Reema Moussa 0:00
Hello everyone and welcome back to the Tech Policy Grind podcast. I am your host, Reema Moussa, and I'm joined by the lovely Lama Mohammed as we first dive into the news, and then turn it over to the core of today's episode, which is a recap of CYBER CON, which is the Foundry's first ever virtual cybersecurity awareness event in celebration of Cybersecurity Awareness Month, which is the month of October. So hey Lama, what's new?

Lama Mohammed 0:39
What's new is I'm learning how to use Mastodon because everyone thinks that as a 20 year old, I know everything and all things social media, even though I'm only exclusively on Tumblr. So that's been that's been the week for me. What about you?

Reema Moussa 1:00
Yeah, I am in travel recovery mode. It's been a long semester of a lot of travel to different conferences, which has been a ton of fun. It's been great to meet so many people in the privacy and cybersecurity space in particular. But last week, I had the pleasure of going to Washington, DC for the Privacy and Security Forum hosted at George Washington University by Professor Daniel Solove and Professor Paul Schwartz. So that's what my past few days have looked like. And now I'm settling back into LA and on the study grind.

Unknown Speaker 1:52
[Laughter]

Lama Mohammed 1:52
I don't know how you do it.

Unknown Speaker 1:53
[Laughter]

Reema Moussa 1:55
We do it, we do it we make it work.

Lama Mohammed 1:59
For sure, for sure. All right, so let's talk about the news. Before we dive in, once again, the full disclaimer that the opinions discussed on this news segment do not reflect the institutions, organizations and companies that we are affiliated or work with. We are just two young women figuring out the mayhem of the tech policy world. So Reema let's get into it.

Reema Moussa 2:27
Yeehaw.

Lama Mohammed 2:31
What's top of mind for this week?

Reema Moussa 2:34
The FTC, as always.

Unknown Speaker 2:38
[Laughter[

Reema Moussa 2:38
As always these days. So the FTC recently brought an action against Chegg, which is an educational tech provider, well known for providing resources to students on specific assignments for their professors and whatnot. And Chegg has come under fire from the FTC for lax data security practices that have led to four separate breaches now. And the FTC has proposed settlement order would require the company to bolster its cybersecurity practices, and implement data minimization policies, as well as offer multi factor authentication to users for account security, as well as allowing users to access their data and delete it.

Lama Mohammed 3:38
Right on, and I think it's interesting, because, and I would say, it could be a little bit more worrying than how most companies go about their data practices. But according to the FTC, Chegg didn't have a written security policy until January 2021. And sort of failed to provide sufficient security training details for their employees to sort of identify phishing attacks. And that sort of led or could sort of lead to, you know, the compromise of data being leaked regarding social security numbers of both their employees and students. And, you know, just some of these more basic cybersecurity practices we weren't seeing, which is a little worrying given, you know, we're in 2022 and some of these basic ideas of multi factor authentication, that using the same password or training employees to recognize phishing attacks is sort of almost old news.

Reema Moussa 3:38
Yeah, and you bring up two really interesting points that were actually a big part of the conversation at the Privacy and Security Forum that happened last week. And the notion that (A) the FTC is is focusing in on sensitive information, vulnerable communities and populations is really interesting, an interesting pattern to see across the different cases that the FTC is examining. But it's also interesting to see that the FTC is really going after the most abusive, or the most extreme cases of data security and privacy violations. You know, Chegg has been breached four times, at this point. A lot of the other cases that the FTC is looking at, and this was mentioned, time and time again, at the conference, they're really kind of just trying to get these companies to do the basics as far as cybersecurity and privacy best practices. So it will be interesting to see, as time goes on, if the FTC continues to look at those companies who are doing far less than the minimum, or if they will start to get

a little bit more aggressive and progressive in the types of companies that they're looking at, that might be violative, of other laws that have much more, you know, substantial obligations. So that's one thing to watch.

Lama Mohammed 6:43
It's definitely something to watch. And definitely, we'll be watching to see if this will set a precedent for the rest of the ad tech industry.

