Q: Can you explain why the term revenge porn is problematic and which term Without My Consent uses?

A: “Pornography” is generally understood to refer to an image or a video of people who are in various stages of undress. The term “revenge porn,” typically used by the media, does not encompass all of the issues associated with these images, i.e. when they are used without the consent of a victim, whether they were shared in the context of an intimate relationship or the image was obtained through some unauthorized means. The term “revenge porn” implies that a scorned lover shared the image, perhaps because they are trying to exact revenge. We use the phrase “nonconsensual distribution of sexually explicit images” or the term “nonconsensual pornography” because it is more accurate as to what is really happening in these situations, and it recognizes that individuals are victimized in a variety of ways. There are many ways in which sexually explicit images are posted without the consent of the person in the photo. For example, a person’s cell phone or computer may be hacked, and their images are put on the Internet through illegal means or an image may be shared with one person, who shares it with someone else,
who then posts the image online. There may not have been an ill intent in sharing the image originally, but the image is now on the Internet. Unfortunately, there is now a cottage industry based around the distribution and sharing of nonconsensual pornography. Some websites will post a victim’s image or allow third parties to post a victim’s image. When a victim contacts these websites to have the images removed, the victim may be asked to pay to have the images taken down. This is an extortive model that further harms victims.

Q: Is there a particular population that is experiencing this?

A: This issue affects people of all ages and backgrounds. As an organization, we receive emails from women and men across the United States and abroad and from individuals of diverse socioeconomic and educational backgrounds. This issue does not discriminate. Anyone who is online, uses social media, or uses another form of Internet technology is vulnerable to this type of cyber exploitation crime. In addition, people who do not use social media are also vulnerable: a perpetrator could easily access their device, steal an image, and distribute it without their knowledge.

Q: What has been happening on a legislative level?

A: Currently, 34 states have adopted digital abuse, online harassment, or nonconsensual pornography laws. As recently as 5-7 years ago, the nonconsensual distribution of sexually explicit images was not specifically laid out in many harassment statutes. Now, there are laws that are very specific about online harassment. Specificity makes it easier for attorneys to demonstrate to the court why the behavior is illegal. Lawmakers in California recently determined that victims of the nonconsensual distribution of intimate images can seek assistance from any police department or law enforcement agency within California, regardless of which jurisdiction they live in or where the crime occurred. This is a big step because victims often do not know where to start or where to go for help to report the crime. It is discouraging as a victim to go to law enforcement and be told they cannot help because of jurisdictional issues. Further, in 2015, former California Attorney General, now U.S. Senator, Kamala Harris formed a Cyber Exploitation Task Force and invited different nonprofit organizations, victims, and technology companies to work together to provide victims, law enforcement, and a variety of other stakeholders with resources. They also worked to support tech companies to create avenues that would make reporting harassment and abuse incidents on their platforms easier. In addition, U.S. Representative Jackie Speier (D-CA) has introduced the Intimate Privacy Protection Act that would criminalize nonconsensual pornography on a federal level. This is critical to meeting the needs of victims in the 16 states without online harassment laws and harmonizing the approach to combatting this form of cyber exploitation.

Q: How have Twitter, Facebook, and the other technology platforms responded to this issue?

A: One of the most important steps these companies have taken is to provide victims with a direct access portal to report abuse. One of the biggest hurdles for victims is reporting abuse and obtaining a result, such as an image being removed. They lose hope if nothing happens, however these new portals increase the likelihood the nonconsensual content will be responded to by someone within that company. Internally, many of these companies are trying to figure out what their policies should be around digital abuse and harassment and taking a conscientious approach to developing policies to adequately address cyber exploitation. Many of these platforms have to be very careful about removing content from their website, due to provisions such as Section 230 of the Communications Decency Act, from which they derive immunity from liability for user-generated content. If they want to remove a user who is engaging in harassment from their platform, they
can lean on their policies to remove the user and the content.

Q: Do you have tips for professionals who are working with victims of stalking and what they need to know about this issue?

A: When working with a victim of this crime, the most important first step is to document all of the evidence involved. This includes information related to the devices used, the content, and the platforms it has been distributed on. Then create a detailed account of who the victim thinks is involved and how the content may have initially been distributed. It is important to take screenshots and collect and save all of the evidence as soon as the crime is identified. It is also important to construct a chronology of events. The more details you are able to record, the easier it will likely be to engage in legal processes to achieve justice for the victim. Professionals may also have a role in helping victims understand the importance of having legal counsel who are familiar with online harassment laws, how technology is used, and different options for having content removed. Good legal counsel will also take the time to understand the victim’s goals. Most often, the first priority for victims of nonconsensual pornography is getting the content off of the Internet. This often requires engaging the court system to obtain a restraining order or some other form of civil harassment order depending on your state. One question that is frequently asked is how one can avoid becoming a victim in the first place. This is a tricky question. While it is easy to say do not create the content in the first place, that is not fair since privacy law protects your right to do so. As an advocate, we are working to update laws constantly to protect people from nonconsensual acts perpetrated against them. Of course, a preventative measure is to not produce or share content, but victims should not be shamed for doing so. I advise, when engaging in any activity with a connected device or on the Internet, that individuals understand the technology they are using, the policies of these technologies, and are aware of the sharing capacity of social networks and their storage policies, whether it be Snapchat or Facebook.

Q: Do you see this intersect with a lot of other crimes, such as domestic violence, sexual assault, or stalking?

A: Yes, nonconsensual pornography is a tool for perpetrators of abuse, and we see it used in both violent intimate partner relationships and as a stalking tactic. In some situations, the perpetrator is the only one who has access to or control of the technology. They may coerce the victim into taking nude images to use as a control mechanism, thereby creating a power dynamic. With the traditional justice system, you apply for a domestic violence restraining order or a civil harassment order in order to stop the harassment. Yet, this may not adequately combat online harassment. There is a need for stronger, more comprehensive and constitutional laws that balance the right to free speech and protection for victims of cyber exploitation.