

Stop Trafficking! AwarenessAdvocacyAction

Anti-Human Trafficking Newsletter • October 2025 • Vol. 23 • No. 10

FOCUS: The focus of this month's newsletter is on the increasing use of Deepfakes and their role in exploitation.

Artificial Intelligence (AI) systems have empowered people to work more efficiently. But cybercriminals abuse this same technology to produce Deepfake nudes and create audio, videos, and images that are fake but look and sound realistic.

Deepfakes are photos or videos that have been manipulated to depict an individual doing something they did not do. To create a Deepfake, old data and new data are blended to produce something fake. Facial-recognition software is becoming so advanced that any person can be put into a Deepfake image. For example, a child's face can be placed on another person's body to create image-based sexual abuse.

Deepfake technology, once primarily associated with political disinformation and entertainment, is now being misused in schools and elsewhere as an insidious form of cyberbullying. Unlike traditional bullying, Deepfakes allow for the creation of realistic but counterfeit sexual content depicting students in made-up and harmful compromising scenarios.

Deepfakes can also be made by so-called "undressing apps" in which a person uploads a picture of a person, and the app generates a fake nude photo. Cases using these apps have sprung up at middle and high schools around the world, with teen girls frequently being victimized by their male classmates. Recently, the **FBI issued a warning** to parents and anyone who posts pictures on social media after a "back-to-school" photo turned into a Deepfake. The FBI also issued a warning that sharing such imagery of minors is illegal.

The production of nonconsensual, sexually explicit Deepfakes has increased significantly in the past 2 years. These are often used as tools for blackmail, harassment, or public shaming, causing trauma, anxiety, loss of personal trust, reputational damage, and even withdrawal from social or professional life for the victims. The misuse of Deepfakes can take many harmful forms, including financial fraud, emotional manipulation, and technology-facilitated sexual abuse. The deceptive nature of Deepfakes not only violates personal privacy and safety but also underscores the urgent need for strong legal protections and technological safeguards.

Human Trafficking and Deepfakes

The rapid advancement of Artificial Intelligence (AI) technologies, particularly Deepfakes, introduces alarming challenges in the fight against human trafficking by facilitating exploitation, abuse, and recruitment. According to the Law Journal for Social Justice, traffickers can use Deepfake technology to create convincing fake images or videos of victims for commercial sexual exploitation online. Deepfakes also contribute to the production and spread of child sexual abuse material (CSAM).

Recognizing the challenges posed by these technologies is essential for developing effective support systems for victims. The realism of Deepfakes makes it incredibly difficult for victims to prove that the



Human Trafficking and Deepfakes (cont.)

pictures or videos are not authentic, potentially exacerbating their trauma and hindering their ability to seek help. By understanding how traffickers manipulate these technologies, we can better prepare ourselves to recognize and counteract their tactics.

The rise of artificial intelligence has also profoundly impacted the fight against sex trafficking, offering law enforcement new tools. However, as of today, the rapid development of AI has outpaced the legal frameworks that govern it.

Deepfakes are also used in revenge porn, which is often motivated by a desire to get back at a former partner. Revenge porn is used to seek power over or bully the subject of the images.

The Role of Deepfakes in Sextortion

After Elijah Heacock, a 16-year-old Kentucky teenager described as "a vibrant teen who made people smile," died by suicide this year, his parents discovered he had received threatening texts demanding \$3,000 to suppress an Al-generated nude image of him. He was just one of thousands of American teens and preteens targeted by digital blackmail.

Elijah's death also called attention to how advancements in artificial intelligence, like Deepfakes, "nudify" apps, and Al-generated pornography, raise the stakes on the crime of sextortion, when individuals are blackmailed after sending compromising photos, texts, or information to someone who turns out to be a scammer. Perpetrators using Deepfakes in sextortion take ordinary pictures from social media and manipulate them to create fake, explicit images.

