Module 3: Discussion with Viktorya Vilk from PEN America

[00:00:00] Hi and welcome back to module three of online harassment journalists strategies for defense. Today, we are going to be talking about different tactics that online abusers use to harass and intimidate journalists online. And today, we are very fortunate to have with us Victoria Clarke from America, and she is the program director for Digital Safety and Free Expression. And she needs this organization's work to counter online abuse. So welcome, Victoria. It's a great pleasure to have you here today. You just start off by telling us a bit about the organization and the work that you do gladly.

[00:00:42] And thank you so much for the opportunity to contribute to this wonderful course. And America is a nonprofit that celebrates and defends the written word here in the U.S. and internationally. We actually have over seventy five hundred members who are professional writers, journalists, editors, publishers, folks in the creative and media sectors. And they started reaching out to us probably around 2015, 2016, asking for help, navigating online abuse. And when we did a survey in about 2017, we found that writers and journalists had been targeted by online abuse, not only experienced significant psychological and emotional stress and trauma, but actually started to engage in all kinds of acts of self censorship so they would change what they wrote about. They would leave social media for stretches of time or permanently. They changed how they wrote about certain topics, which was enormously alarming to us as a free expression organization. And so what we realized is that online abuse is actually deliberately intended to intimidate, discredit and silence the voices that we actually need to hear from most. And so we've been tackling that problem from several different angles. We've developed tools and resources to empower journalists to defend themselves, like our online harassment field manual, which I know will be mentioned later on. And at the end, we work with newsrooms and publishers to put in place stronger policies and protocols to support staff who are facing abuse. And we are also now leading research and advocacy efforts on how digital platforms can better protect their most vulnerable users. So we try to tackle the problem from different sides all at once.

[00:02:17] Great, thanks, Victoria. So we've spoken about online harassment, can we delve a little deeper into the common tactics that you have seen being used primarily because your organization is based in the US against us, US journalists?

[00:02:36] Absolutely. So before I delve too deeply into the tactics, I do think it's really important that we start with a shared understanding of what we mean by online abuse. It's a term that has know there are a lot of different terms that circulate cyber harassment, cyber abuse, cyber bullying, not all of them being the same thing.

[00:02:53] When we talk about online abuse, what we're talking about is an individual or group that targets somebody in a severe or pervasive way online in order to cause them harm. So the words that are really important so severe basically is that it implies that just one incident of abuse, if, for example, somebody publishes your home address or threats, you can be enormously destructive for a person's safety and mental health. Pervasive really gets at the fact that maybe an individual incident like an insult or a piece of spam is water off your back. But if you are being bombarded daily for years with this kind of stuff, or if all of a sudden in three days you are bombarded by tens or hundreds of thousands of messages, that, too, can take a major toll. And it's important to understand that abusers can be anonymous. They can be somebody you know, they can be a publicly known figure, they can be an individual. They can be a group. And the tactics themselves are evolving very rapidly. Some of the ones that we have seen a lot of impacting journalists in newsrooms in particular are threats and, you know, the threat of physical violence. But for journalists who identify as women or non binary, it's often threats of sexual violence, hate. Right. Hateful expression, imagery, slurs, et cetera, that target somebody because of their identity, their race, their gender, their sexuality, their ability. Journalists who identify as women, as LGBTQ or as people of color are often disproportionately targeted as a direct result of their identity. With hate speech and hateful expression, dog piling has a lot of different names. Sometimes people call it cyber mob attacks, but it's basically when a whole cluster of accounts online target one individual from all sides. And it sometimes looks organic, but it's often coordinated. Behind the scenes in some cases, and then distribution of nonconsensual intimate imagery and what that essentially means is that somebody takes a sexually explicit or intimate photo or video of somebody else and then distributes it without their consent. Sometimes people

call it revenge porn, but I really don't like that term. I think that term is a total misnomer because it so rarely has anything to do with revenge and often rarely has anything to do with sex or sexual acts. It's really about power and humiliation, and it can put women's lives at risk. But it is important to understand that at least in the United States, there are now 41 states and counting where distributing nonconsensual intimate imagery is punishable by law. So that's something to keep in mind, that there is a shift in kind of legislative solutions to this one specific abusive tactic of nonconsensual intimate imagery.

[00:05:42] Well, that's at least some positive, I suppose, advancement in that area. I'd like to touch a little bit more on on this this this tactic of using nonconsensual and intimate images of women journalists in order to try to silence them.

