CYBER ABUSE PROJECT PODCAST 1.5

KRISTELYN: Intro
Welcome back to the Cyber Abuse Project Podcast series where we invite guest to talk about the use and misuse of technology, sexual assault, domestic violence, dating violence and stalking, including cyber stalking. This project seeks to support the work of criminal justice professionals and campus administrators as they navigate these cases at their respective universities. My name is Kristelyn Berry and I am the Training and Technical Assistance Specialist with the California Coalition Against Sexual Assault. Joining me is my co-host and colleague Marta Beresin, who is the Policy and Legal Director with Break the Cycle. Hi Marta!

MARTA:
Hi Kristelyn! Today we're lucky to have two great guests with us, Ian Harris and Detective Christopher Brown. Ian Harris is the Legal Manager at the Safety Net Project of the National Network to End Domestic Violence, and Detective Christopher Brown works at California State University, Long Beach. In our conversation we'll be discussing evidentiary issues in cyber abuse cases on campus from a local and national perspective. Welcome Ian and Detective Brown. Can you each tell us a little bit more about your role and your respective organizations? Let's start with Ian.

IAN:
Thanks so much for having me. I am really happy to speak with you all today about a topic that is really near and dear to me. So, I am the technology safety legal manager at the National Network to End Domestic Violence's Safety Net Project, which looks at the intersection of technology and domestic violence. We do a variety of different things, but some of the work that I'm particularly working on is we create resources at our techsafety.org website, which has resources for survivors of domestic violence or for individuals who are working with survivors -- whether they be attorneys, advocates, or law enforcement. We're also doing a great deal of training around the country on technical assistance. The last thing I just wanted to mention is one of our newer projects that I think that people might be interested in we that we are creating an app that will help individuals who don't have an attorney to collect digital evidence that they can hopefully use within their legal cases to get more effective relief, when they are experiencing cyber abuse.

MARTA:
Great! And Chris can you tell us a little bit about your role at California State University Long Beach?

CHRIS:
Absolutely and I would also like to thank you, it is a privilege to be involved in an organization like this and to be involved with a project that's so important to our community members. I've been a police officer at the Long Beach State University Police Department for a little over 10 years, currently assigned to the Detective Services Section where I handle crimes related to sexual assault, dating, domestic violence, and stalking. I'm fortunate to work in an expanded

community team at the University through a grant provided by Cal OES and supported by CALCASA where we provide services to survivors in a trauma-informed way. I work on a team that consists of sexual assault advocates, long-term trauma counselors, our coordinator for the Women's and Gender Equity Center, and our Title IX investigators. And it's really allowed us to tackle the problem of sexual violence on our college campus. We've done a lot of preventative education on what sexual violence is, what bystander intervention strategies look like, and what resources are out there for survivors.

We tend to focus on three key areas of our campus community, which include student residence, student athletes, and our Greek organizations. But we've also done a lot of work on institutionalizing our resources by training staff and faculty members on how to respond to survivors who may disclose to them, really keeping intact the idea that if a survivor has disclosed to them, that there is an inherent trust in that relationship and we want to foster that trust into and through not only the criminal justice system, but the university system as well.

I also work for a consulting firm called D-PREP that conducts a lot of training and consulting services for disaster preparedness and critical incident response for civilians and law enforcement. In today's environment when we're dealing with a lot more mass casualty incidents we're finding that a lot of these incidents happen to revolve around leakage that occurred on social media and the idea that these offenders are giving out information about what they plan to do via social media. So we started to do a lot of work on training individuals about the issues of social media and cyber abuse in K-12 environments. We talk a lot about how to recognize abuse, how to report it, and why it's so important to not only have policies in place to address the abuse itself, but why it's equally important to have prevention strategies and to have these kind of strategies to help the offenders as well.

KRISTELYN:
Wow, thank you both for describing your work, sounds like you're doing awesome things in both of your organizations. So, we are going to jump right in, how are cases of stalking and sexual assault, dating and domestic violence impacted by cyber abuse?

IAN:
So, before I started at my current role at the National Network to End Domestic Violence, I had about 10 years of experience as a civil legal services attorney in New York City, and what I found in that work is that today's cases of domestic and dating violence almost all have some type of technological component to it. While technology itself is not abusive, it's oftentimes used as a tool of abuse, and the impact can be really substantial. For example, because we constantly have our cell phones with us, our smartphones, our computers, there is an aspect of technology that is being misused. You essentially have a 24-hour cycle because for so many people, getting rid of the technology, stepping completely away from the technology is not really an option, whether it be because that's part of their businesses or because it's just necessary for communication with friends and family. The ability to track someone, to monitor, to consistently and constantly send harassing text messages or calls can really be incredibly disruptive to somebody's life and can again have this 24-hour impact. It also has another aspect

where not only you have to deal with abuse from one abusive party towards somebody who is experiencing the abuse, but you also have the potential or an expanded potential for third party abuse. So, the potential to have sort of mob attacks where by putting something onto social media you can get other people involved in the attacks. These types of large scale mob attacks online can have tremendous impact, not only because it can be hurtful, but it can also impact the potential for future employment, to get into schools, other types of employment, current employment opportunities. So what we are talking about here is a type of abusive behavior that is really doing a lot of the same types of harm as domestic violence, dating abuse behavior that we've seen for many, many years but has a much more expansive capacity because of how frequently one can do it and the fact that you can get so many more people involved in the process.

KRISTELYN:
Thanks Ian, Chris do you have anything else you want to add?

