**The Latest in GenAI: Updates on the Regulatory Landscape and Company Best Practices to Engage in Now**

**Hosted by: Katie Gardner**

Thank you for joining me everyone. As a quick preview. This is part of a series of webinars that we launched on AI. It is designed to be an update on new developments in the last quarter. So it doesn't recap in detail what's been covered in earlier presentations. So if you are interested in those. These are all recorded, and you can find them on Gunderson's website.

Here's an overview of some of the previous presentations that we've done

My name is Katie Gardner. I'm a partner in Gunderson. Strategic partnering and licensing practice. 90% of my practice involves counseling companies. It begins with, you know, founders at the seed stage all the way up to public company legal teams, and I advise on a range of issues relating to products and services with a focus on the technology sector, including negotiation of licensing deals, partnerships and strategic commercial deals in every space and unsurprisingly, I've spent a significant amount of time this year, advising companies on AI strategy and risk as well as advising investors in their investments into AI companies. The content of this presentation today summarizes the takeaways that I have from both closely watching these developments, and I also wanted to provide my insights on trends and predictions for the future as well as takeaways for what you can do now, especially as you know, a lot of information is unfolding.

I consolidate the updates into 4 areas. First, I'll cover updates to government regulation and enforcement. This will include, you know, the Congressional efforts to get themselves kind of up to speed and educated legislative proposals. There's been some action from the Ftc. As well as you know, industry participants that are embracing self-regulation. To some extent. Then I'll cover the copyright development which can largely be framed in the context of this rising tension between the industry of content creators and publishers on the one side and AI models. On the other side there have been strike petitions and new litigation filed.

I'll cover some new trends in deployment of AI models, and where we've seen a couple themes such as kind of open source versus proprietary models and enterprise, hesitation to adopt AI tools being responded to with more and more enterprise, safe tools, and then last, I will cover legal diligence and risk allocation in licensing deals, financing and acquisitions. And this area is Nathan. But I'll cover what's starting to emerge in those fields, and what we where we think things are going.

At a Federal level there have been several Congressional hearings held, and a few of them have been focused specifically on regulation and invited business leaders to testify. The CEO's of both and Open Ai and Anthropic testified making proposals for how Congress should think about regulation.

One of the suggestions included the establishment of a licensing agency before products go to market. I think this would be something similar to the FDA, and they would oversee compliance and safety standards and require independent audits. But this is very much evolving the same time, you know. Throughout the month of June we saw several new AI related bills proposed in Congress. The first one was No. Section 2 30 immunity AI act. And for anyone you know, with a Internet company, you know, understands very well how important this act is for their business. So this proposal would strip section 2, 30. Immunity for claims that are based on generative AI, which means that consumers could do AI models for damage from harmful content that's produced and given the unpredictability of the output right now. That certainly could open up a kind of big area of potential liability for companies.

Given that section 2, 30 is really responsible for the proliferation of the Internet as we know it. This is this is one we are. We are watching closely. Also introduced in June were 2 bills that were more focused on frameworks for regulating AI. The first was a National AI Commission Act Bill which proposes a Federal commission to study AI and potentially establish regulations.

It would kind of evaluate current AI oversight and establish a risk-based regulatory framework, and Senator Chuck Schumer also launched what he calls the safe innovation framework for AI, which was a framework for how Congress should think about developing future AI legislation and it outlined a number of principles on, you know, safeguarding national security and developing transparent systems, protecting IP, establishing a system for accountability and liability and he also announced that he's going to host a number of Congressional briefing series. I think the information gathering exercise that Congress started with these Congressional hearings on regulations is going to continue in in a number of different format parallel to these Congressional efforts to learn more from the industry and developing these proposals. The White House worked with directly, with companies to get voluntary. Assurances from the key players. The first, you know this AI agreement is what they're calling it, and several large tech companies pledged to commit to these safety security and trust standards and share, you know, information with each other and with the government to watermark content as AI generated and otherwise really just help kind of develop a system of kind, of combating a lot of the concerns that people have around these systems.