The perpetrator then demands money to prevent the distribution of Deepfake content featuring their image in sexual positions. The impact of these scams extends far beyond financial loss. Cybercriminals create Deepfake materials that tarnish the victim's reputation. They prey on the fear of public humiliation. This fear often drives victims to act quickly, as they want to avoid a scandal. Most victims of sextortion are males between the ages of 10 and 17, although there have been victims as young as seven, and girls have also been targeted. Sextortion is a federal crime with a punishment of up to two years in cases with adult victims and up to three years in cases with victims who are minors.

AI-Powered Image Generators: Perpetrators employ advanced software designed to alter images. Two common types of these tools are Autoencoders and Generative Adversarial Networks (GANs). These programs can analyze data sets of faces and make new images that look real.

Social Media Scraping: Platforms like Instagram and Facebook are filled with personal photos. These images, often shared publicly, become easy targets for people looking to create Deepfakes nudes. By collecting pictures from these sites, scammers have a rich source of material for their projects.

Anonymous Hosting Services: Once the nude Deepfake is created, it needs a safe place to be stored. This is where anonymous hosting services come in. These platforms allow creators to upload their content while hiding their identities and often do not comply with The Digital Millennium Copyright Act (DMCA) practices for handling copyright infringement on the internet.

Digital Forensics Corporation

On July 17, 2025, the **FBI warned** of an 'alarming number of suicides'
associated with blackmail using AI-powered 'nudify' apps.

Synthetic Pornography

Another form of media that can lead to virtual imagebased sexual abuse is synthetic pornography (SP), which is different than Deepfakes in that Deepfakes include actual people's faces and identifying characteristics on bodies other than their own, while synthetic pornography involves AIgenerated, non-actual bodies engaging in sexual activities. Despite SP not showing actual children's faces, it is important to know that this form of media can still have children's bodies in it and can potentially be harmful.

41% of women between the ages of 18 and 29 self-censor to avoid online harassment.

Online Harassment,
Digital Abuse, and
Cyberstalking in America

Members of Congress Affected by Deepfakes

Last December, more than two dozen women members of Congress and one congressman, representing diverse party affiliations and geographically dispersed areas, fell victim to sexually explicit Deepfakes. The victims were neither affiliated with one party nor geographically connected.

The American Sunlight Project (ASP), a think tank that researches disinformation and advocates for policies that support democracy, released findings last week that identify more than 35,000 mentions of nonconsensual intimate imagery (NCII) connected to members of Congress. ASP did not release the names of the legislators to avoid fostering searches for the images. They contacted the offices of everyone impacted by the images to alert them and offer resources on online harms and mental health support.

ASP noted that the images were removed relatively quickly, a fact they stated does not usually occur to women impacted by Deepfakes that are not members of Congress. They also noted that removals do not prevent material from being shared or uploaded again. ASP also pointed out that the harms of AI and Deepfakes disproportionately target women and marginalized communities.

Nearly 16% of all the women who currently serve in Congress — or about 1 in 6 congresswomen — are the victims of Al-generated nonconsensual intimate imagery. ASP also warns that Imagebased sexual abuse can have devastating mental health effects on victims, who include everyday people who are not involved in politics, including children.

"Over 90% of all Deepfake videos made are nonconsensual sexually explicit images, and women are the targets 9 times out of 10."

-Alexandria Ocasio-Cortez who has been targeted with such

Deepfakes herself.

• • • 3



Are Deepfakes Illegal?

It is illegal to use Deepfaked voices in robocalls, per a 2024 FCC ruling. In general, criminal impersonation laws that make it illegal to impersonate, say, a doctor or government official, may apply to Deepfakes. Otherwise, even in the entertainment industry, which has dealt with Deepfake issues for a relatively long time, the laws are behind the times.

The U.S. Copyright Office considers AI-generated works on a case-by-case basis and welcomes public input on these issues as free speech protections usually apply to Deepfakes as long as they do not encroach into defamation, obscenity and fraud. For more information, go to the National Conference of State Legislators.

2024 Deepfake Statistics from **Security.org**

According to a McAfee survey, 70
 percent of people said they aren't
 confident in their ability to distinguish
 between a real and a cloned voice.



That said, 40 percent of people in the same study reported they would help if they got voicemail from their spouse who needed assistance.

