TO ZERO
Co-creating a path to end childhood sexual violence

solutions insights lab

“Impunity has to be addressed”: Sean Litton of The Tech Coalition on regulations, collaborations and compliance in the tech industry.

Lissa Harris
July 25, 2024

Lissa Harris: If you could introduce yourself, your organization, and talk about the problem that you're addressing and how you are tackling it.

Sean Litton: I'm Sean Litton. I'm the president and CEO of The Tech Coalition. The Tech Coalition is an industry alliance of over 40 large, small and medium tech companies from around the world that have come together to fight and combat online child sexual exploitation and abuse. It's an industry association. So I work for industry, with industry, to help industry move the ball forward in this effort.

The Tech Coalition's unique in that it's the one place where companies can come together and collaborate with each other in a safe place where they can bring their greatest challenges and work them together. We leverage the power of our membership, particularly the larger companies, to help the medium and small companies. We're driving towards two primary goals. One is upleveling the capacity of our individual members in terms of technology, in terms of policy, in terms of operation and practice, and then identifying opportunities to uplevel industry as a whole. So through collaboration, find the synergies across platforms that will keep kids safe.

Lissa Harris: Who are your big players?

Sean Litton: We have everyone from Google, Microsoft, Apple, Meta, Amazon to medium-sized companies to internet service providers. We have AI [artificial intelligence] companies, we have dating companies. We have companies deep in the text stack like Cloudflare. X is a member. It's a broad variety of companies and a broad variety of sizes.

Our members come together in working groups to deal with issues like financial sextortion, age verification, investigations and reporting, supplemental reporting to name a few. With respect to generative AI, we've had several working groups because we have several companies that have generative AI models. So developing a common approach for risk assessment and mitigations. And then another working group looking downstream at the impact of generative AI and how to deal with it.

And then a third group that was looking at on a legal basis, how to respond to this material and how to safely test these models. So those are the kinds of things we do. We also facilitate engagement between industry and third party stakeholders—regulators, government, law enforcement, civil society, survivors. For example, last year we held a multi-stakeholder forum on financial sextortion of children. NCMEC was raising the alarm, and then we convened this gathering, about 200 people from around the world, to come together and drive to a common understanding of the problem and begin to share what people were learning and look for paths forward. And we'll have a follow-up to that later this year.

As a result of that, our members pulled together a working group. Most of our working groups will produce a member resource. So they get all their best thinking together. And now that resource is available to all the members. We also fund some research, and we also do our very best to keep our members updated on their compliance obligations globally. So regulatory and legislative developments.

Lissa Harris: And that is a very shifting landscape.

Sean Litton: Yeah. It's super dynamic. One of the primary concerns in the tech industry is compliance now, because there's a lot of different regulations coming from different directions. It's all new, whether it's the UK Online Safety Act, what's happening in Australia, what's been going on in Brussels, [or] different states within the United States. But I want to be really careful to say—we do not lobby. We are not an advocacy group. Our fundamental purpose is to help the companies collaborate and improve industry's response to online child sexual exploitation and abuse. So when we engage with government actors, we're simply doing it to facilitate engagement with the companies or to educate them on the current state of play in terms of what the coalition is doing. We don't represent industry to legislators, et cetera. So we're not a lobbying or advocacy organization.

Lissa Harris: What makes your approach distinct from other folks working in your space?

Sean Litton: The primary thing is that it's industry only. And it all happens under a non-disclosure [agreement], so we've managed to create a safe place where they can genuinely come together and collaborate, and it actually works. The organization was originally started in 2006 with NCMEC as the sponsor. And then it incorporated independently about five to 10 years after that, but remained a pretty informal coalition until around 2020 when we launched Project Protect. At that point the members began to put significant resources into it, which allowed the coalition to hire a staff. That's when I was hired. And the initial strategy was to drive the innovation and uptake of new technology, continue this information and knowledge sharing among the companies, which is really at the heart and soul of the TC. Facilitate collective action through multi-stakeholder engagement, fund research, and lastly, drive industry transparency on these issues.

Lissa Harris: Is there an example that illustrates the impact of the work that you do?

Sean Litton: There's several. One is, for some time people have been aware that bad actors work across multiple platforms, but the industry didn't have any safe and secure and responsible way to share signals about those bad actors. Each platform was operating independently and without knowledge of what was happening on other platforms, so we went to work on that at a relaunch at the beginning of 2001.