Reema Moussa 6:53
Well, that brings in the notion of what kids are using these days, and feels like TikTok is a huge part of that conversation. So what's going on in the world of TikTok and kids privacy?

Lama Mohammed 7:13
So as a fake Gen-Zer I am not on TikTok, I refuse to be on TikTok.

Unknown Speaker 7:19
[Laughter]

Lama Mohammed 7:21
But I know many of my siblings, friends are on it. And it's a very popular app among the Gen Z community. And I won't lie, some of the videos to sort of mobilize get out the vote have been really have been pretty influential. So that is not to discredit the the influence and great use of Tik Tok for sort of our generation. But I digress. So this week, members of the US House Representatives issued letters to Apple and Google questioning their policies regarding TikTok, and other apps that could pose privacy threats. The House of Representatives sent a letter to the Google CEO and Apple CEO sort of questioning if there is sort of a fine line for how apps may or may not be taken off the Google Play Store App Stores respectively, if they sort of crossed the line of putting Americans at risk to foreign surveillance, especially adversarial actors like China. And so what I found really interesting about this letter is that it references research, by a security expert by the name of Felix Krause, who I may have totally butchered his last name. But I thought this was especially interesting because they bring up the use of potential keystroke logging within the TikTok app. And for those who don't know, what keystroke logging is, it is a sort of new form of such as it is a new form of a cyber threat. And essentially, hackers can take your keystroke logs from when you type on your keyboard, and sort of decipher your password, any sort of any other information that's entered onto the keyboard. And that may mean that cybercriminals can figure out your PIN, your account number, your login information for financial gaming, or online shopping accounts, and you know, even your personal social media. So what does this mean for 2023? What are your thoughts? Reema?

Reema Moussa 9:29
It's going to be fascinating to see how policy around TikTok from the US perspective emerges in a hot topic in the headlines lately, as far as what sort of data TikTok is collecting, where is that data stored? Who has access to it?

Lama Mohammed 9:53
TBD and we may see how this case might also influenced by bipartisan bills to come in the next Congress specifically aimed to protect the privacy and online safety of young users, especially because that was sort of a big deal at the beginning of the year. It sort of died down now. But I'd be curious to see what changes in the next year.

Reema Moussa 10:15
Absolutely. So before we wrap up our little session on the news and get to the bulk of today's episode, let's talk about data scraping. So LinkedIn v. HiQ is a case that has been ongoing for quite a while now. But the news out of these past couple of weeks is that LinkedIn got sort of a semi-win in the case so far, as far as getting a partial win from US District Judge Edward Chen, from an October 27 order that ruled that HiQ actually breached its, breached LinkedIn's user agreement by directing its HiQ's contractors to create fake accounts in order to scrape data from LinkedIn. But still to be decided is whether LinkedIn waived its right to enforce its user agreement, since HiQ did openly discuss its business model and reliance on data scraping from LinkedIn at industry events that were attended by LinkedIn executives. This is according to a great article on Law 360 from Piper Hudspeth Blackburn, we'll have it linked in the show notes. But really interesting case, a lot of fascinating implications for data scraping as a practice as a practice that many business models rely on. And also will be interesting to see the implications as far as interpretation of the Computer Fraud and Abuse Act, which is sort of poised as the predominant U.S. anti hacking law. It will be fascinating to see how this turns out. We will wait and see with an upcoming trial on the breach of contract claim that is supposed to begin on February 27 of 2023. So, couple more months of this to go, possibly more depending on how long this gets dragged out. Well, thanks Lama as always for chatting about the news. And now we'll turn it over to today's episode, which you're also involved in Lama, in which we chat with our colleagues from the Foundry. Allyson McReynolds and Grant Versfeld on our recent event, CYBER CON, which was the Foundry's first ever virtual cybersecurity summit in celebration of Cybersecurity Awareness Month, which was the month of October.

All righty, I'm here with Allyson McReynolds, Lama Mohammed and Grant Versfeld. Welcome back to the show, guys.

Lama Mohammed 13:52
Thanks for having us. Excited to be here.