- Criminals can use a small snippet of a person's voice to target the person's loved ones for financial gain, perhaps staging a situation where they appear to need help in a difficult situation. One in ten people report having received such a cloned message, and 77 percent of these individuals lost money due to scams.
- According to Google Trends, searches for "free voice cloning software" rose 120 percent between July 2023 and 2024. Users don't need a lot of technical skills to generate manipulated audio with these free apps.
- Three seconds of audio is sometimes all that's needed to produce an 85 percent voice match from the original to a clone.
- False news, lies, or rumors can spread faster than truthful news, which explains how Deepfakes can be so effective. They evoke emotional responses and provide new insights. In one study, the top 1 percent of rumors on Twitter (now X) reached between 1,000 and 100,000 people, while truthful news rarely reached more than 1,000 people.

The DEFIANCE Act

The Disrupt Explicit Forged Images and Non-Consensual Edits Act (DEFIANCE Act) of 2025 is a proposed piece of US federal legislation aimed at combating non-consensual intimate digital forgeries, often referred to as Deepfakes. The Defiance Act defines a nonconsensual sexually explicit Deepfake as a "visual depiction created through the use of software, machine learning, artificial intelligence, or any other computergenerated or technological means to falsely appear to be authentic" that "depicts the victim in the nude or engaged in sexually explicit conduct or sexual scenarios."

The bill would grant survivors the right to take civil action against individuals who knowingly produce, distribute, solicit, receive, or possess with the intent to distribute nonconsensual sexually explicit digital forgeries. The statute of limitations for the remedy is 10 years. The bill text is available here.

"Sexually-explicit 'Deepfake' content is often used to exploit and harass women and girls, and no one should have their privacy and autonomy violated by someone else generating explicit AI-generated content of them. Although the imagery may be fake, the harm to the victims is very real. Victims have lost their jobs, their reputations, and many have suffered from life-altering depression or anxiety. By introducing the DEFIANCE Act, we're giving power back to the victims; cracking down on the production, receipt, distribution, and possession of 'Deepfake' images; and holding those responsible for the images accountable."

-Senator Durbin in reintroducing the DEFIANCE Act

The Take It Down Act

The TAKE IT DOWN Act was signed by the President on May 19, 2025, after passing both the House and Senate. The act criminalizes the nonconsensual sharing of intimate images online, including those created using AI (Deepfakes), and requires platforms to have a "notice-and-removal" process. Notably, the act explicitly states that consent to create an image does not imply consent to distribute. This means that even if an individual has willingly shared an intimate image or video with someone, publishing it without their explicit consent is now a crime. The platform must remove the images when the individual depicted requests it.



• • • 5



How Deepfakes May Help Law Enforcement

Law enforcement is utilizing artificial intelligence to detect and disrupt trafficking networks. They analyze online data for patterns and identify suspicious activities. Tools like <u>Veritone's IDentify and Track</u> can cross-reference images and track individuals across multiple camera footage, playing a crucial role in this fight. However, it's important to note that these tools have their limitations and are not a solution for all trafficking-related issues.

Thorn developed Spotlight, which utilizes AI to scan vast online data for signs of child trafficking. The rapid pace of AI development can outstrip the ability of legal frameworks to address the misuse of Deepfakes in human trafficking.

Addressing this challenge requires a multi-pronged approach that involves not just technological solutions and strong legislation, but also collaboration between governments, NGOs, and the tech industry, while carefully considering the ethical implications of using AI in this fight.

Following a high-profile
incident with sexually
suggestive AI-generated
images of singer Taylor
Swift going viral on X,
formerly Twitter, multiple
legislators introduced
state and federal
legislation to combat the

Gavin's Law, officially Act 54 of 2023 in South Carolina, makes sexual extortion a felony offense. It specifically addresses the act of blackmailing someone using sexually explicit images or videos, with aggravated penalties if the victim is a minor, vulnerable adult, or suffers harm from the crime. The law also mandates that schools educate students about the dangers and consequences of sexual extortion. It is named in memory of Gavin Guffey, a South Carolina teenager who died by suicide after being sexually extorted.

