

WIRED SAFETY.ORG
Leader, Parry Aftab
ID #9848787
04/17/03

Date of Transcription: April 17, 2003

Valerie: Good morning. My name is Valerie, and I will be your conference facilitator today. At this time, I would like to welcome everyone to the WiredSafety.org Conference Call. All lines have been placed on mute to prevent any background noise. After the speakers' remarks, there will be a question-and-answer period. If you would like to ask a question during this time, simply press *1 on your telephone keypad. If you would like to withdraw your question, press #. Thank you. Mr. Wenderoff{phonetic}, you may begin your conference.

Mr. Wenderoff: Thank you. Good morning, and welcome to WiredSafety.org's conference call to discuss the results of a study on cyberstalking. Hosting the call will Parry Aftab, Executive Director of WiredSafety.org, and a leading internet lawyer and online safety expert. Her name is spelled P-A-R-R-Y A-F-T-A-B. Joining her are Kelley, a nurse and mother of two, who was a victim of cyberstalking herself before becoming Deputy Executive Director of WiredSafety.org; and Gambler, who heads up WiredSafety.org's security efforts. Due to the sensitive nature of the subject and for security reasons, we can only provide their first names. Kelley's name is spelled K-E-L-L-E-Y, and Gambler is G-A-M-B-L-E-R. If you have not received a copy of the release, or if you'd like a copy of the study, please call Judy Lee at (212) 515-1920. That's (212) 515-1920. Now, Parry, if you're ready.

Parry Aftab: I am. Thank you very much. My name is Parry Aftab and I've just been introduced. I donate my time, along with the thousands and thousands of other volunteers, in helping protect people on the internet. Two things have come up that have caused a particular concern in the area of cyberstalking and harassment. Cyberstalking harassment is not when someone's trying to lure a child into an offline meeting for sex; cyberstalking harassment deals with death threats. They may take your head and put it on a naked body on a porn site. They may offer you or your children up in a sex ad. They may attack you. There might be identity theft, where they pretend to be you. They may reach out to your boss or someone in your family or someone with whom you have a relationship saying horrible things about you. Sometimes you know about it; sometimes you don't. We have been working on cyberstalking help since 1995, and we have been working on cases and taking them one by one when they come in to us with special help volunteers, specially trained, who act as an intermediary sometimes between the victim and law enforcement and sometimes just helping the victim avoid

problems and make it go away without having to get law enforcement involved.

We've noticed some alarming trends -- some are alarming; some are interesting -- and we thought that we should start getting the word out to people who use the internet and people who can influence opinion on teaching internet users how to avoid problems online, how to use it safely, and what to do when things go wrong. We find that in the study most of the victims, as we had previously known, are women, minors, and senior citizens. In particular, people who are new to the internet -- who we, in internet terms call "newbies" -- are at greatest risk. What we did learn, though, is that although women are the greatest percentage of victims between the 18-34 age group, that in some age groups men are victimized more than women. We find that in minors, predominantly because minors tend to be cyberstalked by other minors and, frankly, boys are better at it than the girls are so far. We're also finding that men are cyberstalked at slightly older ages, and we are learning that the percentage of cyberstalkers who are women has increased from 25% of the cases reported to us in 2001 to 40% of the cases reported to us in 2002.

Because of the statistics we've gotten from the cases that have come to us, we decided to do a much larger survey; and that survey will be done in cooperation with the University of Southern Illinois and will be conducted online, and it will be the largest survey ever conducted about cyberstalking to date. That survey document will actually be launched on Monday and available at the WiredSafety.org site. If any of you have publications in your own websites and you want to make the survey available, there is a link. We're happy to provide that information to you, and we'll give you information on cyberstalking prevention as well.