[00:06:02] So this is a tactic that you have seen in the US. But actually, I think a lot of our participants involved in this course will also have seen this tactic used against them in countries around the world. And we know that this is not just about intimate images of women, but it can just actually be a normal photograph of a woman that is then misappropriated and changed and boxed and doctored to to represent something that it is not. And just the mere act of that is enough, you know, to to cause increased and sustained levels of online harassment, quite often accompanied by death threats and violent threats as well. There is the case of runner up the the the journalist from India whose image was taken and morphed onto a pornographic image and circulated widely online and the so-called deep images which we have seen an uptick of, I would say, in the last few years. And this is where video is manipulated in a way that it's almost impossible to tell whether the images is real or fake. And we have seen that being used against women, women journalists as well. So if you are a woman journalist, it can be complicated to protect yourself against manipulation of your image online, especially if you're a broadcast journalist, for example. So I was just wondering, Victoria, do you have any tips that women journalists can use in order to better protect themselves or to precautions that they could take?

[00:07:55] Yeah, absolutely, so for journalists who are not broadcast journalist, who's, of course, images are everywhere, but if you're not if you are not a broadcast journalist, I would say be very, very mindful of what image you post of yourself on social media. Try to minimize those as much as possible, especially on social media accounts where you have the settings set to public. We'll talk a little bit more about that later. But as a general rule, be thoughtful about which images of your face you include on your social media accounts. You can also do something that's really useful called a reverse image search. There are a couple of ways to do it. I'll tell you the simple way that a slightly more sophisticated way, a simple way is if you basically Google your own name right. Or search for your own name and a search engine, then go to the images section and where you see photos of yourself, you can. Right click them and search Google for image. So in a way, you're literally kind of doing it in the reverse where you're looking for that image all over the rest of Google and anywhere where it pops up on the Web, at least you'll know and then you can decide to make comfortable with that image being there or not. And if you're not, you can try to get it removed. The more sophisticated way to do reverse image search is to use in a search engine like Bing or potentially a tool like tonight, where it actually lets you drag your profile photos from Facebook, from Twitter, wherever into the search engine and search the web for any misuses or uses of those profile photos. And again, if you discover your photo somewhere you don't want it, you can try to get it taken down. It doesn't always work, but it's often worth a try, especially if you own the copyright to your own photo. You can make a claim that basically as well. That's my copyright. I want I don't want my photo op on your website. It's also a really good idea to have a pretty serious conversation with your friends and family about what images of you they post online and ask them to reduce that as much as possible and also ask them either not to tag you or to turn your settings in such a way in your social media accounts where you can approve any tags people add to your images, if that makes sense. Right. So you just want to ask your family to be mindful about reducing images of your face on the Web and reducing tagging of those images of your face on the Web.

[00:10:08] All right, thanks. So we've talked about this obviously very abusive tactics that are used by online abusers to target journalists, but they are also more more subtle attacks. I was just wondering if you could expand a little on on on that concept of what is a subtle attack and how it damages the journalist's reputation.

[00:10:32] Absolutely. So the problem is that abuse of trolls are endlessly creative when it comes to inventing more subtle forms of abuse that are harder to track and limit. And I can talk you through some of the ones that we see a lot of. One of them is impersonation, it's when somebody creates a hoax account that looks like you, uses your photo, uses your name, but of course isn't you, and then tries to spread offensive or inflammatory statements in your name with the intention of discrediting you or defaming you. And I've seen this happen with a lot of journalists in the U.S. where a Twitter account will pop up using your face in their name. And that Twitter account will deliberately be used to spread disinformation, bad reporting, or to say hateful things about other journalists. And the idea is just purely just to damage your reputation. It's actually comparatively easier to get this kind of abuse taken down than others. Impersonation accounts are a violation of all platforms, rules and standards. And so if you report it, you can often get it removed. Unfortunately, occasionally one of these abusive accounts will say Perati somewhere in tiny letters in the corner. And then that's the way to get around the you know, the terms in the standards. You can still get those accounts taken down, but sometimes you actually have to escalate them to the platform, either through your newsroom for a press freedom organization like I like college, like Penn America. They can sometimes escalate it directly to the platforms, but the parody accounts are harder to get taken down. But that's something to keep in mind it can be done. Message bombing is when somebody's an abuser, floods your cell phone or your email account with so much spam, with so many messages that you basically can't use it because you can't find what you need. This happened in a really public way several years ago to ProPublica, the journalism organization, the U.S., several of their journalists were flooded with spam emails and they actually had to kind of revamp their entire email system in response to a lot of journalists who identify as women or non binary experience, something called concern trolling. Concern trolling is when somebody, an abuser poses as your fan or your supporter and they pretend to be saying something nice or constructive to you, but then you start talking to them, more things become abusive. So, for example, women are often given helpful suggestions about how to improve their appearance or are asked endlessly detailed questions about the reporting that start to actually try to undermine the quality of the reporting or the sort of intention of their reporting. So it's really important to keep an eye out for that and not get sucked into those conversations if you feel like that's the direction it's going. And then finally, I will mention dog whistling, dog whistling. You know, I probably has different names in different places, but everywhere has dog whistling. Dog whistling is when an abuser uses a word or a symbol that has a double meaning. And it's often used to signal other abusers to attack someone. So to give you just one example, in the United States, there was a period of time when abusers would put three parentheses on either side of the name of a Jewish journalist in order to identify that journalist is Jewish. So that anti-Semitic and far right trolls could then all attack this one journalist from all sides of the Internet. What's interesting is that in the United States, a whole bunch of Jewish journalists basically decided to. Take control back of this symbol, and so they started proactively putting the three parentheses on either side of their name and their Twitter handles in their bylines and elsewhere. So that's an interesting example of people who are fighting back against dog whistling. But the basic premise of dog whistling is to try to generate a set of attacks against you and to signal to other people to come after you.