A few days later a subset of those parties for the AI agreement independently announced that they were launching an industry group called the Frontier Model Forum. Again to, you know, establish the safety issues and regulatory concerns, and they were going to develop a public library of solutions to support industry, best practices and they invite participation from, you know, other organizations that are developing foundational models, to join meanwhile at a State level throughout 2023. We see, you know, numerous State privacy laws that are modeled after the Ccpa. And that have been enacted, and nearly all of these include opt out rights for automatic decision making, which is the piece that really hits the most at the way that kind of AI can be can be implicated.

There was one new AI specific regulation called local law, 1, 44. That went effect in New York earlier in July, and this relates to the use of AI in the employment context and requires bias audits and notice in that context there are numerous other state proposals and bills pending. But for the most part on a state basis, we're operating under the privacy regulations and some AI specific bills. And in high-risk case environments. There's a few other and employment context insurance, you know, insurance context, financial decisions.

So those are the things to look out for. Last, there were some developments coming out of the Federal Trade Commission that are meaningful to AI. First, the Sec. Entered into 2 proposed orders or judgments. One was with Ring, which settled for some amount of money, and it was related to their failure to impose security restrictions on the use of certain data for the purpose of training algorithms, and another was against Amazon. Also, you know, a fine related to their use of children's data to train algorithms. The important thing to take away from these is in both of these cases into something such to delete these algorithms or models that are trained using this data that was collected in a noncompliant way. For any company that is, spending a lot of money to train proprietary models and understand how expensive it is to train models.

This could be, you know, materially impact.

The Sbc also open, invested open an investigation against Open Ai and asked for, you know, records and information on risks that they are seeing with respect to their models, and that is, that is another one. We were watching so themes and predictions on regulation, you know, at this point there is no overarching AI regulation like an analog to the EU AI act, and I don't think we should expect that for some time, if ever.

We should expect that us regulation will continue to focus, at least in the short term on high risk uses of technology. In certain contexts and employment insurance, this automated, you know, decision making.

There are questions about whether Federal regulation is the answer. The knowledge gap between AI developers and policymakers is broadly acknowledged, and they're concerned that the fast pace of development of AI doesn't allow the time that's required in our traditional legislative process.

And so we're also seeing more industry participation. So you know, the key players are really seem eager to participate in the process and cooperate with government and provide feedback.

And you know, agreed to these self imposed guidelines. Think we'll also see a lot of enforcement through State privacy regulation, and by the ftc, right now, kind of the laws that we that we mostly have in effect, that that are kind of impact use of AI bar, the State privacy laws, and the authority under the Fdc. To enforce unfair and deceptive trade practices a few key takeaways, you know, evaluate your use of AI. Understand the ways that you are using AI systems, what data you're using to collect or what data you're collecting to train models, the legal terms and policies that apply to third party systems and understand the risks that are associated with those uses, and make sure you're flagging any high risk uses such as you know uses for automatic decision making or employment for further legal review. You should also review your public statements.

What you're telling your users regarding or collecting you sharing and deletion of data and making sure it aligns with your practices. And for anyone you know who's building a foundational model, you know, consider self-regulating and adopting practices and policies that align with the statements and concerns of regulators, particularly around, you know, transparency and bias and accountability and privacy moving on to copyright.

There were a number of developments we last left off with the cases by, you know, Getty images against stability AI and the cases of relating to copilot and codecs. In June and July there were several new class actions filed against Open Ai, Meta and Google with claims relating to their use of, you know, Internet data for training. And we are many years away from the outcomes on those cases. But we can expect that the models that are defendants in those cases will be, you know, bringing that bringing kind of defenses on the grounds of fair use.

Meanwhile there have been, you know, numerous protests, so to speak, around the industry. In May Hollywood writers, writers announced the strike, in part over the use of AI to reproduce their content, and then the authors. Guild announced that more than 10,000 authors had signed a letter to leaders of generative AI companies asking for fair compensation in connection with the use of their copyrighted materials.