CHRIS:
Absolutely, you know I would echo Ian's assessment that cyber abuse not only are we dealing with the initial incident, but now we are dealing with a very expanded range of how this kind of abuse can affect one person and how it can involve an entire community, family, workplace. It's such a critical component of these investigations, and you know I think the biggest thing with cyber abuse to me is that it can happen anywhere and at any time, so not only are we dealing with the trauma of the physical incident, we have to deal with the potential for the trauma to be triggered in times and in places where the survivor would normally feel safe. So cyber abuse has a very big impact on how the survivor relates to themselves, how they relate to the individuals that offended them and how they relate to their internal community and how they relate to their expanded community, especially in locations like a college campus. I can't tell you how many cases that I've investigated where the incident is between one person and another person in the dorms, but by the time it's reported to the police department, the entire floor or building knows about it and everyone has their own spin on what happened and how it occurred, and they're all wanting to report different facts or circumstances, so it has the ability to really get out of hand very quickly. But from an evidentiary perspective, cyber abuse can be very good in providing electronic records of text messages, emails, images that can be very powerful to be used in court in criminal cases and civil cases, but we also have to be really cognizant of the types of activity that are happening on the internet and through social media. AndI think it is really important that officers understand that that's very powerful evidence especially if we are looking into charges of witness tampering or criminal threats.

IAN:
That's such a great point. I really think that technology and the evidence that comes from technology has become completely transformative for domestic violence and dating abuse cases. Cases historically have been between two people, one person saying something happened and another person often times denying that it happened with very little testimonial evidence from other people, and technology really has the potential from an evidentiary standpoint to provide a lot of context to experiences that are otherwise often times hidden from

law enforcement and other parts of the system that are trying to assist. So that type of evidence is so important for how cases are worked on nowadays.

CHRIS:

Absolutely!

MARTA:

Yes that's such an interesting point that you both raised because when we think about cyber abuse, we think about the social media platforms being such new things out there that courts are learning to deal with and prosecutors are having to learn to deal with and young people are having to learn how to deal with and it's this whole new world of discovering how do we prosecute this kind of stuff and how do we deal with this stuff. But on the other hand you are saying that it is a new tool of abuse, but it's presenting some new ways that people can actually find justice and report because it's providing evidence where there may not have been evidence before. The evidence may have adjusted the he said/she said situation, and that kind of leads me to the next question. What are the types of social media platforms that you're seeing young people using today and how are they being misused?

CHRIS:

I think the three most common social media platforms that I'm seeing out there today in the cases that I work are the big ones-- Facebook, Instagram and Snapchat. I think the reason why is that they are the most socially acceptable, they are the most socially provocative and I really don't know anyone that doesn't have a Facebook or at least an Instagram account, and I think those are the most common social media platform that are out there. When I teach the K-12 social media classes, those are by far in the top 10 by population size. We're talking about billions and billions of people on these kinds of platforms, and these platforms are constantly evolving and designed in a way to provide user interface easily and to provide information easily and being able to connect in communities because realistically, that's all social media iselectronic communities online, groups revolving around a similar idea or perspective that form communities and engage in social media relationships

IAN

So there is this joke about the fact that young people are leaving Facebook right? And their parents are starting to join, and I think there is some truth to it. There has been slowing numbers in terms of Facebook usage when you look at national statistics, but I definitely agree that Facebook is still a major player for young people, and Instagram and Snapchat are really huge. Pew just came back with a poll fairly recently that showed that YouTube is also one of the most commonly used types of social media. I do think what's interesting though is that when I was looking through the latest recent research from Pew, what they did is gave a number of different platforms and saw how many people were using them. What was left out of there though is there wasn't a huge opportunity for individuals to talk about the things that they use that fall outside of those. So, there is a lot of commonality across populations in terms of young people use of social media. And those are probably the big ones, but I do think that teens are not a monolithic group.

KRISTELYN:
In terms of platforms how are you seeing them being misused? And what are the trends you see in cyber abuse cases right now?

CHRIS:
So like I mentioned, Facebook, Instagram and Snapchat are the big ones that I see in my investigations right now. Particularly with Facebook there's a couple of things that brings to mind, one of them is the Facebook live feature, and that's the feature where you can live stream video with really no buffer on time in which that as you record it's being spread live across the Facebook universe, and I think that that has a tendency to affect a lot of different communities -- in especially what's being recorded. You know, we see time and time again on the news incidents of child abuse, perceived misuses of force on behalf of law enforcement, gang violence, domestic violence, sexual violence, kidnapping, all these different types of videos that are live-streamed onto Facebook and through different social media aspects, have a huge ability to impact how it is that law enforcement can respond. While used intendently, meaning that people purposely stream on the internet, there's no misuse of that, what they're capturing is really highlighting something that a lot of people normally typically don't get to see in their every day environments. You now go to work, you go home, you go to school, you take care of your family, and you don't typically expect to run into a violent scene or a domestic violence scene, something that is so shocking to the senses, but what's happening now is that we are seeing it more and more on the internet and on the media that's it's kind of desensitizing people. So I think we have more to worry about in regards to what it is that's being live-streamed on the internet and how we can interact and react to those kinds of situations.

I'm also seeing an increase in kind of extortion types of cases. We've had a couple of cases on our campus where unfortunately individuals will befriend someone of the opposite or same sex and will make adult videos on the internet and then basically through Facebook the person threatens to release the video to family members unless they agree to pay a certain amount of money. And usually typically that's happening from outside of the country in because when we track those records down, it's usually individuals from countries outside of the United States that are conducting the extortion, and it's hard to follow up on those cases because obviously we are outside of our jurisdiction and those kind of cases have to be forwarded to our federal partners. But that's typically the kinds of misuse I see on Facebook.