[00:14:18] Yeah, I think a lot of people taking this course and they may not be familiar with the actual language and terminology that that you are using here, but they will be familiar with the tactics.

[00:14:29] And I know through my work that I have spoken to journalists in Latin America, for example, who have indicated to me that they have been harassed online using the tactic of dog whistling normally link to to political parties where they have been clearly identified as a journalist who know supporters of that party should be should be attacked. And I'm sure many people taking this course will have experience. Something similar might be something useful and interesting to share, possibly in in the Facebook group, the names of shifting tactics that people are using in different countries. I think that's actually quite an interesting area of study further down the line, maybe so we thought we've looked at these these subtle attacks. We've looked at very abusive attacks. But there is one attack that has become I hesitate to use the word famous, but it is particularly infamous. Yes. The infamous strategy of doxxing, which we have seen, I would say an increase of over the past few years. So could you just explain what doxing is and why is it so, so serious so quickly?

[00:15:45] So doxxing is the publishing of sensitive private information online, like your home address, your cell number, some form of government ID number that you might have, even the names of your children or other family members.

[00:15:59] And this is something that is so pervasive now. It's happening across the United States. It's happening all over the world. I'm hearing about it every day at this point. And it's dangerous because it is still sometimes live under this illusion that somehow online harassment is not real life, which is, of course, is absurd because the especially under the pandemic, the boundaries between, you know, what's in person, real life and what's online become completely fluid. Our lives are entirely online right now. But the thing that's so terrifying about doxxing is that if you think that somebody knows your home address or has your cell phone number or knows things about your children or your family, it starts to feel even more like an online attack and sort of. Incur into your physical safety and into your physical well-being and your physical life, and that is why it's both dangerous and really alarming and can have a real psychological toll on people as well. I actually built a hands on workshop with another wonderful organization called Freedom of the Press Foundation that teaches journalists how to Duc's themselves. And of course, I don't mean that literally, but really it's to try to think like a doctor, think like an abusive troll who's trying to dig around on the Internet, find information about you so you can find that information proactively and see if you can get any of it removed. And the thing that's good is that journalists are actually very good at digging through the Internet and finding information. They just very rarely apply that theory to themselves or that practice to themselves. And so what I would encourage journalists to do is to actually turn their investigative reporting skills on their own data and their own information to find out proactively what's online.

[00:17:35] That's a really good tip there. So do you have any any kind of step by step advice for journalists who now may be interested in investigating themselves instead instead of investigating others?

[00:17:53] Sure, I can walk you through a whole bunch of steps. So the first thing to do that, the simplest, most logical place to start is to Google yourself. Right? Not just your name, but variations of your name, your phone number, your home address, the online handles that you use. However, it's really important to understand that Google is so good at tracking you that it give you customized personalized search results, which is not helpful because that's not what a doctor, an abuser would see. Right. So a good thing to do is to either use incognito mode or private mode, private browsing mode, or better yet, try a different search engine, a privacy focused search engine like Dr Go. There are many others and see what kind of information are you finding? Where does it live? Is it on your social media? Is it staff bios? Is it web pages of websites that you forgot that you were ever involved in? You know, where is this information cropping up? That's the first thing to do. The next thing you can do is to set up a Google alert for your full name, maybe for your phone number, your home address, whatever private data you're concerned about, set up a Google alert. And that way, if suddenly that information pops up online and starts circulating, you find out about it right away because you have a Google alert. The other thing I would recommend is to really seriously audit your social media accounts and type in your settings. Abusers will comb through your social media accounts and look for private information they can leverage against you. Maybe it's an embarrassing tweet that you forgot about a long time ago. Maybe it's a photo where you accidentally reveal the street name or the home address that you have. And so the first thing I would do is just kind of go through your social media and make sure that you haven't put things like that on there by accident or forgotten about them. But I would also suggest you just be strategic about which social media platforms you use for which purposes, and then adjust your settings accordingly. So, for example, let's say that you use Instagram, you have an Instagram account and you're using it for photos of your puppy or your child or something that's very private and personal. You want to make sure that your privacy settings on that account are as tight as possible. On the other hand, if you're using Twitter professionally to get sources to promote and publish your work, it's OK to have more public settings on your Twitter account. But in that case, you shouldn't be including private information like your birthday or the names of your children on your Twitter account. So that's kind of what I mean about being strategic. Last couple of tips, I suggest look at your bios and Steve's and the information you include on your personal website. A lot of us made those before the Internet got as nasty as it did, or maybe before we became higher public profile and people started to come after us. And so you may accidentally have included a lot of very private personal information on your CV or your bio, et cetera, that you

