Perspectives on privacy, AI, and cybersecurity from the front lines of FinTech and Blockchain | The FinTech and Blockchain Podcast | transcript

March 31, 2025

00:00:00 Dario de Martino Hi everyone and welcome. I am Dario de Martino, an M&A partner and lead of our fintech and digital assets group based in New York. Today's episode focuses on one of the fastest-moving and most consequential areas in fintech and digital assets: privacy and cybersecurity. This conversation is part of our Global podcast series where we explore the issues we believe are shaping the future of financial technology and digital innovation. Joining me today are two of the most knowledgeable people I know in these areas: my partners Helen Christakos, our US privacy lead, and Anna Rudawski, our partner in cybersecurity and incident response. Fintech and digital assets are evolving rapidly. AI is transforming everything from credit decisions to fraud detection. But the risks are also multiplying. Today we'll look at how companies can navigate fragmented regulations, sophisticated cyber threats, and the evolving compliance landscape. Helen, let's start with the basics. What does the privacy landscape look like right now for fintech companies in the US?

00:01:14 Helen Christakos It's really complex, Dario. Unlike other countries, the US doesn't have a single overarching federal privacy law. What we have is a patchwork of federal and state laws instead. At the federal level, we do have laws on specific subject areas such as health information, children's information, or, importantly for fintech, financial information under a law called the Gramm–Leach–Bliley Act. To the extent that it's not covered by federal law, we have state laws in place as well. Twenty states have enacted comprehensive privacy laws, fourteen of which are in effect, and six of which will come into effect over the next year or so. To the extent that they're not preempted by federal law, they are also applicable. Additionally, there are standalone privacy laws on AI and biometric data, which can also be applicable to fintech companies.

00:02:14 Dario de Martino And that patchwork must be a nightmare to operationalize. So how are companies actually handling it?

00:02:22 Helen Christakos There are common threads between the laws. For example, state privacy laws require privacy notices and, in certain cases, consents. But there are also conflicts between the laws. Some are more restrictive, like in California, while others are more permissive. It really depends on a company's business goals. If data is really important to the company for business reasons, they may choose to implement these laws on a state-by-state basis and apply them inconsistently with respect to their consumers, because the more permissive data rights in some states are really important to them from a business perspective. For other companies where data is less important for business reasons, they generally implement the most restrictive approach across the board for ease of implementation and to ensure consumers feel like they're being treated similarly.

00:03:19 Dario de Martino Got it. Thanks, Helen. Anna, from a cyber standpoint, how does this fragmented regime affect threat exposure?

00:03:28 Anna Rudawski It's huge. You have different standards for breach reporting and different expectations for securing data, especially sensitive data like biometrics or data relating to critical infrastructure. So, it becomes really a governance risk, not only a legal one.

00:03:42 Dario de Martino Got it. Let's talk a little bit about biometrics. Helen, how are things like face scans for identity verification being regulated right now?

00:03:53 Helen Christakos It's very layered and complex. The comprehensive state privacy laws that I referred to earlier all regulate biometric data as sensitive data. There are different requirements under different state statutes with respect to collecting and processing that data, sometimes requiring additional notice and consent, and sometimes requiring a DPIA (Data Privacy Impact Assessment) prior to processing that data. In addition to that, there are standalone biometric laws in Illinois, Texas, and Washington, which regulate this independently. Illinois, in particular, has a very aggressive, stringent law, and there's been a lot of litigation in that area with private rights of action and class actions.

00:04:40 Dario de Martino Got it. Thank you, Helen. Let's shift to AI. How are fintech companies actually using AI and how is that regulated right now? Helen, let's stay with you.

00:04:54 Helen Christakos They're using AI for decisioning in critical areas, such as determining who gets access to credit and at what rates. This is precisely the type of critical decisioning that's being regulated by state standalone AI laws. Any sort of generative AI and critical decisioning without significant human oversight in these critical areas is exactly what the AI regulations are tackling. Again, there's no unified overarching AI law; regulation is done on a state-by-state basis. We're also closely watching what's going to happen with the Trump administration with respect to this. Trump has, of course, repealed the Biden Executive Order on AI, signaling an overall more hands-off approach, which could potentially mean fewer federal controls on bias and model transparency. However, to the extent that state laws are in place and are more restrictive, they would still likely be applicable.

00:06:00 Dario de Martino Got it. Anna, are we seeing AI on the offensive side too?