Recently Barry Diller announced that he was organizing a group of publishers to form a coalition to leave potential litigation efforts or press for legislative action against the use of website content for training purposes. We also saw New York Times just updated their terms of service to prohibit the use of their content. For AI training we saw Reddit shut down the free access to their Api and Twitter, or X, filed a petition for damages against a number of unknown entities for data scraping. So you have all this industry pressure kind of mounting on the one side and on the other side we see a few actions from the companies that are building these tools to try to mitigate risk. The Open Ai announces these licensing deals with Shutterstock and the associated press indicating that they are exploring. You know, legal avenues for high quality data. Google and Zoom. They both updated their policies recently, clarifying their right to use data for training, though, interestingly, there was a lot of backlash against Zoom. As recent as yesterday, they've been clearing the meaning of those updates.

And I'm going to talk about llama, too, on the next set of slides. But it's worth taking note that their open release did not disclose the source of training data, so that was likely a measure to limit liability. Given the lawsuits that are filed against them right now.

We should expect to see more lawsuits filed against companies that are that are scraping the Internet to train data as well as pushback from publishers and creators. Whether that's in the form of you know petitions or strikes, or technical blockers or legal restrictions. I think we'll also see those who do have high quality data finding avenues, more avenues to monetize it for training purposes. Whether that's licensing it to, you know. Llms, or developing their own, their own products internally link fair use will continue to be a subject of debate, though I think that much of the use of data for training does seem to align with precedent that would indicate a lot of it is transformative, fair use. So we'll have to see how that plays out. I think another interesting angle to follow here is international policy. Both Japan and Israel have come out doing that. Training models with Internet data likely is fair use that could influence some of the outcomes in these cases.

Some takeaways. If you are deploying products that are based or used. Third party lms to customers, make sure you're making appropriate disclaimers, particularly given the proliferation of litigation and the uncertainty around IP risk companies probably shouldn't expect to receive, you know, indemnity, coverage, or strong rents and warranties from those vendors, except in narrow circumstances. Also consider. You know, license use cases, not every use. Needs a large language model, and there are a lot more fine-tuned models. Coming out that are developed for specific use. Cases that are trained using license data, or, you know, mitigate a lot of the risks associated with Llms, and they offer more legal protection and also beware of prompts. User prompts that invite substantial similarity to another's work, so prompting a model to create images that are in the style of, for example, maybe something that's more likely to produce output that is substantially similar to an artist's original content. This is another reason why it's important to have internal policies guiding your employees on acceptable use of AI systems.

Last, do your diligence on the vendor fee using and their sources for data trading to the extent that it's available, as well as their, you know, methods for testing and validating. The big news in July on the technical front was Meta's release of Llama 2. This was released as source available, which means you can host it yourself, and it also permits commercial use which was different from their release of Llama, one which was only allowed for research purposes.

Most people are referring to it as open source. But there is actually a license agreement with some restrictions. So it's not technically open source. One of those restrictions is that permission is required. If your monthly active users exceed 700 million.

I think this essentially means that they're happy for companies to be very commercially successful using this. But they don't want, you know the likes of Google, or open a hiring of the large language models to be benefiting from it, and Meta has been a strong proponent for open models and the release of llama to intensify the debate between open versus closed models on the, you know, one side. You the kind of proponents of open models call out the transparency and the fact that people can go and look at the code, and it mitigates a lot of the risks and concerns. That people point to when they when they talk about large language models for companies themselves, they can host it themselves. They can fine tune it. The code can be kind of changed on them or taken away since they have it, and it's not being provided through an Api on the other side. You know there, there are people who are worried that the open approach makes models too easily accessible to bad actors, companies that have their proprietary models have, you know, continued to moderate them and try to prevent misuse or really harmful use. And that's something that can be done with an open, with an open model. And you know, proprietary models also, you know, continue to update them for security. So if there's, you know, prompt injection attack, they can. They can make changes to protect it again. Something that you know an open model would not would not be able to take advantage of.

We also, have seen this kind of continued enterprise. Caution. Some more announcements from companies that have shut down their employees, access to AI tools out of concerns around, you know, data leakage and trade secrets that started with the banks several months ago, and then Apple and Samsung followed. And I think you know, in part, in response this continued enterprise, caution.