might want to start removing at this point. And if you need to have your address or your email or your cell phone visible for some reason publicly. Create a public facing version of that, right? Have a public facing cell phone, a public Facebook email, and keep that separate from your private cell phone, your private email account, which you only use for friends and family and people you trust. And the only thing that should be circulating online is the public face stuff that the private fees and stuff. And maybe the last point is that if you're in the US, this is true in a few different countries, but it's really, really bad. In the US we have these things called data brokers. They're companies like White Pages or Spokeo that literally just scoop up your private information online and sell it for less than a dollar to anybody, which is crazy, but it's true. And so you actually can request that these companies take your information down, but you have to write them. It's really labor intensive and time consuming, but it works. Or you can pay a data scrubber subscription for various companies that are out there to actually have them do that, removing of data for you, which will save you time but does cost money.

[00:21:38] And finally, remember that your family and friends may also be vulnerable to boxing. When when a journalist is very high profile or they become a lightning rod for attacks, people will often come after their friends and family as well. And so if you're worried that you might be at risk of being taxed, it's actually really important to talk to your loved ones about their own online presence and figure out whether you may have to actually detach yourselves publicly from them online so that your accounts are linked or just ask them to be really careful and respectful about the kinds of information they post about you and about themselves, at least for a period of time if you're concerned about safety and about doxxing.

[00:22:17] Great, thanks, Victoria. These are particularly helpful tips for journalists and I think maybe a lot of journalists taking this course might be thinking, why is it important for me to understand the tactics that abusers are using in order to me? How how does understanding what is happening help me in any way?

[00:22:41] That's a good question. I think that. From the experience I've been doing this work over several years, I actually have found that probably the very first step when you're dealing with online abuse is to identify and name what's happening to you in a really clear way. So if you're being critiqued, even if it's in a mean way or you're being insulted, somebody calls you an idiot or someone tells you you're a terrible writer. You can choose to refute that, you can choose to let it go. OK, but if you're actually being abused, people are making you feel physically unsafe. They're doing harm to your mental and physical health. They're doing harm to your family. It is really important to call that what it is to call it abuse, to figure out what the tactic is and give it a name, because that not only signals, it's a tangible problem that has real serious consequences, but it's actually really important if you're going to have conversations with allies, with your friends, family, with editors, with law enforcement. Once you've decided that you understand what's happening to you, you've given it a name. It's really important to document it. Right. So to take screenshots, safe hyperlinks, save emails and voicemails of what's happening to you, you need that documentation. It's proof to other people of what's happening to you. And it can help you again in conversations with allies, employers, and if you want to pursue legal action. And finally, naming what's happening to you is also really important if you want to report abuse on the platforms, because most people who have experienced trying to report abuse on the platforms know that the platforms will ask you to pick from several different tactics and to explain what's actually happening to you. And so being able to say what it is or point to the right thing increases the chances that your reporting will be effective, even though sometimes reporting can be really frustrating and ineffective. But it can also yield results in some cases.

[00:24:28] Great. Thank you, Victoria. Victoria, thank you so much for speaking to us today and sharing your insights on abuse and tactics used by online harassers. If people who are taking the course are interested in finding out more information and tactics that they can use themselves against online harassers, where will they be able to find this information?

[00:24:53] So there's a couple of places I really encourage you to check out our online harassment field manual that Pennsburg that's the name of the website. It's a pretty comprehensive guide on how to deal with abuse. And there's a whole page in there with guidance on how to docs yourself. So that would be the place that I would go to start. And then there are

lots of really wonderful resources from organizations like the IMF and many others that you could also take advantage of.

[00:25:16] Great. Thank you. We also just to point out to participants that I don't have an PennyMac. I have some infographics that you can find in our reading material for this week as well, which outline the tactics that we have discussed today for you as well. Victoria, thank you so much for your time. And I look forward to speaking to you again soon.

[00:25:45] It was my great pleasure and I'm very honored to be part of this course. Thanks so much. Thank you.