Legal and Ethical Challenges

Deepfake technology has emerged as a significant challenge for those working in cybersecurity and governance. Many existing laws were not designed to handle situations where the content is not real, making it hard to apply traditional legal frameworks.

Since the content used in Deepfake sextortion is fabricated, it often creates a gray area which criminals can exploit. When someone is harmed by false information, their options for recourse are limited, leaving victims feeling helpless and unprotected. Please click here for more information.



Digital Forensics Corp



Digital Forensics Corp assist businesses and individuals in recovering from digital attacks, including online blackmail, Deepfake nudes, and

With the rise of online blackmail and sextortion they have created a system that works to uncover the identities of blackmailers and stop their malicious activities. Using advanced technologies, such as IPto-location tracking, they can obtain the location and data about the perpetrators and intercede on the client's behalf. They also ensure that explicit content is taken down swiftly, and in case of leaks, we work to minimize exposure.

FBI Tips

In June 2023, the FBI warned that technological advances in AI would bring scams to a nightmarish new high through Deepfakes and face-generating programs. The FBI urges victims to report exploitation by calling the local FBI field office, calling 1-800-CALL-FBI, or reporting it online at tips.fbi.gov.



Here are some recommended steps parents can take to protect their teens from falling victim to a growing threat.

Privacy settings to the max

It is essential to use effective privacy settings. Ensure that you use extremely restrictive settings so that information is visible only to people within your tight-knit network.

Read the fine print of social media terms.

It's essential to check the settings on your social media to make sure content is not visible outside of your network. It is common for social apps to share a significant portion of a person's usage data, personal information, and sometimes biometrics with third parties, which is typically noted in their terms and conditions. Reading through these agreements in depth is the best practice to ensure that your data, photos, and other sensitive information do not fall into the hands of malicious actors.

Have an honest conversation.

The best way to prevent teenagers from putting themselves in harm's way online remains informing them of the life-altering risks. It is also critical for parents to let their kids know that they can and should come to them if they are victims of sextortion, stressed Frank Ahearn, a privacy expert who consults with people who are being blackmailed.



If you have been a victim of image-based sexual abuse, the Cyber Civil Rights Initiative maintains a list of legal resources



How to Identify Deepfakes

You have the potential to identify a Deepfake by combining several methods. **Security.org** suggests the following tips:

- Review the content in question for a label or announcement that it is artificially generated or a Deepfake. Many content creators, entertainers, and others label their Algenerated content as such.
- Look for jerky movements, distortions, and unnatural movements like too much blinking (or a lack of blinking).
- Watch for inconsistencies in facial features. Pay special attention to the cheeks and forehead. Also, look for facial hair or moles that seem unusual. If the person wears glasses, do the glasses reflect the natural workings of light? If the person moves, does the angle of any glare on the glasses also change?
- Analyze speech patterns for differences in tonality and pitch compared to everyday human speech.
- Verify that the lip movements align with the spoken words.
- Consider whether the person in question would realistically be in this setting, saying or doing such things.
- Check the photo or video for digital watermarks. These watermarks can be visible to the human eye (such as a logo), but their removal or alteration is possible. Despite being visible, these watermarks are useful for copyright protection, and you can combine them with other types.

You may be able to use Deepfake detection software.. Audio Deepfakes are more complicated to identify than image and video Deepfakes. Audio Deepfakes are also easier and cheaper to create. Identifying Deepfakes audio requires high levels of expertise, and only a few labs worldwide can do so reliably.



National Center for Missing and Exploited Children

In the past year, the

National Center for

Missing & Exploited

Children has received

more than 10,000



sextortion-related reports. NCMEC has free resources to help children navigate an overwhelming and scary situation. NCMEC also provides a free service called "Take It Down," which works to help victims remove or stop the online sharing of sexually explicit images or videos.

American Academy of Pediatrics



DEDICATED TO THE HEALTH OF ALL CHILDREN

To learn more about the potential impacts of Al-altered images, see the American Academy of Pediatrics portal response The impact of Deepfakes, synthetic pornography & virtual child sexual abuse material.

If you're a parent or caregiver of a child involved in Al-generated, image-based sexual abuse, here are tips on how to move forward and resources that may be helpful from the American Academy of Pediatrics.