With Instagram and Snapchat, since a lot of that stuff is more immediate, a lot of the misuse has to deal with people, well we're dealing with college students, we are dealing with people outside of their home in some circumstances for the first time without parental oversight, their trying to find who they are as adults, they're trying to experience the college life the way they feel it's intended to be experienced, so they're doing things and experimenting with things they haven't done before, they're dealing with behavior they haven't experienced or had to deal with before

and a lot of that stuff is getting captured on social media. A lot of that stuff is getting captured through videos and posts and like Ian said earlier, it has the definite ability to impair their future selves.

We're also seeing a lot of instances where people will trade back and forth images of their personal body parts or videos of them having sexual intercourse and obviously when relationships end, some of them end badly and sometimes individuals will take it upon themselves to release that kind of video footage in an effort to cause emotional pain to the other party. So now we are dealing with cases of revenge porn and criminal threats and things like that. So those are typically the types of misuse that we see, that I see when I'm investigating.

The other thing that I'd like to bring up about these kinds of platforms is that we're dealing with entire communities here, so if you're dealing with a personal issue between your spouse and significant other and it's involving domestic violence, dating violence and you talk about that kind of violence on the internet that information, like Ian said earlier, is getting broadcast to a larger network. Where in the past you might have told those closest to you, you're now explaining some of your personal issues to the entire world where some of those people and some of those issues might not be perceived in the same way. So now we are dealing with extended family members not believing what it is that you're saying, we're dealing with cultural implications where the female in the relationship is expected to act a certain way, and by reaching out and reporting and doing these kinds of things, we're challenging social and cultural norms, so the expected range on these kinds of things is really impacted by how we handle these investigative cases.

IAN:
Those are all really great examples and I definitely agree with a lot of what was said.So we at the National Network to End Domestic Violence recently did a yearlong survey of judges and law enforcement prosecutors and survivors to ask "What were the tech abuse issues that were most relevant in their lives and in the cases that they were seeing"? And we very consistently received feedback that the two biggest issues that most communities were confronting were abusive text messages, harassing text messages, and social media posts.

And I agree with Chris' assessment of the way that social media is oftentime used.The only thing that I would add is that there are some interesting subtle things that happen online that can be hard to perceive from the outside, but can be really impactful for people. So for example, I have had a couple of cases in representing young people in New York City in legal cases in which there was domestic violence taking place, in which there was a threat to post pictures, not nude or intimate images necessarily, but just pictures in which my client was in an environment that would've been inappropriate in their own community, whether it be a party or whether it just be with somebody that they're not necessarily supposed to be with because they're not supposed to be in a relationship as an example. And the threat of having that information posted online where their community could see it, even though it wasn't an intimate image, even though

it wouldn’t necessarily be something that would keep them from getting a job later in life or into a school that they wanted to, which definitely does happen, and even though it wasn’t that, it was still enough for at least a handful of my clients to not want to go forward with their legal cases because the impact of that on their community would’ve been so disastrous for them that it just wasn't’ worth it.

Similarly, fear of having something posted and you can see suddle changes in the way that communities start to interact with people, so they kind of blame the victim mentality.That can also play out where a person has experienced violence and has decided to come forward about that violence and the community member, in an attempt to protect the person who was the perpetrator, will either start saying negative things about the survivor’s or the victim’s postings or stop liking them and giving other types of settle inferences that their place in their society and in their culture is shifting.

But I did want to just loop back around and say that by far the thing that we see most often happens to be around text messages, and those text messages that are clearly harassing, threatening, that are clearly demonstrating stalking, as well as text messages that are a little bit more hidden, a little bit more ambiguous, sometimes anonymously sent, and sometimes sent by people connected to the person. So that is the type of third party abusive behavior that I referred to earlier.

MARTA:
Right well that actually leads to another question that I had Ian, which is that survey you did, was that of young people ages 12-24 I wasn’t sure if you said that or was that of all folks across the age range because I’m wondering whether do these cases look different in high school and environments then they do with non-students, in cyber abuse cases.

IAN:
That particular study was across all ages, though there were a couple of groups that we interacted with that exclusively working with young people though we didn’t interview young people themselves, but we did work with a couple of people that were exclusively working with that population what we found was that in that group as well and that group that had a more general age range, that those issues were still the most prevalent. Though I do think while the platforms are very similar, I don’t think that the abusive behavior always is the same, and more importantly I don’t think that the impact is the same because when working with young people more than anything that we’re talking about is a group of people who are trying to find their place in the world and of course in defining identity and may be more impacted by the social system that surrounds them. But we are also talking about a group of people who have greatly diminished experience with/contact with institutions and finding help and have much less resources available. I will never forget in representing teenagers in New York City that there was a court and the court that somebody would go to might be a couple of miles away from their home in Manhattan, which doesn’t seem like that much-- it’s actually probably like 30 mins on the train to get there. But as a young person, the ability to move freely in the world is really restricted and so the idea of being able to get on a train and go to a court that they'd never

necessarily been to, to a part of the city that they've never necessarily had an opportunity to go to, to speak to a judge that they have no understanding of or have no experience with at least, is an incredible barrier to getting access to justice. And so we have to think about these systems barriers that are very much linked and tied to the age and the development and resources available to people.