Allyson McReynolds 13:56
Hi, everyone.

Grant Versfeld 13:59
Hi there. Thanks for having us.

Reema Moussa 14:02
Whoo. So we're gonna talk about CYBER CON today, which was the first ever half day cybersecurity summit that the Foundry has done. And it was a ton of fun to collaborate with you all on this event, but I figured it would be great for our listeners to hear a little bit about what went on and some highlights before they perhaps decide to check out the recording of the event itself. So just going to jump into it. Allyson starting with you, you kicked off cyber con with a threat intelligence briefing featuring two of our very own fellows, Rikki George and Sasha Hondagneu-Messner, as well as Amy Dsouza of Southwest Airlines and the Women in Cybersecurity Privacy, Law and Policy. affiliate. So what were some highlights of the conversation?

Allyson McReynolds 15:05
Yeah, so we had three really great panelists. And they all talked about different things, but they were all connected in one way or another. So first, we heard from Rikki, she touched on how a lot of businesses are interconnected through the supply chain and rely on other small and medium sized businesses to function.

Rikki George 15:23
When you think about supply chain, you know, all of these organizations, the ones I've worked for, and currently work, for included, have a lot of interconnections with third parties. And those third parties are really a good way into the organization, right? Security has always looked at and has consistently looked at the front door and protecting, you know, the front and back doors, but the side windows that are the supply chain, networks that we interact with are a key vulnerability for us. And a lot of organizations rely on similar small and medium sized businesses in order to conduct business. And so I think it's really important for us to understand, you know, what are these smaller organizations that are supporting whole industries, like the financial sector, or the US government or have a global footprint? If you think about SolarWinds, which of course was, you know, big news in the cybersecurity space a little while ago, a lot of organizations across government and the private sector were using their software. So software supply chain compromise was a valuable opportunity for adversaries to infiltrate organizations across the world. And I think we're gonna see more of that going forward, especially as adversaries get more adept at understanding all the smaller organizations that support the larger critical infrastructure, not only here in the United States, but also overseas as well.

Allyson McReynolds 16:42

So the smaller organizations that support large sectors and the government can end up having a global impact if their systems are not secure and adversaries can target them to infiltrate their larger business partners or areas of critical infrastructure. Sasha spoke more specifically on public disclosure of security incidents, specifically, the SEC's proposed rules on mandatory disclosure of cyber incidents.

Sasha Hondagneu-Messner 17:10
The issue is that, as proposed, the notice requirement does not include an exemption for active investigations by law enforcement, coordination with intelligence or national security, or compliance with court orders that may restrict the timing of such disclosure. The SEC does acknowledge the importance of such reporting and such disclosure and and they acknowledge cooperation with law enforcement have asked questions about it. But as drafted, it currently doesn't have that. So publicly disclosed information that law enforcement could use an investigation, it could cause unintended consequences, such as revealing sensitive information which a threat actor could use. The second issue a lot of folks have have spoken about is that the public comments haven't really focused and don't provide an exemption for disclosure were premature disclosure of an incident could cause significant damage to vulnerable businesses or government entities, such as supply chains. So this could go against that principle of responsible disclosure. Responsible disclosure entails basically holding off public disclosure until the parties have been given sufficient time to patch or remediate the vulnerability or issue. This is especially important, a company discovers that its been impacted by a zero day vulnerability may be in an widely used software or something that could affect the supply chain. If such a company is required by the SEC to publicly report an incident before allowing sufficient time to patch, other companies could be caught unprepared. While bad actors could exploit the vulnerability they can exploit the vulnerability across that company and many other companies. So victims of cybersecurity incidents and breaches they should really be allowed to focus on mitigating the incident without the additional pressure of prematurely reporting an incident or exposing themselves to additional risk prior to fully remediating the vulnerability.

