trimble: An organization should already have a breach response process in place (ACC's website provides many helpful resources in this regard), which outlines the process for securing operations, fixing vulnerabilities, and notifying the appropriate parties in the event of a breach. As part of that process there should be consideration for when to notify the organization's outside counsel, insurer, and, if applicable, independent forensic investigator.

In addition, the organization should also establish the internal team that will execute the breach response plan, which will likely include members from IT, legal, and representatives from the relevant business lines. For purposes of reducing the risk of breach under most applicable laws, it's always good practice when working with data analytics to limit the information collected to that which you actually need, avoid collecting sensitive information, and de-identify data sets when possible.

ACC: As for selecting software, contract management systems (CMS) are a reliable solution for in-house counsel to leverage data. What's the best way to determine if a law department needs this software?

Trimble: If you answer "yes" to any of the questions listed below, your organization would likely benefit from a contract management system:

1. Do you need the ability to report and analyze contract turnaround times?

2. Do you need to evaluate the type of legal work generated by your department for purposes of work load balancing and leveraging personnel with the right skill set?
3. Do you need the ability to decrease the amount of time it takes to create and/or combine contract templates?
4. Do you need the ability to quickly compare and evaluate common negotiation points across multiple client agreements?
5. Do you need reporting functionality to allow you to summarize and track your contract obligations?

ACC: You offer a guide for legal departments that might not have the budget for software solutions. What are some common missteps that in-house counsel have made with a more affordable CMS, and how can these mistakes be avoided?

Trimble: The following are common missteps in-house counsel make when using a more affordable CMS as well as suggested preventative measures that counsel can take to avoid these pitfalls:

1. Pitfall: Duplicated efforts. This pitfall is common in large organizations, where subsidiaries may have their own assigned legal teams that are deploying a CMS different than the parent organization (or other subsidiaries).

Solution: Involve representatives from all legal teams and ask that individuals disclose the CMS that they are currently using in order to identify the best universal approach. You may be able to save time and money by leveraging a tool that is already licensed to your organization and has been tweaked for purposes of serving as a CMS.

2. Pitfall: Not exploring the full functionality of a licensed software solution prior to its implementation as a CMS. If you plan to leverage a solution that your organization originally licensed for a purpose other than CMS, the internal group that originally procured the software solution may only appreciate its “off-the-shelf” functionality for which it was originally purchased.

Solution: Engage the right technical resources that will assist you in exploring the full functionality of the licensed software solution and allow you to modify and configure the off-the-shelf solution further so that the end result gives you a robust CMS.

3. Pitfall: Not conducting proper due diligence prior to converting a pre-existing licensed software solution into a CMS.

Solution: In order to avoid violating the terms of your license agreements with third party vendors, make sure to thoroughly review the terms and conditions of those license agreements to ensure they provide your organization with the scope of use right to leverage the solution as a CMS for the intended number of users. You should consider engaging legal representatives from your procurement department to assist if you determine that the scope of the agreement must be increased or additional users added under the agreement.

4. Pitfall: Ignoring the need for efficiency. It is tempting to utilize a CMS for purposes of recording every minutia of detail from a contract because “you never know when you’re going to need it.” In reality, this practice makes the administrative tasks of uploading detail even more time consuming and hurts reporting capabilities.

Solution: Determine what information your organization would benefit the most from collecting and

record that information in a manner that supports reporting capabilities. For example, consider using radio buttons, such as simple “yes” or “no” check boxes to input information rather than free text boxes, which don’t allow for information to be pulled into reports as easily.

5. Pitfall: Over-complicating what should be a simple task. If the solicitation of information within the CMS isn’t written in a plain, straightforward manner, only the original creator will understand the intent of the questions, and the process can’t be uniformly duplicated across teams of personnel. This ultimately leads to inconsistent methods of data collection.

Solution: Keep the design simple. Theoretically any individual should be able to provide the contract detail being requested within the CMS with little difficulty, and the nature of the responses should remain consistent across personnel.

Allison Trimble



Associate Senior Counsel

DST Systems, Inc.

Karmen Fox



Web Content Editor

ACC