The reason we've decided to release the survey this week as opposed to next month when we had originally intended to release it is because there has been an alarming decision in the DC District Court on a case that some of you may be familiar with. It's the Recording Industry Association of America v. Verizon. There is a law called the Digital Millennium Copyright Act (the "DMCA") that was designed and drafted in 1998 to deal with copyright infringements, and some of you may actually have had to use it to protect your own work. When

someone infringes on it, you can do what's called a Notice and Takedown by notifying the ISP where the website is housed, saying, "Someone's infringing on my copyright. Please take down that site until all of this is resolved." The ISPs can then look at the site and determine if it's a credible complaint and, if so, they take it down until it's resolved. There's an expedited subpoena process that's called the 512H Subpoena that allows the person who claims to have a copyright to notify in essence the web hosting company, saying, "I need to know who's behind that site, that storage facility on the internet, so I know who to sue." And by filling out a form at federal courthouse before a clerk -- just filling out a plain old form -- the clerk will stamp it, and it gets sent to the ISP that's hosting the website, and then they turn around and say, "These are the people who own the website." Well, since most website ownership information's public anyway, this is not anything that's terribly frightening to any of us. Somebody's looked at it and determined that there's an infringement -- that is Mickey Mouse on the screen or that is Spongebob Square Pants or Britney Spears.

However, the Recording Industry Association of America sent a subpoena to most of the ISPs, several subpoenas, saying that, "People are infringing the music by using peer-to-peer process." That's like Kazaa and Morpheus process, which actually houses the music that's being loaded onto other computers on your own home computer. So technically your computer becomes the storage facility, and because of this loophole, they went to court and sought to subpoena information about internet subscribers -- the users of the ISP. Who owns that computer? Where do you live? What's your telephone number? What's your name? Verizon for some reason I still cannot figure out has fought the subpoena.

When we heard about the case at Wired Safety, we became very concerned because this judge determined that an ISP is an ISP is an ISP, and if they have to give you information about who owns the website, they have to tell you who the subscriber is if that computer is located in your home. I became very concerned because the people who are cyberstalked the most and are at greatest risk are women, especially battered women who have been harassed by former romantic relationships or imagined relationships, predators who are trying to find where children live to meet them in real life, and others who need your address and telephone number in order to be able to commit identity

theft. We're also particularly concerned because we work quite closely with law enforcement. In fact, many of my volunteers are law enforcement. One of my volunteers on the phone with us is a member of law enforcement with the sheriff's office. {Tone interruption} concerned that undercover operations will be at risk if all somebody has to do if they think there's an undercover operator in a child pornography room or a sexual predator pedophile chat room is just fill out this form and find out who's behind it.

So because of this, we thought it was important that we started to elevate the attention to cyberstalking itself and harassment and teach people how to surf safely, how to cyberdate as safely as possible, and how to preserve their privacy online.

Now, Kelley, you are -- in addition to being our Deputy Executive Director -- you are a victim of cyberstalking yourself at least twice.

Kelley: That's correct.

Parry Aftab: Can you share a little bit about your situation?

Kelley: Yes. The first time I was cyberstalked was back in 1995 when I had originally gotten the internet to communicate with a good friend who lived 3,000 miles away and I started using a chat program to do so; and we would have prearranged times and I got into visiting a general chat channel where if someone was paying me a lot of attention and asking very basic questions about the difference in our cultures and such, I didn't think much of it until the next time I logged on when that person appeared -- immediately as soon as I logged on -- and started messaging me. I tried ignoring, I tried being angry, all of those things, to get this person to disappear and that didn't happen. It continued for three to four months with upwards of 50 to 100 emails a day. And I was absolutely terrified. I had no computer training whatsoever. The local police had no idea what to do other than to tell me to turn my computer off. I had no idea where this person lived -- if they were across the world or across the street. I finally was able to do some searching on my own and find some assistance with our organization and finding out that I had inadvertently, being a new computer user, made my private information available to others who were a little bit more computer savvy in how to retrieve it. They assisted me in

changing that information as well as tracing the person to Turkey -- which eased my mind some in the fact that he wasn't across the street. I was able to stop the stalking, and I continued on with the organization to help other innocent people using the internet avoid this problem.