Allyson McReynolds 19:06
His remarks emphasize the need to develop disclosure regulations that really strike the balance between informing the public and regulators without jeopardizing a company's ability to mitigate the damage or patch their systems or work with law enforcement to assess threats. And then lastly, Amy highlighted how the motivations of threat actors targeting critical infrastructure are very different from the actors targeting consumer data, the financial sector, those breaches that we hear about all the time in the news. She also talked about the move toward combining operational technology with information technology, which will help businesses work better but also creates these

opportunities for cyber threats targeting critical infrastructure. So entities that are combining their operational and information technologies will have to synchronize their cyber strategies when managing both.

Amy Dsouza 20:00
Until now, you know, in like the supply chain plant or, or an airport or an energy power plant, the operational technology was kept quite isolated from, you know, information technology. So to in order to access anything in the operational space like at the airport or at the energy plant, you need to be physically there and then get access to the systems. On the other hand, an information technology employees can work from home, they can access that information from any devices and larges cases there's you know, bring your own device as well. So now that there is a lot of push towards that convergence of operational technology and information technology for this, it's there all great boxes, it's for better digital transformation for better productivity, to get that real time data to make better decisions. But it will open a lot of floodgates. So if you see most of the attacks that data related attacks are either phishing emails that an employee has clicked on a malicious link, or compromised login details, most of them 80% of time, it's that is the reason. Now imagine a case that an employee has clicked on a malicious link that shuts down an entire plant, the convergence of information technology and operations, technology could bring those kinds of risks to all of the critical infrastructure.

Reema Moussa 21:44
So lots of different topics discussed. Thank you so much for that overview between all these industries that the panelists covered what stood out to you as sort of a unifying theme between all other briefings?

Allyson McReynolds 22:02
I think Rikki really summed it up nicely at the end of her remarks. She said that cyber threats are busy, and addressing them will require a partnership among various stakeholders. All three of our panelists really emphasized the need for public-private partnerships, and that those will be key in responding to, mediating, and preventing attacks.

Reema Moussa 22:26
Thanks Allyson. Grant, you hosted the next session with Josephine Wolf of the Fletcher School at Tufts University. Want to give us an overview of how that discussion went?

Grant Versfeld 22:40
Absolutely. Josephine spoke with me about her new book called Cyber Insurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches and Cyber Attacks. In our discussion, she detailed the history and evolution of the cyber risk insurance

industry. And she also explained some of the limitations that large organizations face when seeking insurance against cyber risk. And also, we delved into some of the drawbacks of the various approaches that both insurers and organizations have when thinking about current cyber insurance policies.

Reema Moussa 23:17
That's really interesting. What are some of the main challenges that organizations face when thinking about cyber insurance?

Grant Versfeld 23:27
The core challenges that came up during our discussion that Josephine identified regarded the frequency of cyber incidents when compared to other types of catastrophes. So think about things like floods, car accidents, someone breaking into your home or business events like that.

Josephine Wolf 23:45
And so when people start thinking about data breaches, and cyber attacks, and ransomware, and all these kinds of things as a form of expensive risk, one of the questions that kind of naturally comes up is what can we deal with this the same way we deal with other types of risks.

Grant Versfeld 24:02
Also, cyber incidents can be unique because of the scale of harm that they can potentially have, both in terms of how many people are affected by the incident, but also how many people are affected outside of just one organization or area.

Josephine Wolf 24:16
That's the place where there's kind of the most pressure on policymakers and governments right now. Because what you're scared of or what insureres are scared of there is just kind of the scale of damage. How do we pay for a cyber attack that takes out the entire electric grid, a cyber attack that sort of shuts down so many companies and has such extraordinary costs? That there's no way to kind of do that and not go bankrupt.

Reema Moussa 24:50
Are there any takeaways that come to mind when thinking about the future of cyber insurance?

Grant Versfeld 24:56
Yes, particularly around the way that we gather data that relates to events that lead to cyber insurance claims. Josephine talked about how a lot of insurers are currently trying to figure out how they can build metrics to create a consensus about what defines the threshold of an incident covered under cyber insurance.