We developed a program called Lantern, which is a signal sharing initiative, and there's now 21 companies involved in that. Lantern allows companies, once they've detected a violation of their terms of service—their user agreement with respect to online child sexual exploitation and abuse—they take action according to their policies and report out as required by law. And then they can put signals into Lantern that other companies can ingest. Signals about the content perhaps, and signals about the bad actor that other companies can then ingest and conduct an independent investigation to determine whether that same material or that same actor is at work on their platform. And if so, whether it's violating any of their policies or terms of service, and then take action accordingly.

This is really important for things like, for example, grooming or financial sextortion, where the actor may contact the child on one platform, try to move them to another platform for purposes of communication, and then even a third platform to exchange imagery and maybe a fourth platform for some financial exchange. Or things like URLs, where in order to avoid detection individuals may advertise CSAM [child sexual abuse material], they may be selling CSAM, but they don't have any imagery. And so it may not be detected. But they have URLs. And the company that's hosting URLs may not know that they're actually hosting CSAM because they may not have scanned that. So [Lantern] allows companies to share these URLs. And it's been extraordinarily successful.

We finished a pilot and then launched this globally in November. Through the pilot phase and through last year, I think over 38,000 accounts [have been] disabled. Right now, we're all quite focused on financial sextortion due to the extraordinarily harmful impact it's had on young men in the United States and I believe globally. So it allows companies to share that information quickly and disrupt those bad actors' actions on other platforms. That's one thing I'm super proud of.

Another example is with generative AI, you have some of the largest AI platforms in the world coming together and developing a common risk assessment for child safety and discussing it in a safe and secure environment, and then working out how to mitigate those risks. That's incredible. That means that the organization that's the furthest ahead in the world gets to share their expertise with the others. They may be further ahead in different aspects, and so they can all share, but you've got some of the best child safety people in the world working with some of the best AI people in the world. And you've got companies doing this jointly. That to me is incredible and will prevent a lot of harm down the road that these companies were able to share that information and do it in a safe and secure place.

We won't be able to measure the impact of that because it's the things that won't happen, the CSAM that won't be produced, the children that won't be harmed, et cetera. But I am so proud of that, honestly, and the people that participated in it. There are many [examples] like that. There's genuine collaboration between the companies. But again, what sets us apart from everyone is we are industry only. There are a lot of coalitions around this, but this one, because it's industry only, because it works under a non-disclosure, it creates this environment where they're able to be more transparent about the challenges and share solutions and work problems together.

Lissa Harris: I'm really struck by how important it is at every level in this field for there to be places where people can speak in what they feel is a safe environment, whether you're talking to survivors or community members or the biggest, most powerful companies in the world.

Sean Litton: Yeah. Let's say you're a brand new AI startup. It would be unlikely that you have child safety experts on your team, but by coming into this conversation, you get access to some of the best child safety experts in the world who have already thought through all the risks relating to generative AI, and then you can build that into your model.

Wellness and resilience is a big issue in the space. So companies also work together and share on that. And then we bring in external resources and experts as well. One of the things we're continually doing is bringing people in from the outside: people with threat intelligence, or NCMEC so that our members understand the trends that they're seeing. But absolutely, wellness and resilience is a big, big challenge in this space.

Lissa Harris: Sometimes we learn as much from things that don't work as things that. Do you have an example of something that didn't work that you tried, that you learned something from?

Sean Litton: We haven't been going that long, and so I don't yet have a great example. I'll just say this, and I'm going to say it in a positive way. You get a much more transparent conversation when you have industry only in the room. When you bring in other parties, you can still have the conversation, but people become more guarded. And there's a lot of reasons for that. So if you genuinely want collaboration, the one thing I've learned is you need to make sure that people feel safe and that the information they're sharing is secure. But at the same point, we have had some really great conversations with external stakeholders. So I really don't have a great example yet, but I hope to have one, because if you're not failing at things, you're probably not swinging hard enough.

The first step is to prevent the bad thing from happening. For example, we've had working groups on Safety by Design. How do we design our products in a way that reduces the potential for harm? The next step is to detect anyone seeking to harm, or any bad imagery, etc. Then to report it, to disrupt it, to action it and enforce your policies. But all these reports are going out to NCMEC, and the numbers keep growing into the millions. My biggest concern is, what's the capacity downstream to absorb that level of reporting? So I worry about the emphasis on more detection from industry, which in some cases I'm in favor of. We want more reporting, but what will we do with that if currently we don't have enough capacity to handle the current level of reporting? So what I don't think works is just looking at one part of the problem. We have to look at the whole pipeline.