I was then cyberstalked again a couple of years back. While working in the capacity of Wired Safety and assisting, we had had a very dramatic increase in the number of cases come in and I was assisting our team in trying to get a handle on them and answer them in an appropriate amount of time; and a person had emailed about a flame war, which is basically an online argument, so I did the investigative work behind it and checked the site and notified this person that it really wasn't a cyberstalking situation and how this person could end it -- not realizing that his person was disturbed and this transferred his attention from this website to myself, finding a lot of information about me. And the biggest fear -- it went on, like I said, for two years -- the biggest fear was when he was able to access my personal website and pictures of my family and was threatening to take pictures of my daughter, who was seven at the time, and post them into the pedophile use net postings with my identifying information as to where I lived and such so that pedophiles would have access to her, knowing where she lived as well. And that's when things finally came to a head. He had also been going after Parry towards the end of this and we were, thank God, able to get law enforcement to act on this because he was making death threats; and, it turns out, he's a very disturbed young man.

Parry Aftab:

And Kelley, as trained as she is in helping others, the first thing you need to do is to ignore the cyberstalker because any attention inflames them unless you have a personal relationship with them offline, and then nothing you're going to do is going to make a difference. But when someone starts threatening your 7-year-old, announcing that they're going to tell everyone where you live and put your daughter's picture up there so they can find her, even the best-trained volunteers will start to panic. This person was a 24-year-old from New York, and when police knocked on his door found him in Pokemon pajamas. This person is not stable. And these are the people that you're really worried about, and all they have to do is fill out a form in a federal courthouse before a clerk. No lawsuit has to be commenced. No proof of ID has to be given. They can even use a P.O. box and they

can find out exactly where she lives. Luckily, he hadn't gotten closer than just her down; but, in a small town, that's enough. Gambler?

Gambler: Yes?

Parry Aftab: You, I know, work with the sheriff's office so you see the law enforcement side of this, and you also work our cases so you see some pretty heinous cases. Could you tell me why you're concerned about anyone being able to get the personally identifiable contact information of anybody they want online?

Gambler: There are several reasons. First, it gives them a heads-up how they can get into the person's phone calls. They can start calling the person at home instead of email. They can immediately take it offline and they can have the home address and start mailing things to them -- mailing letters, mailing packages -- or show up at their house if they're within reasonable distance.

Another one that concerns me also is the fact that if law enforcement needed the same information, there are more steps we have to go through before an ISP will release it to us. An individual can go up, lie to a clerk, and get the subpoena right away. It takes law enforcement sometimes up to two weeks to get the same information.

Parry Aftab: Now does law enforcement have to go to a judge to get the subpoena?

Gambler: Either a judge or a district attorney or a state's attorney.

Parry Aftab: All right. So it's something that requires a Grand Jury in many cases, and typically a judge to determine whether or not you're going to get the subpoena to find out who's behind it?

Gambler: Correct.

Parry Aftab: And to do that, you have to have reasonable cause to believe that a crime has been committed?

Gambler: Correct.

Parry Aftab:

So this really gives any predator who wants to a leg up over law enforcement as well. Gam, I know you've worked a lot of cases and you've seen some deadly things. The two cases I recall the most are one where a little girl wrote "hello" on a neighbor's sidewalk and he became angry enough that he went onto the internet to child molester chats, posing as the little girl who was then nine, and said that she was having sex with her daddy and she wanted to have sex with other men like her daddy, and this was where she lived and her telephone number. So when her parents started getting phone calls at 3:00 in the morning and drive-bys looking for their daughter, they had no idea what was going on. Luckily, one of the people who was calling explained that he was just calling in connection with this ad. That person was fined \$750 and nothing else happened. Another case was the case in California where a woman's address was posted in an S&M chat room saying that she was interested in gang S&M sex, and her address was given out, and people showed up at her front door. So that what people think in terms of "sticks and stones may break my bones, but words will never hurt me," we're talking about giving out personal information on people who may not like you because you are the wrong color or the wrong racial background or the wrong gender or you said the wrong thing. They may attack you because you're a cancer survivor. They may try to find you because you're a child. There are a million reasons that people who are out there who are disturbed would try to get to you, and the last thing you want to do is make it easier. Could you share a case with us, Gam, other than the ones I just talked about? One particularly that alarms you?