Josephine Wolf 25:16
I think for cybersecurity, there were kind of a couple pieces that people, myself included, have felt have been missing for a long time. And one is the empirical data about which of the various security consulting countermeasures we have are most effective, right. So if you think about sort of fire insurance, car insurance, we have pretty good consensus on like, here are the things you need to do for car safety, here are the things you need to do for fire safety. We don't we don't have as much of that around cybersecurity.

Grant Versfeld 25:46
We were talking about the NotPetya case, which was a major ransomware attack that had pretty significant implications for the ransomware industry.

Josephine Wolf 25:53
I think one of the reasons that the insurers decide to challenge the NotPetya claims, is they feel they have really solid attribution there. And the reason they feel that is because there are, you know, a dozen different governments in February of 2018, including the United States, but many others as well that kind of come out and make formal statements saying the Russian military was behind NotPetya. And so I think the insurance looked at that. And they were like, Okay, well, at least we're not going to have to fight the the attribution battle here, because we have more evidence that this was a nation state than we have for you know, any other cyber attack in the world.

Grant Versfeld 26:27
Josephine's remarks are particularly interesting on that regard. Because recently, since our discussion, on November 4, there was a major breakthrough in that case. And it was found that the organizations who were trying to claim against the cyber insurance would be allowed to make those claims, even with the act of war exclusions that normally exist on cyber insurance policies. So we still have a bit more of appeals to go in that case. But her remarks came at a very good time for the future of the cyber insurance industry, and the way that we think about how these attacks matter.

Reema Moussa 27:04
That's fascinating. Thank you so much for diving into that Grant.

Grant Versfeld 27:09
Absolutely.

Reema Moussa 27:10
Now switching gears, our next session was cyber hygiene for the legal profession with Kassi Burns, who is a senior ediscovery attorney at King and Spalding, as well as a board member for the Women in Cybersecurity Privacy Law and Policy Affiliate. And she gave some really interesting takeaways on the importance of cybersecurity best

practices for not just cybersecurity attorneys, but really every attorney.

Kassi Burns 27:44
You may have attorneys that have been practicing for a long time that don't even think about the fact of if I'm sending my client's data, it's not my data, it's my client's data, I should make sure it's password protected, or I should make sure it's encrypted. Or maybe I shouldn't send it in email, or maybe I should send it in FTP. Really, I think what we can encourage, you know, as people in the cybersecurity space is you know, creating those mechanisms of education with our peers. We're not just talking about, you know, the client's PII out there, we're also talking about, like, how we're engaging with our clients, how we're engaging with each other, how we're engaging on our own devices. Those are all really important things.

Reema Moussa 28:25
And last but not least, our session closed out with a discussion with Eva Galperin of the Electronic Frontier Foundation, and Siena Anstis of Citizen Lab. Lama you did a great job hosting this session, which really bridged the intersections of domestic violence and cybersecurity awareness. And the month of October happens to be a month of awareness for both subjects. So what was your vision behind the discussion?

Lama Mohammed 28:55
Yeah, of course, thank you so much. So when people think of cybersecurity, they tend to envision a hacker in a black hoodie or a video scrolling through lines upon lines of green code. But this is a very terrible trope and quite inaccurate presentation of cybersecurity as both a field and profession. Cybersecurity unfortunately now has evolved into something that has real physical consequences, impacting 1000s of people outside of just stealing money and preventing access to a computer. Scarily malicious actors have become so sophisticated in how they execute threats that a cyber attack now has the ability to bring real physical harm. Whether that is through a ransomware attack on a hospital and a critical patient misses an important procedure because their file was deleted, or an activist's life is in real danger because they're being watched, tracked and followed their laptop or phone via spyware without even realizing that the spyware is on their device.