CHRIS:
You know I would have to agree with Ian-- there's a definite change in the impact of cyber abuse when we're looking at age groups. As a university police officer, we primarily deal with younger groups of students, 18-24, but we also have a fair amount of graduate students and doctoral students on campus and so the types of cyber abuse I think don't typically change too much when we're talking about those different age groups. I just think the impact and the responses from the victims and offender will vary when we are talking about different age groups again, we are getting individuals that are fresh out of high school. Like I said earlier, it's the first time that they're out on their own, they're experiencing new things, they're developing their own identity, they're coming to terms with who they want to be as an adult and they're kind of meandering through this quagmire of life that we call college. And so cyber abuse cases or cyber abuse within cases of sexual violence, domestic violence, stalking and things like that, physical incidents or the spawning incident of these cases, typically don't vary But it's how the individual responds to these cases that I think is what varies and what the impact is on that person. Because I've had cases where, the survivor is like "it's not really a big deal to me", and then I've had other cases where the cyber abuse is very minimal and it would seem like it should impact the person in a very minute way, but it's the end of their world. We tend to see that more in younger students, and I would hazard a guess that, like Ian pointed out, when we're dealing with K-12 students, we're dealing with individuals who are still learning, they're still growing as human beings, and so that idea of identity is so important to them that what may be a little blip on the social media radar can have a huge impact on someone. So that's typically where I see the change in cases is the impact, not necessarily the type of cases.

KRISTELYN:
So, with the way the technology is evolving and changing, can you compare and contrast for us the process of gathering evidence in a cyber abuse case versus in an offline dating abuse, domestic violence, sexual assault and stalking case?

IAN:
Like I mentioned earlier, for me personally, the fact that there is so much evidence that's going to be available is quite a rich resource. I can give you lots of examples of cases that I've worked on that a text message or social media posting of a video, has really been the difference between somebody getting the relief that they requested in court versus not. I also think it has an extra benefit of speeding up cases in a lot of ways because it can be harder, when you actually have the evidence to prove, it can be harder to just make blatant denials, which can be impactful.

What I will say is this, that when someone is experiencing dating violence, domestic violence, and something extremely traumatic, most people experiencing that are not going to be thinking about evidence collection as a primary issue. That's are going to be the first thing on most people's mind and so you have to ask better questions to get to the issue, to make sure that you're really identifying what might be there. And also you need to give a little more information to make sure people are effectively maintaining the evidence that they have. While there is this greater availability of evidence form digital sources, it's also evidence that's quickly deleted or oftentimes lost. You know, Unfortunately the reality when you really think about technology and domestic violence, one of the ways that abusive behavior oftentimes plays out in domestic violence cases, is that somebody will take someone's phone and destroy their phone, destroying the place where this evidence may live. And so it's really important, in the gathering of evidence, in the storing and maintaining of evidence, to let people know very clearly what is the information that you need and how does it need to be stored and maintained, so that it can actually be useful. You know if somebody has a bruise, has gone to the hospital, and has some sort of record, people know a little bit more and people often time take a picture. Or the institution itself, whether it be the medical institution or the police, will take that type of information and store it. That doesn't always happen in the same way when it comes to technology. So, evidence is really impactful, there is a lot of it, but it is very quickly destroyed and modified and so it is really important to get to people early to make sure you actually get good evidence from what's available.

CHRIS:
I would absolutely concur that the electronic evidence that can be gathered as a result of this is fleeting at best, a lot of times we are provided with a very short window to provide in which provide legal order to social media companies, for example to preserve evidence, because if we wait too long all of that evidence is lost because they just do not have the capacity to save things. Particularly in my role as a sexual assault investigator at Cal State Long Beach, a lot of my cases typically involve individuals who know one another and have some kind of friend relationship or dating relationship, and the issue of having sex, whether or not sex occurred, is usually not up for debate. Both parties usually admit that sex occurred, but what I struggle with in my investigations is whether or not that intercourse or that sexual activity was consensual. In California we have an Affirmative Consent Law, which says that every sexual act has to be affirmatively consented to by the other party, it's not enough to just not respond; there has to be knowing consent between each party, and so a lot of cases that I deal with is where we are looking at the issue of "Did sex happen?" We are looking at the issue of "was there affirmative consent"? And so a lot of that typically revolves around a he said/she said or some kind of argument where we don't have direct physical evidence to prove one side of the story versus the other. And I use the he said/she said verbiage because typically that's where sexual violence occurs, but it doesn't mean that sexual violence doesn't occur between members of the same sex. A lot of times, the evidence that I can gather from text messages are huge and important in so many cases, not just these kinds of cases but all kinds of cases, the social media communications, the posting all of these things, can be very valuable in proving that one party knew that it wasn't affirmative consent. For example, I've had cases where the survivor will message the other party and say, "hey you know, you knew that what you did was wrong, and

you asked me or didn't ask me, I didn't say anything, did you think I'd enjoy that if I was just lying there and crying?" And we'll get good responses from offenders that say, "well yeah, but I thought you were okay with it" or "yeah I knew you said no, but I thought you were just playing around". So, we're getting good evidence from these text messages and social media messages because we're dealing with, obviously social media posts, but there is also this underlying message feature on all these platforms, these private message features that we have access to where we can find good evidence on whether instances were consensual or not.

And then of course when we deal with cases like dating or domestic violence, those kind of communication can be really damaging in court when we are looking at witness tampering or criminal threats, where the offender might be telling the survivor that if you report this, if you tell anyone, I'm going do this, I'm going to tell your family all these kinds of things to put added extra emotional turmoil on the survivor. And then specifically in stalking cases, criminal stalking can be hard to proves, especially if it's being done consistently over the internet, not in person, because you need to have behavior that's likely to put someone in fear of their immediate safety and sometimes in cyber abuse cases that can be very difficult.