The companies who are producing these tools have continued to make changes to facilitate enterprise, enterprise, adoption. So this started all the way back in March. When Open Ai updated its terms of service to state that they would not train models on input data. This does not include Chashd, but for enterprise companies paying for, you know, GPT. 3 and a half, or QPT. 4, you can get more comfort, at least on that front. These models can also be, you know, deployed securely, such as an anzure. There have been new enterprise tools announced and updates to terms again, to try to get companies more comfortable. Few examples. And you know, adobe announced that users of Firefly would be indemnified for IP infringement claims relating to the output. The copilot terms were also updated to clarify that they wouldn't use input for training and Microsoft released enterprise again, to give, you know, greater protection for businesses who wanted to leverage those tools.

I think we're going to continue to see discourse in this kind of open versus closed model debates. Large language models or other applications are going to continue to seek access to high quality data for use as training and to distinguish their products on the market.

Proprietary models will continue releasing new versions of tools to get enterprise companies comfortable around data security. And IP risk and other concerns. I think I think we'll also see more companies. Consider, you know, alternative options of hosting and training their own proprietary Lms and deploying them locally with source available models like Llama 2, a few takeaways. You know, weigh the costs and benefits of hosting your own model. Using llama to, or using a proprietary model that's hosted by third party and provided through an Api there are a lot of different factors depending on your specific use case and inputs that will that will impact that analysis. But there are more options available. At least make sure you're reviewing the licensing terms of the models and what they are doing with the input.

Also, you know, deploy internal AI policies and guidelines. Your employees have guardrails on how to use these tools. The last set. I just wanted to cover a little bit about what I'm seeing in the legal market. First in commercial deals. I mentioned that the Major, you know. Lms aren't offering much in the way of legal protections, but there are options of some new tools that may be appropriate in certain contexts. Otherwise, you know, disclaimers and pass through to customers are critical to limit liability. If you are using these in a customer facing manner, and in some context. I have seen some larger enterprise. Customers start to request from my clients robust commitments on your use of ethical AI. Frankly, that I think many of them are not prepared to commit to quite yet financing and acquisitions it's really still evolving where the line will be drawn on reps and warranties. But you should definitely be prepared for diligence. Some of what we're starting to see resembles, you know, open source diligence and requests for the specific tools you're using and how you're using them.

As well as you know, some reps that you know company it or proprietor information and source code has not been used as input into any of those tools for public companies. There has been a significant uptick in, you know, public company disclosure around AI risks. And I think this will continue.

We're actually working on a client alert right now, that's specific to this topic. You can stay tuned for that. Some trends, I think, as you know, large enterprise companies adopt AI tools. They'll gravitate towards these tools that are trying to provide the safety guarantees. They're looking for around, you know, IP risk security trust? I think technology's changing so quickly and the risks are changing that it may make it difficult for lawyers to align on what's appropriate for financing and acquisitions. Particularly, some of the first iterations of you know, reps and warranties that I saw proposed really seemed you know, over burdensome and kind of applied to what everyone was talking about 3 months ago. I think it's going to be, you know, tough for everyone to stay on top of what's realistic and what the risks are. That we should be kind of addressing in legal documents.

I think you should. If you're on a path to an acquisition, really expect the acquirer to do deep dives into the models you're using to build, build your products and the license terms that apply to them. And for public companies who are on the line definitely make sure you're bolstering disclosures around your use of AI depending on your deployments and the specific risks that are involved.

A few take ways, you know, update your end. User terms and services agreements, make sure you're thinking very carefully about which lms, you're deploying and how you're deploying them. And again, I you know, I'm repeating myself. But deploying internal AI policies and guidelines to make sure you have a buttoned up approach to adopting AI and understand what's being used and how it is being used.

And that is it. And I have amazingly made it through in less than 30 min. I love your feedback particularly, you know, on this presentation and any other content that would be useful to you. We also have a big announcement coming out tomorrow. It relates to gunners own technology initiatives in the space. Everyone who is dialed in today will receive the alert. Stay tuned.