Gambler:

One that particularly alarmed me was I caught someone hacking. They were hacking a law enforcement agency near me. I turned them in, got them arrested. While they were in jail, they had traced back to my phone when I was calling in, and they called my house from jail to threaten my life. I turned around and called the jail right back and said, "Your phones are recorded. I know that. Play that back." They did.

Parry Aftab:

That's the last thing a law enforcement worker would want is to have anybody know where he lives, especially in a jailhouse. So this could be very frightening.

Gambler:

That was an extreme case. We have them every day where people just start hacking someone to get more information. They're trying to do an

identity theft. They'll try to get into their computer to see what their name is, what their social security number is and all that information. Well, with this DCMA, all they have to do is fill out some paperwork at the clerk's office and send it in and they don't have to hack at all.

Parry Aftab: We don't need high level hackers any more to get into our computers; we've got somebody who can get it through a law.

Gambler: Exactly.

Parry Aftab: I think we are ready for questions, if anyone has any. I'm happy to answer any questions. In just a moment, we'll have the operator come in and tell you how to do it. But one of the things we suggest is just for people to Google themselves. Kids understand what that means and, yes, you can print it without being censored. Googling yourself is going to Google or any of the other search engines and typing your full name in quotes and seeing if you appear online. Type in your children's names or people you care about, and sometimes even the people you don't like at all, you're just curious where they are. Put in your telephone number in quotes and your address in quotes, and see if you're listed online. That's sometimes the first way of finding out whether someone has stolen the identity or whether you're the victim of cyberstalking and you're just the last to learn about it. So, if the operator's still on, maybe she can tell us how we can hear some questions and answer them.

Valerie: If you would like to ask a question at this time, please press *1 on your telephone keypad. We'll pause for just a moment to compile the Q&A roster.

Parry Aftab: There is additional information at WiredSafety.org. We're the world's largest internet safety and help group. We're all unpaid volunteers. We're a 501(c)(3), and we run three major sites in addition to Wired Safety: Wired Patrol that deals with our net patrol, our cyberstalking team that defends people online; our child exploitation team that finds and reports child pornography sites and child molesters online and helps people when things go wrong in packing{phonetic}. We have our Wired Kids which teaches children and their parents and teachers all about internet safety. And we have our Cyber Law Enforcement

division which has our law enforcement volunteers that both train and assist law enforcement on the ground in cyber investigations.

Kelley: And the survey is up, Parry, just to let you know.

Parry Aftab: Oh, thank you very much. So if you go to WiredSafety.org or WiredPatrol.org, you will see a banner that talks about cyberdating and cyberstalking and, if you click on it, it will give you the actual numbers of our study and information about safety tips and what you can do to avoid it, as well as cyberdating and how you can do it as safely as possible.

Valerie: Your first question comes from Drew Clark of "National Journal."

Drew Clark: Yeah, with "National Journal Technology Daily." Two questions, Parry. The first, did you say that you were surprised that Verizon fought the subpoena? Could you elaborate on that? Were you being sarcastic?

Parry Aftab: No, I was serious. I mean, all of the other ISPs had just caved and given away the information of their accountholders. I do not see a real reason for Verizon spending the amount of money they are in the fight on fighting this other than the fact that they think it's right. And, you know, I'm a child of the '60s. I don't see corporations spending a lot of money on what they think is right terribly often, so I'm delighted in this case.

Drew Clark: Uh-huh.

Parry Aftab: They fought it, and it's costing them -- and I'm hurting them I'm sure on a lot of different fronts -- but they're taking a stand to protect the privacy of their own subscribers. I intend frankly, when this is over, to move my account over to Verizon, because if they're going to protect my privacy, I want to give them my business.

Drew Clark: Uh-huh. Could you talk about the Justice Department's decision to weigh in on the Recording Industry's side? Could you just talk -- you and Gambler; and, by the way, is that your real first name?