But what I appreciate about working on a college campus is that we have Title IX, which says that it's illegal for you to be discriminate based on gender, sexual orientation etc. And so where we might not be able to proceed with a criminal case because we just don't have the elements to prove the crime or we don't think we have a strong enough case in court, we have an ability to significantly impact students' lives on campus because we have a lower threshold when it comes to student conduct issues and so we have a wide variety of ways we can help to not only prevent the crime itself from occurring, prevent additional instances from occurring, but really affect how someone responds to those kinds of complaints. I can't tell you how many times I've responded to a party call with a local city agency and the students in the house really don't care that the police department is there, they want to have the party and they're going to continue to have the party even if a violation is handed out to them. It's a $500 ticket and if everyone throws in 10 bucks then we're good. We're good for the rest of the night, but the minute university police arrives on the scene and we start to talk about student conduct issues and we are threatening student issues on college campus, and we're saying, "we're going to tell your coach, we're going to tell student conduct, you know you could run the risk of getting disciplined at school" they button right up and shut the party down. And I think that threat of harming their future, that's a way they might get kicked out of school or they might get disciplined in such a way that they might have to explain to future employers, really impacts the way they respond to the kinds of conduct that's happening on campus.

So again, social media, text messages, all that kind of electronic information and evidence is really important in cases and it's not stuff that you would typically think to gather in physical cases in dating abuse and domestic violence and sexual assault. That's why I really encourage all of my officers that when you are involved to take initial reports on these kinds of situations, find out if there's any electronic contact between the two individuals because we can lock that down and get those records, then we might have a much better chance of being able to prove violence did occur or the threat of ongoing violence.

MARTA:
Chris, just to follow up on that, can you talk a little bit more about what you advise your officers because it does sound like part of the challenge here with preservation of evidence is the victim really understanding this is evidence. So what do you think are the most important tips in relation to evidence for campus safety personnel to keep in mind when they are investigating these types of cases?

CHRIS:
I think there's two keys things here. First thing is finding out if there's any electronic communication between the two parties:

- Are they Facebook friends?
- Do they communicate via social media?
- Do they have each other's personal pages?
- Do they text message?
- Do they email?
- Have they snapchatted?

If you identify that they are in communication on social media platforms or through text messages, we can go in and try to better track down that evidence, even if it's just to simply to prove that they did have communication because sometimes we'll have cases where one party will completely deny ever having been involved with the other party, but we can prove with communication logs that they did talk to each other, that they did share text messages or pictures, things like that.

The other issue is timing, like Ian pointed out earlier we have a very short window to collect evidence if one or both parties delete that information from their handheld devices or computers. Like I said, most social media companies and cell phones companies deal with outrageous amounts of data and they just do not have the capacity to keep it for very long. So, for example Facebook: Facebook usually has a 7-day window. If you delete something from Facebook, I usually have about 7 days before I can snag it from their servers, before it becomes officially lost forever. If I can't grab it before then, then there's really no way to get that evidence.

So timing is everything for these officers, and one way that we can help to preserve that evidence is by issuing what we call Preservation Request. In California, I don't know how it is in other states, but in California we have the ability to basically send a document to these cell phone companies to social media companies and basically say look we have an evidence code here and per this evidence code you need to freeze everything that's on this social media page or on this social media account and hold it, and we have a certain amount of time to provide you with a court order or search warrant to get that information. But it's basically designed to freeze frame and preserve everything that's in there right now, including deleted material. So I tell all my officers in my department, "if you think there is something in the cell phone or online that might be really important about this case, tell me about it so I can get these Preservation Requests in." Because sometimes, especially when you're dealing with these larger agencies, it may take a little bit of time before a detective who might have more extensive technological

knowledge on how to go about getting these search warrants and serving them and collecting this information, it could be a while before they even see that report because the report has to be written, then it has to be approved, then it might get sent to the records department before it's submitted to the Detective's Bureau. So we are talking about maybe hours, days or even weeks before a detective even has a case land on their desk where they might be able to take some investigative action. So by recognizing the kinds of information that may be available to you and informing the appropriate people that need to know about it, whether it's a detective or maybe as a senior officer at your department, you have the ability to craft search warrants or get that information out.
It's very intuitive on behalf of the survivor something that a police officer might look at that and say that's not threatening at all, they didn't say they were going to hurt you, stab you, kill you, but it's a threat to that person's livelihood or a threat to that person's family organization or it's a threat to that person's work. Subtlety is everything when it comes to electronic information and sometimes when we see these things via text message or social media, they might not come across as criminal threats, but they are threatening to that individual. And if we can capture that information and are able to produce that information in a legally sound way we can make the difference between somebody making bond based on their own recognizance or in a lot of cases, if we have a lot of evidence, it might be that much better for the offender to take a plea deal, not ever have to go to trial in the first place and retraumatize the survivor by having to testify in front of a courtroom full of people that they don't know about what happened to them in a very personal way. So I think that identifying the amount of information and types of evidence and the timing on how to collect that information is really important for all law enforcement to be aware of, particularly on college campuses.

MARTA:
And Ian do you, from the perspective of an attorney or advocate, do you have any tips that you would like to give to campus safety personnel about campus safety evidence, based on your experience?

IAN:
Yeah, absolutely thank you, I mean I definitely agree with all of what Chris has said. What I want to add is this, I think there's three points and they all kind of revolve around trust. The one thing that I've learned from working with young people in particular is that, we shouldn't assume that there's going to be trust from those individuals that we're working with because there's actually a lot of reasons for young people to not trust individuals who are in position of authority, in systems, and so we shouldn't assume that**.** I was working with a group of students, and one of things we did is I had them look at universities in the general area and look at the statistics that were presented and provided by the universities about the number of domestic violence, stalking, sexual assault incidents that were taking place on campus. And what was really shocking to myself as well as my class, they looked at the statistics and they saw colleges in the local area and how many incident they were reporting, and it was generally less than a handful and we looked around and I could see-- and I could remember the stories-- that I had more students in my class who had told the throughout the semester that they experienced those issues then the entire schools in the local area had reported for the entire year. What that tells

me is that there's a lot of reasons that people don't necessarily come forward and there's a lot reasons why they don't report it because oftentimes there's a lot to lose. But if you think about it we have, by really focusing on trust building and really focusing on hearing people's stories, that we have a great opportunity to help explore and provide a real pathway to get the help that's needed.