00:06:06 Anna Rudawski Definitely. Right now, the way we're seeing it the most is in really, really good phishing emails. We're also seeing it a bit in our communications with threat actors during negotiations. They're clearly using ChatGPT, and we're seeing a lot of social engineering. The real concern, though, is that this is what's happening now, and I think it will drive threat modeling over the next 12 months. Further down the line, a real concern coming out of regulators is AI that's able to write and iterate on its own malicious code or AI that can scan systems for vulnerabilities and quickly exploit them. When that happens, or if that happens, it will really change the defensive cybersecurity game for a lot of major organizations.

00:06:49 Dario de Martino Got it. Let's talk about a recent case that we all followed closely in the crypto industry, and that's the Bybit case. Can you tell us a little bit about what happened?

00:07:04 Anna Rudawski Yes. A few weeks ago, Bybit was subject to a cyber-attack by a group out of North Korea that emptied about $1.2 billion out of end-user accounts in less than 16 hours. There were a few surprising things about the incident: one is how quickly it unfolded, two is that this threat actor group had been modeling and practicing this attack on other fintech and crypto companies for about a year, and three is that the security tool implemented across the environment was a commercially available consumer tool, not a highly sophisticated tool protecting these accounts or the Bybit environment.

00:07:52 Dario de Martino Got it. That's pretty chilling. And as a reminder, Bybit was a centralized organization, which is how the hackers were able to get in. But what happened to ransomware?

00:08:08 Anna Rudawski Ransomware is still the thing that takes up most of my time. We saw a slight dip in ransomware in 2024, but it is back with a vengeance in 2025. We're starting to get some numbers from our trusted partners, especially third-party ransomware negotiators, who are telling us they're getting a new case every single day. It's driven by the fact that it remains hugely profitable and the changing geopolitical landscape is creating a lot of opportunities for these threat actors.

00:08:46 Dario de Martino And how do our regulators respond? Is there a common playbook?

00:08:50 Anna Rudawski I wouldn't say there's a common playbook. Similar to privacy, there's been a state-by-state approach in the United States. We are definitely seeing a lot more anxiety over it. New York DFS has been leading the charge, being assertive about asking questions and investigating cyber incidents. They're even looking at applying their current tools and regulations to AI. The SEC was very aggressive pre-Trump on some cyber actions. Texas has also been active, using their existing privacy and consumer protection laws. Internationally, there's a lot of movement with NIST2 and other regulators. Law enforcement has been consistent in partnering with companies to address these issues, with the FBI having task forces dedicated to different ransomware groups and some

prosecutions coming out of US attorney's offices. However, many perpetrators are outside US jurisdiction, making it a real challenge.

00:10:21 Anna Rudawski But it is still a real challenge because so many of the individuals perpetrating ransomware crimes are outside the scope of US jurisdiction.

00:10:30 Dario de Martino Got it. All right, last question, lightning round. If I'm a fintech or digital asset GC, what's one thing I should do tomorrow? Helen, let's start with you.

00:10:41 Helen Christakos Two things. First, give priority to a state-by-state gap assessment if you haven't already done so. There are differences in those laws, and you may be subject to laws that you don't necessarily think you're subject to. Second, take a hard look at how you handle biometric and AI-driven data. There's a proliferation of laws being passed in these areas at the state level, and I think there will continue to be.

00:11:10 Dario de Martino Anna, over to you.

00:11:13 Anna Rudawski Yeah. What we've been saying is that your tools are not going to save you. You could have the best cyber tools, but if they're not implemented or governed correctly, they're not going to save you. We've seen this more in industries with a lot of money to spend on tools but lacking governance or implementation. So, make sure you have resources directed toward risk and where your biggest risks are. Don't just buy the best tool on the market because just signing up and buying a software license is not going to save you.

00:11:56 Dario de Martino Great advice. Helen, Anna, thank you both so much. That brings us to the end of today's episode. What I think we've heard today is that the convergence of privacy, cybersecurity, and AI is no longer abstract. It's really reshaping the fintech and digital assets landscape. The regulatory frameworks are fragmented, the threat actors are evolving, and the tools we use, whether for decisioning or defense, carry real legal and reputational risk. So, whether you're a startup or a market leader, now is the time to rethink how you govern data, deploy AI, and defend your systems. Again, many thanks to Helen and Anna for their insights and to all of you for listening. I hope you enjoyed this episode. If you'd like to learn more, be sure to visit www.aoshearman.com/en/industries/financial-institutions/fintech where you'll find all of our related content. Thank you again, and we'll see you next time.