Top 10 Technology Trends and Topics for Attorneys to Watch

Written By **E. Bradley Evans** (ebe@wardandsmith.com)

March 6, 2020

From technical competency to artificial intelligence to cybersecurity, Ward and Smith's Director of Information Technology Charles Collins counted down the top 10 most critical technology topics for lawyers.

Collins has more than 15 years of experience in IT and application development for the legal industry and is responsible for leading Ward and Smith's evaluation and implementation of all technology platforms. His "Top 10" presentation was part of Ward and Smith's 2019 In-House Counsel Seminar.

No. 10: Technical Competency

As of September 2019, 37 states — including North Carolina — have adopted the ethical duty of technical competence for lawyers, Collins said.

"It's a big topic for everybody in the room," he said. "They now require you to complete one hour of CLE devoted to technology."

Many younger attorneys, he said, are expected to be able to use technology in their legal practice. And many companies expect their attorneys to know what technology is available to them and understand how to use it to maximize the value of their legal services.

Cybersecurity, e-discovery, docketing, file-sharing, and other existing and emerging technologies are critical for attorneys to understand, Collins said, as they become more and more widely used in courtrooms and other legal settings.

No. 9: Legal Lean

Legal Lean and Lean Six Sigma are a combination of process improvement, project management frameworks, and tools geared toward legal practice.

"It takes 'lean,' which is identifying the waste in a process, and 'Six Sigma,' which identifies the defects in a process and it kind of combines those and adapts them for a legal environment," Collins said. "What we're

able to do for our clients is to identify processes that can be improved throughout the firm and then create consistent, reliable, efficient, predictable outcomes."

Collins and several others at Ward and Smith are trained and credentialed in Legal Lean Sigma and Project Management by the Legal Lean Sigma Institute.

Many people in law do things the way they do because "this is how I've always done it," Collins said. "That doesn't necessarily mean that's the right way to do it anymore. Technology has changed and evolved in a way that that process could be streamlined and improved."

No. 8: Applications

For applications, Collins created a top 10 list of the types of software that are most important for lawyers. They are:

1. Productivity apps, such as Microsoft Office.
2. PDF applications.
3. Document automation software.
4. Document management programs.
5. Time and billing applications.
6. Case management software.
7. Data back-up apps.
8. Project management programs.
9. Internal instant messaging tools and enterprise social networks.
10. Collaboration tools.

Many of the applications in these categories have desktop computer versions and mobile versions for smartphones.

"The only caveat I'll say is that with your mobile devices, they may not be as feature-rich or as robust as what you could get on your desktop or laptop," he said.

No. 7: Adaptation and Adoption

Client demands, Collins said, are driving how the firm is evolving its practices and technology.

"To stay on top of that, we have to be more proactive than reactive," he said. "We need to understand what it is you want and put those in place before you come and ask for it."

New technology allows the firm to streamline processes and workflows, provide more reliable and predictable outcomes, and provide higher quality work more quickly and, sometimes, more cheaply.

Do you want to go with someone who says they can do it?" Collins asked. "Or do you want to go with somebody who says they're already doing it?"

No. 6: Document Automation

Document automation uses templates, plus data already within a company or law firm, to quickly generate

customized legal documents.

"I'd say it's probably one of the most beneficial technologies available to law firms because it allows us to remove the need to edit and create documents manually," Collins said. "It reduces errors by automating that process and eliminating a lot of manual entry."

Because lawyers spend most of their time drafting documents, it also speeds up legal work and reduces costs by allowing attorneys to create documents more quickly, he said.

No. 5: Artificial Intelligence

AI is not going to replace human lawyers anytime in the foreseeable future, Collins said, but it could dramatically change how lawyers and legal departments work.

Machine learning, for example, is being used for legal research and programs that predict litigation outcomes, Collins said. E-discovery software can speed up the sometimes-laborious task of searching through many documents.

AI will probably enable legal departments to work faster and cheaper without the loss of quality," he said. "It's still early. We don't know exactly how it will evolve within the legal industry at this time."

Nonetheless, AI applications focused on due diligence, contracts, legal analytics, and other critical functions.

No. 4: Data breaches

Data breaches are happening to all kinds of people and organizations every day, according to Collins. He identified three main types of breaches: ransomware, user error, and phishing.

Ransomware is a malicious program that encrypts data on a computer and holds it hostage until the owner can make a payment to decrypt it.

"This is where data backups really come in handy," he said. "When that data gets encrypted, and it gets held hostage if you have your backup, you can just restore over and recover. If you don't, you have to face a choice as to whether you lose that information or whether you pay that ransom."

User error is when information is accidentally sent to the wrong person. This can be as simple as a mistyped email address. Phishing is a fraudulent email that contains a link that unleashes malware when it's clicked on.

In 2017, one global law firm was entirely shut down within 20 minutes of an administrator clicking on a link in a phishing email. The entire firm was down for a week, and it took them months to recover fully.

Think about the lost work product. Think about the reputation when you have to recover from something like that," he said. "It's really, really important to pay attention to what you're doing."

No. 3: Be Proactive with Security

This means not only having the right technology in place, Collins said, but also providing training to all employees about how to recognize and prevent cybersecurity intrusions.

Does your organization have a security training program for employees?" he asked. "This is something that most of the attorneys in the room from Ward and Smith are very familiar with. I wouldn't say we made everybody paranoid, but we might make them a little paranoid."

Ward and Smith, he said, goes through security audits from clients, and also conducts its own internal security audits. "Education and awareness are key," he said.

No. 2: Mobile Devices and Cloud-based Software

Nearly everyone has at least one mobile device — usually a smartphone — and some carry more than one, Collins noted.

"Has your cell phone ever been lost or stolen?" he asked. "There's a lot of information that we store on our mobile devices."

It's important for people to understand how their mobile devices work, what company information is on them, how to protect it, and how to back it up. Many companies, he said, use software to manage mobile devices and protect company data that may reside on them.

He advised attendees to back up their devices regularly, put a password on their phones — ideally more than four digits — and make sure it's set to lock when not in use automatically.

"Make sure there's something there protecting that phone," he said.

No. 1: Social Media

Many organizations have social media policies, Collins said. One area to focus on is geo-tagging, which can inadvertently reveal more information than intended in an otherwise innocent social media post.

Geotagging, he said, "is information that's attached to a tweet, a status or a photo that you upload to Twitter, Facebook, Instagram, wherever, that provides the physical location where that post was made."

That kind of information, Collins noted, can be used to determine where you are, when you're there, what your patterns or behaviors are when you're traveling, or on a daily basis.

It can all be used against you," he said. It might allow someone to know when you're not home — making you vulnerable to break-ins — or it could reveal information that could breach client confidentiality.

For example, a publication of a corporate lawyer's location in a restaurant across the street from a public company out of town might prematurely tip-off confidential merger negotiations," Collins said. "It's important that we understand the repercussions behind those posts and that behavior through social media."

More insights from Ward and Smith's 2019 In-House Counsel Seminar:

- Group Exercise Highlights Tricky Employment Law Issues

--