But we also have to recognize that we can sometimes serve as barriers, and one of the things that I wanted to focus on was that I did a little personal experiment and basically what I saw is that I know the statistics around the revenge porn or the non-consensual sending of intimate images, which basically show that it's a very common issue. Chris referred to earlier, I think the statistics suggests that 1 in 8 social media users has experienced either threats or actual images being disclosed without their permission, we're talking about very high percentages. But what I noticed in my caseload is that only about 1 in 30 or 1 in 40 individuals were saying that they experienced this type of abusive behavior, and that was a little bit confusing to me and so I changed the way that I asked about it. And when I asked them in a different way where I took out some of the judgement, I brought the issue up myself and just asked them plain, without suggesting that what they had done is inappropriate, many of my clients have experienced issues where they're concerned about a video or a photo being sent around, is that something that you want me to possibly ask the court or law enforcement to help protect against?" And when I brought it out and I just said it and did it without judgment, I started seeing about a third to about half of the individuals that I talked to were sharing that they had that type of fear and type of concern. And so that sort of trust building, getting rid of our own fears and our own ideas about what's appropriate and what's inappropriate, can really help people to share in a more effective way the experiences that they are having.

The last thing, and I still think this has a lot to do with trust but trust in a different way and Chris kind of alluded to this, is that the people we are working with-- whether they are teenagers or adults-- have a lot of knowledge about their own lives. They know the abusive behavior and the abusive person way better than we do. And I found that when I'm able to actually bring them into the investigations to ask questions, to clarify, but also to point me towards what evidence they think is going to be most useful,if I clearly state what types of evidence, what type issues, I'm looking for, when I ask them to give me that information I found out they're incredibly helpful in identifying useful evidence and in being able to contextualize and give me a real feeling and flavor that I can express to law enforcement or the court about what that experience was like. And so, learning to trust people that we're working with, even if they are young, if they are 14 or 15 years old, is incredibly important and I think can make pay some serious dividend when you're talking about access to justice.

KRISTELYN:
In terms of how we address cases when the victim is on campus and the abuser is of campus, Chris do you have any thoughts on that?

CHRIS:
Well, working in the LA-based and being a very metropolitan area, I deal with a lot of different jurisdictions and I am fortunate that my agency allows me to pursue cases beyond just our campus borders. Specifically, I look at where the victim was when the offense occurs. If we are talking about cyber abuse cases, to me that means, where was the individual when they got the message or when they saw the post. And if I can build a nexus to our campus, like they were in class or at practice or studying in the library, I'm usually pretty free to work those cases. Since we are a commuter campus, mostly a lot of our student live locally, and I can pursue those cases myself. In instances where I can't, maybe the survivor is from Northern California or from an outside state, a lot of times what I will do as I will talk very candidly with a survivor and I'll let them know that there's not going to be a whole lot of investigative follow up that I can do on my end, and I try to refer them to the jurisdiction in which the crime occurred because ultimately that's where the crime happened and that's the area that needs to pursue it.

But what I've found, especially in the last couple years since we've been doing this grant and we've been really providing a resource and a place for individuals to feel safe enough to come forward, is that a lot of times the crimes occurred in local areas, but they feel so much more secure in reporting to the university police department and the other university resources on campus that they'll come to us often times first before they go anywhere near where they live. Sometimes that's a function of they just don't want their family to know about it just knowing that all the resources are all here in one place. And I explain to them that we obviously have no issues taking the initial reports. But in some situations, those reports will have to be turned over to the other agencies, agencies that would handle those complaints jurisdiction-wise, and so it's all about having an upfront conversation with the survivor and providing expectations for them to have. Some people might think "Oh I'm reporting it to the police, so it's going to get handled and it's done and over with", but there's all kinds of systems that are in the law enforcement world, ways in which we operate that are unknown to the community and might allude them, some of the finer points, so it's all about managing those expectations of the survivor. And if I can build some kind of nexus to our college campus, I'm lucky to have a lieutenant and chief that allows me to pursue those.

One case that particularly comes to mind is a revenge porn case where an individual was sending naked images through the mail of a former girlfriend. And it just so happened that he sent the images to a faculty member here on campus, and she was a student at the time and she had actually reported the incident to the local jurisdiction. But the local jurisdiction didn't take any action, and the mail was obviously reported to me and I identified the victim. And when I contacted her she said "Well I didn't know there was anything else to be done because I contacted my local PD [police department] and they said that there was nothing they could do, so I just thought I had to live like this so…,I found out that this individual had sent images to her church, her place of work, her mom, so really impacting her ability to lead her life with these kinds of traumatic incidents happening So what I was able to do is that because I built that nexus into that mail being mailed to campus and a faculty member opening it, I was able to pursue that case to the Thousand Oaks area where he was employed by another university, all the way to Northern California where he basically had his permanent residence and we were

able to get a conviction for revenge porn as a result of the investigation. for me personally and the way that my agency conducts our business it's very important that if we can build a nexus to a crime that occurred on campus then we can follow through to the best of our ability. And a lot of times that might involve individuals who are off campus, and if we can't personally oversee that investigation for that type of incident, being able to have great working relationships with our local communities and our local agencies is very important and paramount in handing off those kinds of cases. And knowing that those cases with be looked at, worked on, investigated with the same kind of vigor that we would if we did it ourselves. So, we have a very good working relationship with the Long Beach Police Department and with the LA County Sheriff's Department in that respect, and so that's typically how we handle cases involving off campus suspects in regards to cyber abuse or dating, domestic violence etc.