Siena Anstis 29:52
So spyware is a form of malware so malicious software, that when installed on your device gives the operator full access to anything on the targeted device, some people call it a spy in your pocket. So this includes access to the contents of applications that use end to end encryption like Signal or WhatsApp, because the operator is viewing messages sitting decrypted on your phone, the ability to activate the

microphone and camera on your phone access and potentially modify or add files on your device access things you've jotted down a notes, full access, it allows the operator to track your location and it may in some cases allow the operator to access and send and post messages for example, from your from your cloud accounts, giving them the power to potentially impersonate you. So it's quite a wide, wide ranging set of capabilities. The installation of spyware in the targeted device can take place through three different means I'm sure people are curious like how this works. I'm not a tech, I'm not technologists or computer scientists so I'll give you the very basics. One click exploits are where the targeted victim has to actually click or the targeted individual has to actually click on a malicious link or open a malicious file to start the spyware to download to their device. So these links tend to be socially engineered to tempt the target to click on them. For example, if you were to send me an invite to this conference on my phone, perhaps I would be tempted to click on it. Zero click exploits are where the targeted victim doesn't have to do anything for the spyware to be installed in their phone at all. So in other words, you don't receive a suspicious link or message and click on it the spyware is just silently remotely installed from anywhere around the world in your phone. And we've had the Citizen Lab, researchers have seen increasing cases of this type of installation method. And then a third option is manual installation. So for example, you were stopped at the border, they took your phone for a bit came back that might be an opportunity to install spyware

Eva Galperin 31:46
Stalkerware is the entire class of applications that are sold commercially, and are meant to be covertly installed on the device, so tablet, computer, or phone in order to exfiltrate that data to a to a third party. And often this, this kind of software is is very easy to find, and it is sold as a way of you know, track your your to your teenager or your cheating spouse or something along those lines. And it essentially is a fine way of enabling stalking.

Lama Mohammed 32:33
So really being able to mitigate these harms is what makes cybersecurity such an important profession. And truly, in my opinion, a public service, particularly for vulnerable populations, such as you know, tribal groups, local government, nonprofits, low income communities, the LGBT community, the privacy of black activists, and the like. This notion was truly my inspiration for my CYBER CON session with Siena and Eva, especially because they've worked with victims of spyware and stalkerware.

Eva Galperin 33:07
The sort of blind spots that that the cybersecurity professionals that the information security community has to domestic abuse as a as a threat model, they often don't think of the abuser from as coming from inside of the home. This is often something that you will also see

with spyware meant to spy on children. And with the setup of sort of home based automation and Internet of Things devices. The assumption is that if you live with someone that they're spying on you is fine that it is fully consensual that they should totally know what you're doing. And your trust in this person is is never going to change you're never going to need to lock them out. They're never going to keep their you know their logins long after the they should have gone and this is a very big problem that we see over and over again. And it's not just limited to stalkerware. Stalkerware gets brought up in the context of of domestic abuse the most often because it is so powerful and scary and it feels like there are no defenses against it. But the most common sort of abuse that I see in, in these relationships is is almost always account compromise. I if if there is something with a login, I have seen it compromised.

Lama Mohammed 34:44
Cybersecurity is also a very interdisciplinary field. It touches on everything from business's best practices to social justice, and it's really important that we work to change these misconceptions of cybersecurity through conventions like CYBER CON and I was really happy and actually very honored to have been part of that change through our keynote address.

Reema Moussa 35:07
Thanks, Lama. And yeah, it was a fascinating session. And I think especially the intersection of domestic violence and cyber security as sort of the real life implications of this work that we're doing in the tech policy space, it's so important. So thank you so much. Well, team, it was great collaborating with you all on our first ever CYBER CON. And if you're listening, be sure to check it out. The recording is available on the Foundry's LinkedIn page, as well as YouTube.

Lama Mohammed 35:50
Always a pleasure being here, Reema. Thanks so much for having us.

Grant Versfeld 35:53
Thanks again. Reema. It's been a pleasure.

Reema Moussa 36:01
Thank you so much for tuning into this episode of the Tech Policy Grind. I'm Reema Moussa, and I'm the producer, host and editor of the show, and really glad that you could join us. Huge thank you to Lama Mohammed, our Social Coordinator, and Allyson McReynolds, our Accessibility Coordinator for all their help in making this show possible as well as our whole team over at the Internet Law and Policy Foundry. Have a good one y'all.

Transcribed by https://otter.ai