8 • •

The Impact of Deepfakes

'Digital Parenting: Raising the A.I. Generation'

NBC News' Valerie Castro shines the spotlight on a teenage victim of online Deepfakes and experts Dr. Jennifer Hartstein and Adam Dodge join live to talk about how to deal with the dangers of Deepfakes and how to protect your kids. Please click here to view this 12-minute video.

Foundation RA

<u>Foundation Ra</u> is a survivor led, registered 501(c)3 nonprofit organization that supports children, women and men that are victims of online image-based sexual abuse. Foundation Ra also works relentlessly to protect and prevent any types of victims of image based sexual abuse, regardless of their background, beliefs, preferences, personal choices or circumstances, we believe that everyone deserves to be treated with dignity and respect.





MSA, U.S. Federal Agencies Advise on Deepfake Threats

The National Security Agency (NSA) and U.S. federal agency partners <u>have issued advice</u> on a media threat known as Deepfakes. This emerging threat could present a cybersecurity challenge for National Security Systems

(NSS), the Department of Defense (DoD), and DIB organizations. They released the joint Cybersecurity Information Sheet (CSI) "Contextualizing Deepfake Threats to Organizations" to help organizations identify, defend against, and respond to Deepfake threats. NSA authored the Cybersecurity Information Sheet with contributions from the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA).







Al-generated nonconsensual intimate imagery opens up threats to national security by creating conditions for blackmail and geopolitical concessions. This could have ripple effects on policymakers irrespective of whether they are directly the target of the imagery.

• • • 9



<u>Thorn</u>, in collaboration with the National Center for Missing and Exploited Children (NCMEC), found that about 10% of financial sextortion reports in 2023 involved images that were not authentic. That number has only grown worldwide. Moreover, Thorn's research with youth found that 1 in 6 minors who experience online sexual interaction never disclose it to anyone.



Boys may be less likely to disclose being victims of sexual crimes, often due to societal expectations and gender norms that discourage them from speaking out.

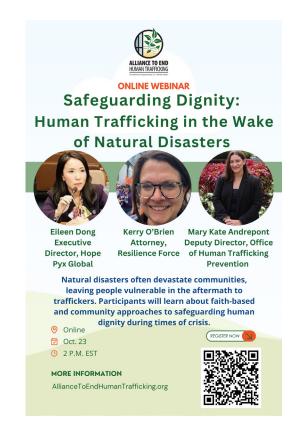
When Deepfakes are involved, the fear of not being believed can intensify, creating an even bigger barrier to seeking help. Open, ongoing conversations about online safety are essential, but we must also recognize that children might not always turn to parents and caregivers first.

Thorn's **NoFiltr youth prevention program** allows youth to engage with their peers on important topics regarding online safety.

The advice to youth of "Don't share nudes" can be insufficient. Deepfakes only magnify the shortcomings of this message. Children who have never taken and shared an explicit image of themself can now be easily targeted by sextortionists using generative AI image creation.

Financial sextortion happens online every single day. Its effects have led to severe consequences among young victims, including self-harm. Understanding why a child might be reluctant to seek support, and taking action to reduce those barriers can truly save lives.





What Can You Do If You or Your Child are Victims?

The following information is from the <u>American Academy of Pediatrics</u>. Remember, it is a crime to publish or share intimate images without your permission.

If you're a parent or caregiver of a child involved in AI-generated, image-based sexual abuse, it is crucial to let them know that you're there for them and that it's not their fault. Take steps to ensure your child's safety.

Block and report the perpetrator. Ask that the images be taken down. Use the "Take It Down" tool provided by the National Center for Missing and Exploited Children to help remove explicit images or videos if the victim is under 18 from participating in online platforms. If the victim is 18 or older, you can use the StopNCII.org tool. On the Cyber Rights Initiative website, you can find a detailed Online Removal Guide to help you remove images from Facebook, Instagram, Twitter, Reddit, Tumblr, Yahoo, Google, and Microsoft.

You can also tell the Federal Trade Commission if a company posts your image without your consent and won't take it down.