MARTA:
Ian can you talk a little bit about whether you've ever had a case where the abuser was actually someone anonymous, where the client was saying to you, I don't know who this person is, but they're harassing me, they're doing other things on social media. How do you handle a case like that?

IAN:
I think there's two issues there really, which is that it's quite common for somebody to think that they know who the person is, but that that person is using different types of technology in an anonymous way it can be hard to prove those things. The truth of the matter is that the ability to be anonymous has improved in many ways, It has become quite difficult in many cases actually identifying people. The interesting thing about technology vs. other types of evidence is that there is a great deal of metadata, which is the information that sort of lives behind what you actually see on the screen. That metadata can oftentimes be used to link people, but the problems with it is that it's very resource heavy and oftentimes requires giving access to devices, in ways that are hard to get access to either through a criminal justice system investigation where devices have been taken, so anonymous postings are very difficult to deal with. They are especially difficult to deal with in the civil system where it's hard to get subpoenas actually responded to by most of the large companies.

So what we tend to do and what we tend to suggest is, if there's resources to do forensic analysis and investigations and that's always a good addition. But in addition to that it can be really helpful to essentially really try to build out a picture of what's happening, if there's repeated postings or if there's spoofed calls, so somebody is hiding their number when they're calling or sending texts. We oftentimes tell people to go through the process of creating a log where you're identifying what time the occurrence is taking place, whether there were any things that you noticed that are kind of unique signifiers. So for example, I had an anonymous cases where the person thought that they knew who it was but was having a hard time proving it and what they were able to demonstrate was that this person, when they would make these posts, they essentially would write a sentence, put a space, they'd put a period, they'd put another space, and they'd continue to write another sentence, which is kind of an interesting way of writing and communicating. And so we were able to take that little seemingly insignificant thing

compare it with some other emails that she received from a person and that in addition to some contextual information within the posting, helped us to prove that it was in fact the person that she thought it was who was posting those images. So, getting a picture of it can be really useful. On techsafety.org --our online place for resources and our blog for the National Network to End Domestic Violence-- we do have a high-tech stalking log that people can use in thinking about that process. But I will just acknowledge that it is extremely hard nowadays to actually link people when they're making an anonymous posting. Even though the evidence is there it can be quite difficult to access.

CHRIS:
You know, I agree a lot about what Ian has to say. You know it is very difficult to get some of that information especially in the absence of a court order or a search warrant. A lot of times in my investigation I'm fortunate enough to get access to that information, I can find out communication logs, date stamps, timestamps. Sometimes I'm very fortunate to even get the content of communications, but at the end of the day we have to be able to identify the person behind the phone or the person behind the keyboard and so if a person is going out of their way to make themselves anonymous by using spoofed phone numbers or burner phones and things like that, then it's going to be really difficult for us to get a handle on who that person is. Thankfully the individuals that are committing these crimes of cyber abuse, dating and domestic violence, and sexual violence and stalking, they're not super interested in hiding who they are. So with the spoofed phone numbers and things like that, I've enjoyed very good success in being able to track those phone numbers back and getting actually identifying information.

Ian's absolutely right, it takes a lot longer. physical investigations of these cases can take days or a week or so. Especially if we are dealing with someone who is in custody, we have a very short window of time to deal with the investigation. But when we are looking at cyber abuse cases or cases that are very digital electronic heavy in evidence, we can be talking months. So we have to make sure that we're identifying the information and trying to get that evidence as soon as possible, but it is very lengthy in time.

And the one other thing that I wanted to point out is individuals that are being victimized over the internet or by an anonymous source, even though local jurisdictions might not be able to intervene or provide resources, the one thing that I do encourage people to do is to report it to the FBI on the internet crime complaint website-- IC3.gov. And while that specific response might not be answered by the federal government, what they do is they build cases and they look at trends and they see what's being reported and where it's being reported and so that if they do identify a significant trend, then they can work on it. So, my recommendation for a lot of individuals that are being abused or victimized from an anonymous source, is not only reporting to your local jurisdictions but reporting to the IC3.gov website, so that at least it's tracked on a federal level and we can investigate it that way.

IAN:
That's a really great point too because those reports also allow advocates to really push for Congress to provide more extensive resources-- to help get the resources necessary to respond

to some of these cases. And so that's why reporting, even if it may not have an immediate impact, can have some long-term benefits to survivors.

CHRIS:
Absolutely!

KRISTELYN:
And that's a really great segway to our last question. So what advice do you give to young people with whom you work with about gathering evidence on these various platforms?

IAN:

I really try to think about what it's like to have something on your phone that is threatening, harassing, emotionally concerning, and I really understand why people don't always want to maintain that sort of evidence. So, one of the things that I really push with clients is to say, "I get that, and I understand why that's concerning. Is there a way that we can maintain it, collect it, store it or put it aside, put into some kind of folder that allows you to keep it without having to deal with the constant burning sensation about that thing being present?" And we talk about that-- the same answer is not going to be available to everybody. I think different people are going to have different answers to that, and whether you need metadata or whether a screenshot might suffice that's also a serious question that needs to be talked through. I do really push the idea that I understand why people don't always necessarily want keep it.
The other thing, piece of advice that I regularly give, it's not uncommon for me to have clients come into my office and already have screenshots you know already have an image of some sort of inappropriate behavior-- many young people know how to take screenshots and do it. But what I frequently find though is that the information that they bring is not always the most useful. And that makes sense because people who are experiencing violence are not thinking through and primarily thinking about evidence collection. Their thinking about other things that are necessary to think about when you're dealing with a crisis. So one of the issues that comes up a lot is people bring to me a portion of a conversation that they think is the most relevant, but they don't have the entire conversation or they bring something that doesn't have a time or date stamp connected to it. And so the thing that we really push on one complete conversations because a court is always going to want to know that information, if you want to go down the criminal justice system process, which a lot of people do and it's a great resource for many survivors, there is important to maintain it in a way that the evidence can be collected in the best possible way.

