

ABA Cyber Task Force Co-Chair Eyes AI Education Boost

By **Allison Grande**

Law360 (September 11, 2026, 6:03 PM EDT) -- With the legal industry presenting a more and more enticing target for cyberattacks, it's becoming increasingly important for practitioners to know how to best protect clients' data and most effectively use emerging artificial intelligence tools — a task that the American Bar Association's Cybersecurity Legal Task Force is well positioned to assist with, its incoming co-chair recently told Law360.

Kate M. Growley, a Washington, D.C.-based partner at Crowell & Moring LLP and a founding member of the firm's privacy and cybersecurity group, received an ABA presidential appointment last month to serve as co-chair of the organization's Cybersecurity Legal Task Force for a one-year term, alongside Jones Day government contracts and cybersecurity partner Fernand Lavallee.



Kate M. Growley

While the task force has existed for more than a decade, the newly installed duo are taking the reins as cyberattacks on law firms are **on the rise** and attorneys are facing growing scrutiny over how their use of AI systems for research and other work tasks is affecting their ability to safeguard the sensitive and confidential data they hold.

"When you're talking about the biggest cybersecurity challenge facing the legal profession right now, I would say it's the convergence of AI and cybersecurity risk," Growley told Law360 in a recent interview.

"On the one side, you've got AI making threat actors much more sophisticated. You have these phishing attacks that are harder to detect. Social engineering is so much more convincing. The speed of attacks is accelerating," Growley said. "And then on the other side, you have lawyers who are adopting AI tools that introduce these new questions about data security and client confidentiality that we, as a profession, have not yet had an opportunity to fully work through."

Given its position at that intersection of cybersecurity and AI, the 38-member task force — which held its first meeting with its new co-chairs on Sept. 4 — is poised to do "some really important work" in supporting practitioners working through these issues in the coming year, Growley said.

While the task force's agenda is expected to be shaped based on members' input, Growley said that she and co-chair Lavallee have discussed bringing ideas to the group that center on boosting the educational resources available to legal practitioners across the board.

These potential initiatives include not only updating key cybersecurity guidance and expanding learning

opportunities for practicing attorneys but also exploring ways to ensure that law schools are educating aspiring attorneys about the potential effects of emerging cybersecurity risks and growing AI use on their legal and ethical responsibilities to clients, Growley said.

"One of the core mandates of the task force is to educate members of the bar and the public on cybersecurity risks, how to protect data and how to respond to a cyberattack, and at least from my perspective, I think that mission is best served if we ensure that we start it where the legal career starts, which is at law school," said Growley, a longtime ABA member who in past leadership roles has collaborated with the cybersecurity task force on presentations and other work.

Growley talked with Law360 about some of the key initiatives potentially on the horizon for the task force and how these topics intersect with efforts by lawyers, regulators and legislatures to stay on top of rapidly evolving cybersecurity, AI and legal privilege concerns. This exclusive interview has been edited for length and clarity.

The cybersecurity legal task force dates back to 2012, when it was created to help lawyers protect client data and contribute to national cyber policy. What is the mission of the task force, and what does it look like today?

Our jurisdiction is over matters that affect how lawyers protect their practices and their clients' confidential information, particularly in the midst of a cyberattack. And obviously, that's a serious responsibility, and right now, with how AI is affecting the conversation, it's a mandate that's extremely important.

Additionally, the task force is structured to be genuinely cross-cutting. Our members are representatives from each ABA entity that has an interest in cybersecurity issues. We also have members at large and special advisers that, importantly, could include nonlawyer experts in their fields, and that diversity of perspective is one of the greatest strengths of the task force. That structure reflects the breadth of cybersecurity as a legal issue, and how the topic does not belong to any one practice area or section of the ABA. It really touches everything.

What are some potential areas of focus for the task force in the coming months?

As incoming co-chairs, Fern and I see our role as facilitating the dialogue among members. At the same time, we have been doing a lot of brainstorming and have a number of ideas and some potential priorities that we're looking forward to discussing with the task force and getting the benefit of their expertise and perspective on before we come out with a concrete agenda.

One theme we'd like to explore is how the task force can more actively engage with law schools on a curriculum focused on AI and cybersecurity while providing a message, particularly when it comes to AI, that's balanced. A curriculum, we think, is best serving its students and our future lawyers if it focuses not just on the perils of AI but also on the opportunities and foundational literacy that every lawyer is going to need.