Parry Aftab: No, Gambler's his code name. He's the head of our security. Kelley uses her real first name because she does media for us. Gambler normally doesn't. This is a special exception, and Gambler is his screen name; it's his security name.

Drew Clark: And is Gambler a law enforcement officer?

Parry Aftab: Yes. He works with the sheriff's office. We can't tell you where.

Drew Clark: A sheriff's office in some locale.

Parry Aftab: In the United States.

Drew Clark: So could you talk about the Justice Department's decision to side with the Recording Industry here and whether you or Gambler or other people in the law enforcement community have had talks with the Justice Department to try to get them to see your side of the story?

Parry Aftab: Yes, I can answer that. I actually met with people within the juvenile justice area of the DOJ last week, with whom I deal with on a regular basis. When we're dealing with children and sexual predators and child pornography, it comes out of that group. They had actually not even known about this case. They hadn't had a chance to weigh in on protecting children at all. So I'm concerned that DOJ's decision to weigh in and to weigh in in support of the Recording Industry Association of America is done without the full input of the other areas of DOJ where they understand the significance of serious security and privacy significance of this ruling. I think that the Recording Industry Association of America has done a good job on trying to paint the picture, but I don't think they painted the right picture. They've said it's all about copyright; but it's not about piracy here. I mean, I can protect the copyright holders very well. I'm an internet privacy lawyer and, frankly, I represent many members of the entertainment industry. You can protect them without putting people at serious risk, and that's just by telling them to go to a court and file a John Doe lawsuit and then they can get a subpoena the way anybody else can. And if it's abused, we have legal process to deal with; as opposed to somebody just walking into a court clerk's office. So I am hoping that the Department of Justice understands and listens to the other departments that recognize the serious risk that all internet users are put under under this ruling if it's

read that way. It's not a matter of filling out the DMCA; it's a matter of hopefully overruling this particular judge who I think misread it and tried to apply a technology that came out in 2000-01 to a law that was written in 1998. Peer-to-peer did not exist when the DMCA came out, and I believe, having reviewed the law and the legislative history, that it never ever would have been used under this *ex parte* subpoena that doesn't even require a lawsuit to commence it.

Drew Clark:

Okay, thanks.

Parry Aftab:

So hopefully this press conference and our study will help bring this to DOJ's attention. I know there are many, many other groups that deal with internet safety, especially battered women, who are particularly concerned about this; and I just think it's a matter of oversight.

Valerie:

Your next question comes from Brooks Boladic{phonetic} of Hollywood Reporter.

Brooks Bolic:

Are you there?

Parry Aftab:

I'm here.

Brooks Bolic:

Yeah, it's Bolic. I've been out of town. When did Bates rule? I don't think he's ruled yet. I think the case is still before Bates; he just had another hearing on it two weeks ago.

Parry Aftab:

Well, the hearing is on the stay. He has already ruled that Verizon should turn it over. The only issue before him now is whether his decision on them should be stayed. --

Brooks Bolic:

Oh, yeah, to stay on further appeal.

Parry Aftab:

-- subpoena is stayed or not.

Brooks Bolic:

Okay. Has anybody -- any stalker -- ever used a DMCA subpoena?

Parry Aftab:

To my knowledge, not yet, because no one has tried to use the 512H subpoena *ex parte* until the Recording Industry Association of America just did. No one's ever done it before. It's never used in a peer-to-peer situation until very recently. But you know my concern -- and

when we came out on this media -- I had a concern because I knew once I came out to try to fight this that I may be educating people who I don't want to know about this loophole, that it exists. But hopefully if this decision is upheld, someone on Capitol Hill will look at this and recognize that this is not an application that was ever intended and somebody'll fix it. As I've indicated, we can protect piracy very, very strongly without risking privacy.

Brooks Bolic: Yeah. The copyright companies have a different view, of course.

Parry Aftab: As an internet lawyer, I've represented many companies on copyright issues.

Brooks Bolic: And I have another question that's slightly technical. Who backs your group?

Parry Aftab: We're nonprofit. We're a 501(c)(3). We're backed by the public.

Brooks Bolic: Where do you get your money?