Also, if there is a possibility for a date and time stamp, to keep that information.

And then the last thing is redundancy, redundancy, redundancy. So unfortunately it's not always clear how something is going to be able to be introduced into court, and it's good to have a couple different options. So in the civil context, and of course it's different and Chris can speak to this in the criminal court context, but in the civil context, it's very common for screenshot images to be introduced as evidence. And so what I will oftentimes suggest for young people to

do and for clients to do is to take a screenshot, to save that in a place that they know it's going to be secure-- whether it be a secure online place, a flash drive that they have control over-- but to also maintain it on a phone and on a device as well and If there is supporting evidence that you can maintain, also get that. So for example if you're dealing with an abusive or harassing text message you might want to also get your records from the telephone company to be able to demonstrate that this text was sent and received by you. So, having a couple of different ways to show law enforcement or courts about what happened to you is always going to be a good idea.

And lastly, its kind of goes without saying, you know all of us can get lost but document very rarely do. You have one incident of abusive behavior, there's oftentimes many many things that happen of varying degrees of severity, and it's easy to lose track of all of those things and so recording it in a safe way is really important because it's going to give, not only a little bit of texture, a little bit of understanding to whoever the factfinder is or law enforcement, but it's also going to make sure that you don't forget things that are really important. And so helping survivors to document that information is really, really important.

CHRIS:
Yeah Ian, I think you hit the nail right on the head. We don't want people to really delete anything because once you delete things, it gets really hard to recover that information. providing the information through various means and redundancy is always important because we don't know in what way we are going to be able to admit the evidence into court.

So I can think of one particular case where a screenshot for me initiated the cases, but it really wasn't the lynchpin. It was a case involving criminal threats where an individual had gone up to a student organization's Facebook page and had posted some significantly violent threats against the group of individuals, and it was all based off their perceived cultural identification. And what that group did was that they immediately deleted all these comments from their Facebook page because they didn't want their community to read it. And so understanding the reason why they did it and not judging them for it is crucial in those types of investigations because, like Ian pointed out, we want to maintain our trust with community members and condemning them or telling them that they made a mistake is not a good way to foster trust. But they were able to provide screenshots of the threat themselves and while powerful in showing the content of what was said it does absolutely nothing to prove who said it. Luckily we were able to work through the back channels and through Facebook and different evidentiary purposes to show that this individual did commit the crime. And it was interesting in the fact that this person deleted their user log. As a Facebook user I can actually delete my access log and if someone doesn't get to it within a certain amount of time that information is lost forever. So when I served the search warrant to Facebook, they gave me roughly 1600 pages of information from that Facebook Account. And interestingly enough I was able to see that this person had all this activity but had no activity on the specific day that the crime occurred. So in it of itself, it can be very suspicious, but still not proof, and sifting through all of these pages, I was able to find out that about 5 minutes before the threat was posted, that individual reached out and friend requested someone. So I didn't have any access logs for that day, but I had a friend request for

that day and around the same time of that threat and that was really the lynchpin for the case -- to prove that that individual that was sitting behind that keyboard or in this case a phone made those threats and that led to a very successful prosecution.

Again, the first key thing is to not delete the evidence. If we have to move the evidence from one location to another maybe we move it to a different folder on the phone, a different folder in the email, something that you're not having to look at all the time and be reminded of, **we are always cognitive of the fact that people don't necessarily want to report directly to law enforcement for a variety of reason and we're okay with that,** but we need to be able to maintain in such a way that when an individual does decide to come forward and report that we're able to legally access that information and do it in a way that's going to help us evidentiary-wise. So like Ian said, we don't want to cherry-pick our facts, so providing the whole conversation or all of the images or all of the emails is really important in proving intent and sometimes providing content of the cases that we're dealing with. So again, the biggest concern that I have is don't delete the information and if you must move the information, make sure that we do it in a way that's going to keep the entire piece of evidence together in ways that we are going to be able to recover easily. And again like Ian said, redundancy.

IAN:
I was hoping to add just one last thing that just came to me, particularly when I'm working with young people, though I don't think it's unique necessarily, but many people when they are about to engage in some sort of judicial process want to present their best foot forward and are really concerned that there may be something that they have said that will look bad for them But I also have found courts sometimes actually respond much better if you are just honest about the fact that you said a curse word or sent something that was less than flattering after somebody has done something repeatedly or really horrific to you. But again, saving the entirety of the conversation, even our little things that are not always as perfectly flattering to ourselves, can actually help your case rather than hinder it.

KRISTELYN:
Thank you both for those great tips for survivors

MARTA:
I learned so much from this conversation about building trust with clients, about acting quickly. about not blaming the victim because it's so hard for young people just to come forward with these kinds of cases to begin with. So, thank you again for being with us today,

CHIRS:
My pleasure

IAN:
Yes, it was an honor, thank you all!

KRISTELYN: Outro

The Cyber Abuse Project (CAP) addresses the use/misuse of technology in sexual assault, domestic violence, dating violence, and stalking (including cyber stalking) cases. CAP is a project of Break the Cycle and the CA Coalition Against Sexual Assault. And is supported by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the U.S. Department of Justice, Office on Violence Against Women.

Visit Break the Cycle's website at breakthecycle.org and CA Coalition Against Sexual Assault at calcasa.org to learn more about our work and CAP resources.