Additionally, as part of our responsibility to share best practices with our members, we need to keep our publications current. We have a vendor contracting project that's a bit of a cybersecurity checklist for vendors, so we want to explore whether now is the right time to update that. Similarly, our marquee publication is our ABA Cybersecurity Handbook. It's comprehensive, but it's also intended to be much more accessible to the average lawyer whose practice does not often intersect with the nuances of

these cybersecurity legal issues. I was just looking on my bookshelf the other day and found the 2013 version of the handbook I bought when I was an associate, so I can speak from firsthand experience that it is an extremely valuable guide for any lawyer who's trying to understand cybersecurity, and that is something that we do regularly update. So the question again is: Is this year the right time to do another update, especially with some of the regulatory developments and the shifts in the AI landscape?

We're also going to explore whether we can start offering some CLEs on the ethics of the intersection of cybersecurity and AI that can be open to all ABA members. I certainly can speak to the challenges sometimes of finding opportunities to get that ethics CLE. So we're hoping that this would be an offering that our the ABA members writ large would find quite valuable.

And finally, one of the task force's charges is studying and analyzing executive and legislative national security proposals. There's certainly no shortage of those, and lots of entities within the ABA ecosystem produce proposed resolutions and submit comments in response to policy changes. So part of our mandate is to figure out when these cyber issues are appropriate for ABA engagement, and then working with the ABA Governmental Affairs Office on what advocacy could look like. That's no small task, and something we want to explore within our task force membership is how can we make sure that we are keeping up with those developments and appropriately evaluating the right time to consider engaging and where we can do so thoughtfully and effectively.

What have you observed about how law schools are handling these emerging cybersecurity and AI issues, and what will be important for the task force to take into consideration?

When I was in law school, and I went to a law school that had a really renowned national security curriculum, there was no cybersecurity or privacy-focused coursework because it wasn't in demand. And I do see from the law students who I've had the opportunity to meet with as a part of our recruiting process that they are much better educated on the legal issues around privacy and cybersecurity than I ever was coming out of law school.

However, what I have seen less of and am keen to learn more about in my capacity with the task force is how much of that is translating into legal ethics and your obligations to clients. It's one thing to know how to help a client navigate a data breach. It's another thing to know how to navigate your own data breach that implicates client information, and so that's the other side of the coin that I have seen less of directly through my conversations with new recruits.

In terms of AI, the analogy that has come up a few times is if you go back to the early days of online Westlaw or LexisNexis research, there was some skepticism around that and the move away from books. This could be analogous to how, in the future, having AI-assisted research and drafting tools in the legal profession will just be baked into the cake. So we want to make sure that the next generation of lawyers enter into their practice with this foundation.

Importantly, we can also all learn from law students who tend to be much more comfortable with this technology. Lawyers tend to be very risk-averse and tend to be very busy, which doesn't always lend itself to experimenting with new technology. But with AI being used to both aid and thwart cybersecurity protections, having some basic literacy about what these tools can do is important both for the nature of our practice and also for how we ensure that we're keeping client confidences. That's a core ethical obligation and one that we think the task force can help develop.

What are you planning to look at with respect to updating existing ABA cybersecurity guidance and

other available resources?

The ABA Cybersecurity Handbook and similar publications are among the more practical, practitioner-focused resources that the ABA produces, and we want to keep them that way and not have them become laden with jargon. They need to be accessible to the lawyers who know nothing about cybersecurity because they're not cybersecurity lawyers, but they are lawyers who need to be conversant in cybersecurity for their own practices.

We're also thinking about how we can get out insights out more broadly. Facilitating collaboration and information exchange is central to what we do, and we can explore how to push that further. So the task force itself will regularly have speakers come in to provide perspectives on the cutting-edge issues of the day, and we want to see how we can make those insights more readily available to ABA members writ large. That may be through some sort of regular digest, or a white paper, or a summary update. We're still in the brainstorming stages, but it's important that those lessons learned are not just staying with the task force but are something that can be leveraged for the benefit of all of our ABA members.

Policymakers at the state and federal levels have been ramping up efforts to better secure critical assets and tackle potential cybersecurity and other risks stemming from the use of advanced AI systems. What effect are these increasingly prevalent laws and regulations having on attorneys and their work?

The type of information that lawyers handle in their practice today has become much more regulated, and that means the stakes when this data is mishandled can be much higher, in terms of not only legal consequences but also ethical and reputational consequences. And again, AI has only exacerbated this because AI runs on data. So basic principles such as data minimization and purpose limitation — the obligations that you as a privacy or cybersecurity lawyer would counsel your clients to follow — are being stressed, and there is an opportunity for attorneys to better practice what they preach, because the landscape is only becoming more complex, and AI just complicates the environment, both for better and for worse.

--Editing by Brian Baresch.