I work for industry, so that may sound like I'm trying to defend industry. That's actually not my job. My job is to build their capacity. And there's plenty of work to do there, and I'm proud to be working with them and doing it. But ultimately, if there is no accountability for the bad actors, if they operate with impunity, industry is just always on the defensive, on the reactive side of things. And there needs to be some restraint out there. The power and the force of the state has to be brought to bear to restrain bad actors and create some form of deterrent. Especially for economically motivated crimes, perpetrators are going to be much more sensitive to enforcement. So I think there needs to be a look at the full pipeline. And from what I hear from law enforcement, they're overwhelmed by the volume.

Lissa Harris: Aside from funding, what are the big challenges that you have still not yet solved that you are working to overcome?

Sean Litton: One of the challenges in this space is there are a multitude of online platforms and there's new ones every day. So let's say you get a hundred of them together who are responsible and are working diligently to ensure their platforms are safe, to ensure there's no CSAM on their platform and ensure their users are safe. But even if you have a hundred, there's thousands of others. And some of those operate outside the context of regulation. So bad actors proliferate on those platforms. Regulators tend to focus on the larger platforms where most of their citizens are. And I understand that, and that makes sense. Those platforms understand that as well, and they're working hard to comply with those regulations. But there's a large swath of the internet that I don't think regulators can reach.

One of the things I'm encouraged about is AI. A lot of people talk about the risks of AI, and I'm aware of those, particularly generative AI on the issues that we work on. But there is a real potential for AI to begin to replace a lot of the tooling that we're currently using and a lot of the human review that's necessary for content moderation. I'd love to think we're six months away; it may be two to three years away. But because of the nuance and the context that AI can do, and once it's stood up, it's much easier to train than machine learning. It would spare the reviewers the trauma of having to look at this difficult imagery. It could even perhaps do a better job because it doesn't get tired and it can remember all the different rules and classifications perfectly. So potentially that could be a game changer to deploy that.

But we have to think about how to do that responsibly and in a way that protects people's privacy. Those rights can be in tension, and we have to ensure there's proper balancing of those rights. But I see for places where there is high risk to children and there's a strong business interest, for example, in ensuring there's not CSAM published on your platform in any form, I can see a future where there are AI tools, large language models that are multimodal and that are working as agents for content moderation. And there's a lot of people working on that right now, but I think we still have a ways to go.

Lissa Harris: Is it at all a part of the work that you do to shift the cultural norms or shift society's view of problems?

Sean Litton: For us, not so much really. Because [we are] not an advocacy organization. Industry is well aware of the challenges they face; that's why they join, and that's why they contribute and show up and participate. There are other organizations that we're friendly with and partner with, like Thorn or NCMEC, who are much more out there educating, advocating, raising awareness. We're working on the problem with companies. The one place where we would ever seek to change attitudes would be within industry, if there are pockets of industry that have not yet realized the potential harm and challenge of these issues, to ensure that they’re aware of it. But it'd be pretty hard not to be aware of it at this point. So I don't find that to be a challenge, really.

I would say the biggest attitude that we're challenging is that collaboration is inefficient and a waste of time. And it doesn't actually produce tangible outcomes. And it's talk, talk and no output. So we are focused on driving tangible outcomes and demonstrating that to both external parties who are cynical and internal. There's lots of companies that are like, "Look, we don't want to join another round table." That would be the biggest attitude we're trying to change.

Lissa Harris: How do you cultivate and maintain partnerships so that you can be effective in this work?

Sean Litton: The fundamental thing is you have to be a trusted partner. You've got to maintain trust and build relationships and serve people really well and provide value. So you've got to understand their agenda, and where their agenda overlaps with the agenda of the coalition, and drive that. In our case, these companies have a strong business interest in ensuring their platforms are safe, that children aren't harmed on their platforms, and that their platforms do not become havens for CSAM or criminal activity. So our interests are aligned, and we provide services that help them do that, and we provide partnership that they can leverage to do better. The other partnerships that are very important to us are with external organizations like

WeProtect Global Alliance, Safe Online, NCMEC. We're grateful for those partnerships and those organizations. We learned from them, and we try to align as best we can with the direction so that we're all moving in the same direction.

They sometimes overlap with us in terms of who they're working with. WeProtect has everyone in the world in it, but we just have the industry part. And that's just one part of WeProtect. Safe Online deals with a lot of people. NCMEC is a global clearinghouse for reporting. They have a ton of information. They're great partners.

Lissa Harris: What do you think are some of the insights that could be drawn from your work that other people working on this problem could use?