Parry Aftab: Most of the funding is mine. AOL is a contributor. NEC Foundation is a contributor. Disney is a contributor. We have only had \$100,000 worth of contributions.

Brooks Bolic: Okay.

Parry Aftab: We've gotten some from a private citizens' group on our September 11 work, but we do not have money from Verizon.

Brooks Bolic: Okay.

Parry Aftab: And all of our volunteers are unpaid, which allows us to operate on a small budget.

Valerie: Your next question comes from Patrick Ross of *Washington Internet*.

Patrick Ross: Yes, it's *Washington Internet Daily*. I wanted to ask you, you mentioned that you were cautious about going forward with this because you don't want to give people the wrong idea; but it seems that you could also be educating these court clerks that maybe they

shouldn't just sign off on any Joe that walks in off the street. If you're an attorney for a record company, there's going to be a certain expectation that this person has probably not participated in cyberstalking; but if I were just to go in there and make some bald claim, I would think that there might be some restraint.

Parry Aftab: You know, I love that idea. I'm not sure that legally the court clerks have the ability to decide which subpoena they're going to stamp and which ones they don't. The only choice they have is, is the application complete or not? But I think that's wonderful and, hopefully, some court clerks out there are listening.

Patrick Ross: Well, let me ask you a further question then because I'm not an attorney. If I'm an ISP and I get one of these 512H's that frankly does not look like it's from a record company, but I can't even tell who this person is or why they're asking for it, is there any kind of mechanism in the DMCA that would allow the ISP to raise a flat?

Parry Aftab: No, there isn't. And the only thing that can be done is what Verizon did here, is just say, "You know, I'm not gonna comply with this subpoena and move to quash," and that means Verizon, in this case, had to bring the first lawsuit on this case. So there's no discretion on the part of the ISPs. If there was discretion on the part of the ISPs or the court clerks, I would feel more comfortable; but there isn't any, and I don't know that that's really something that would work.

Patrick Ross: Have you been talking to Verizon at all? You mentioned you've been talking to some people in the Justice Department.

Parry Aftab: Right. I talked to Verizon -- actually, I'm on the Board of Trustees -- and when this issue arose and the board was looking at this issue and the privacy implications, I asked for someone to reach out to Verizon. I made a phone call to Verizon and looked into this and told them that I was very concerned. Frankly, I think they were surprised that a nonprofit group would become active. And we're not a politically active group. We stay out of politics; we just protect people and we protect them all over the world. This is the first time we've taken a position that could be seen as political or a legal position, and it's something that we feel we have no choice but to take.

Patrick Ross:

Right.

Parry Aftab:

Because this is a serious, serious issue. I cannot teach people how to protect their privacy online when they're doing everything right and some bad guy out there goes into a court clerk's desk and fills out a form and can find out who they are anyway. I don't know how to protect people from that.

Patrick Ross:

Okay. Thank you.

Valerie:

There are no further questions at this time.

Parry Aftab:

All right. Now let me give you my email address. I have no life. I'm online most of the time. My email {tone interruption} is my name so it's Parry, P like Peter, A-R-R-Y at Aftab, A, F like Frank, T like Tom, A, B like boy, dot com (parry@aftab.com). You can send me an email. You can go to Wired Safety -- WiredSafety.org is the umbrella page. You can send an email to me there; I read all of my own emails. You can reach out to Gambler at Gambler@WiredSafety.org or Kelley, K-E-L-L-E-Y, Kelley@WiredSafety.org. And we're happy to answer your questions. If there are individual interviews you want to do or something else you want to follow up on, let us know. If you want to see the study that you can publish, you can use these things at your site, we're happy to help in any way. We are not biased against the recording industry. I'm very active within the recording industry as a lawyer, and that's why I think that if people are being smart, we can come up with a solution that doesn't put people at risk but also protects copyright owners, because we don't condone criminal activity by anybody even people who are infringing copyright. So come to our site and we'll give you more information. Send us an email. We're happy to talk to you by phone or otherwise. And let's help spread the word and keep people safe. Thank you very much.