Sean Litton: Primarily, industry's a key player, in the online space at least. That's one. Number two, impunity has to be addressed at some level. Unless impunity is addressed, it makes keeping children safe much more difficult.

One other insight, which is related to the first two: This is not a problem that any one sector can solve alone. It's not something industry can solve alone or that law enforcement can solve alone or that civil society can solve alone. We actually need to cooperate and work together because we need educators, we need schools, we need parents. We need law enforcement. We need really great care for survivors. We need survivors to have a voice in how we approach these issues.

But no one party can solve this problem alone. So we need to work together. And there needs to be magnanimity. One of the challenges, both when I worked in this space previously in the non-digital form and working in the digital form is it's very easy to blame the other for the problem and put the responsibility on them to solve it. And we can't deny our responsibility, whatever it may be, but at the same point, it's more helpful to jointly move forward.

Lissa Harris: What do you think has a potential to make a significant impact on this field and this problem in the next five years?

Sean Litton: I think AI. And I don't mean that in general terms. I mean it in the way that I was talking about before, in terms of its ability to look at context, look at all the data and make judgments. I think AI could be a game changer. I also think if we figure out how to more effectively and efficiently respond to the individuals that are perpetrating the abuse, I do think that will have an impact as well. I hope that there is more investment. And I want to be really clear. I think the people at the tip of the spear, the boots on the ground law enforcement are doing a fantastic job. I just think they need to be resourced better.

Lissa Harris: You talked a bit about differences of sentiment in the business community and the tech community about how much it is their problem. What do you think it takes to get businesses in the industry on board with feeling responsible for working on this issue for those that are not yet there?

Sean Litton: I think the most important approach with any business is to [ask], “What's the business case?” There's a strong business case to be made for ensuring your platform doesn't become a haven for criminals and child sexual abuse material. That will drive away all your users, it will drive away your advertisers, and it will create all kinds of problems for your platform if you don't take basic precautions.

I think it's also helpful to humanize what those challenges are, because we're all humans at the end of the day. And I think stories are also important and can move people, even CEOs and presidents. But I think we can't just rely on the story or the moral arguments. I think those are important, and they appeal to every human, but business leaders have a responsibility to their shareholders and to their business, and they need to justify why they're taking the decisions that they're making. So we need to build a strong business case for why this is important. And I think that's not that hard to do.

Lissa Harris: Related to that, what would be helpful and useful to businesses in the industry to try to move the needle on this problem? Besides the work that you're doing, are there other things you can point to that needs to happen in order for the tech industry to be successful at combating this problem?

Sean Litton: Clarity of regulation and consistency of regulation. As governments are stepping into the space to regulate industry, if they have conflicting requirements or disparate requirements, it creates inefficiencies, it creates a resource burden. And those resources could be used much more effectively and efficiently if the regulatory scheme was clear and consistent across national boundaries. Because these are global platforms, they have to comply in all the different jurisdictions. So that would be super helpful. And for medium and small companies, clarity and simplicity. Because a lot of the medium and small companies do not have lawyers in house. And if you look at the draft codes that are put out, it'll take several days for a lawyer to wade through some of those, so a small and medium company may never get to it.

Lissa Harris: Is legal also something that you help your smaller members with?

Sean Litton: We certainly do. We don't provide any legal counsel, but we provide summaries and access on regulatory developments and regulatory schemes. Because the first question is, who does it apply to and what are the requirements? And they can be different for different size organizations. But they're still going to need to do a lot of follow up on their own.

Lissa Harris: Is there anything that we didn't get to that you think is important to add?

Sean Litton: The only thing I'll say is I'm very encouraged. I had my doubts about whether the industry was serious about dealing with these issues, and I've been very encouraged to see the level of commitment within the companies that I'm working with to ensure that their platforms are safe. They all draw different lines about how they approach the issue and how they balance the interest, particularly the interest of privacy versus detectionBut a lot of that is related to the risk. So the greater the risk, the greater the intrusion, perhaps. But I've been very encouraged. It doesn't mean that there's still not work to be done, but I don't know of a single company that's standing still on this stuff. They're all at different places, and the challenges are evolving, and they're trying to grapple with it.

Lissa Harris: Excellent. Well, thank you so much. Thanks for your time.

Lissa Harris is a freelance reporter, science writer (MIT '08), and former local news entrepreneur based in upstate New York. She is currently working as a consultant on capacity-building and local solutions-oriented community projects in the rural Catskills.

***This conversation has been edited and condensed.*