If you are a victim, stay calm and report the scheme immediately to the FBI or your local law enforcement agency. You can contact the police or the District Attorney's Office if you prefer to have the matter handled through the criminal court. Suppose the person sharing the images is a current or former intimate partner or family member. In that case, you can go to Family Court to obtain an Order of Protection against them and to prevent them from sharing these images.

Report the predator's account via the platform's safety feature. Most online platforms and apps have a way to report abusive users. Victims of Deepfakes may be able to seek monetary damages.

You can find links to low-cost or pro bono (free volunteer) <u>Attorneys</u> on the Cyber Rights Initiative website.

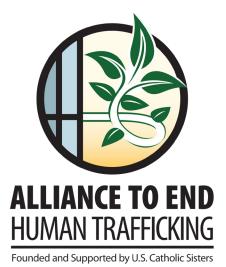
If you are a victim of sexual image exploitation, please call the <u>Cyber Civil Rights Initiative Crisis</u> Helpline at 844-878-2274 for support and advice.

Do not delete any communications or threats from the blackmailer. Take screenshots or screen recordings of messages, photos, videos, and any profile information of the perpetrator. This evidence will be valuable for law enforcement to investigate the crime and potentially identify the blackmailer.

Monitor your child's mental health symptoms and overall well-being: Look for unusual changes in mood, sleep patterns, appetite, energy levels, desire to socialize with friends and family, and consistent attendance at school and extracurricular activities. Reach out to your pediatrician or health professional if you notice any concerning changes.

An eye-opening 60 Minutes segment highlights the alarming rise of AI-generated nude images and their devastating impact, especially on children. Watch the full 60 Minutes segment here.

• • 11



Click on the links below to visit the websites of our sponsors

- Adorers of the Blood of Christ
- Adrian Dominicans
- Benedictine Sisters of Chicago
- Benedictine Sisters of Mount St. Scholastica, Atchison, KS
- Benet Hill Monastery
- · Congregation of Notre Dame
- · Congregation of Sisters of St. Agnes
- Congregation of S. Joseph
- Daughters of Charity, Province of the West
- · Daughters of Charity, Province of St. Louise
- · Daughters of the Holy Spirit
- · Dominican Sisters of Houston, TX
- · Dominican Sisters of Mission San Jose, CA
- · Dominican Sisters of Peace
- Dominican Sisters of San Rafael, CA
- Dominican Sisters of Sinsinawa, WI
- · Dominican Sisters of Sparkill
- Dominican Sisters of Springfield, IL
- · Felician Sisters of North America
- Franciscan Sisters of Peace
- Franciscan Sisters of Perpetual Adoration
- Franciscan Sisters of the Sacred Heart
- Holy Spirit Missionary Sisters
- · Institute of the Blessed Virgin Mary
- Marianites of Holy Cross
- Maryknoll Sisters
- Medical Mission Sisters
- Medical Missionaries of Mary
- Missionary Sisters of the Society of Mary
- Northern California Catholic Sisters Against Human Trafficking
- Our Lady of Victory Missionary Sisters
- Presentation Sisters, Aberdeen
- Presentation Sisters, San Francisco

- Racine Dominicans
- Religious of the Sacred Heart of Mary
- Religious Sisters of Charity
- · School Sisters of Notre Dame, North America
- School Sisters of St. Francis of Christ the King
- Sisters of Bon Secours
- Sisters of Charity of Cincinnati
- Sisters of Charity of Halifax
- Sisters of Charity of Leavenworth
- Sisters of Charity of New York
- · Sisters of Charity of St. Joan Antida
- Sisters of Charity of the Blessed Virgin Mary
- Sisters of Charity of the Incarnate Word Houston
- · Sisters of Charity of Nazareth
- · Sisters of Charity of Seton Hill
- Sisters of Christian Charity Mendham, NJ & Wilmette, IL
- Sisters of Mercy Catherine's Residence
- Sisters of Mercy of the Americas
- · Sisters of Notre Dame of the United States
- · Sisters of Notre Dame de Namur, USA
- Sisters of Providence, Mother Joseph Province
- · Sisters of St. Chretienne
- · Sisters of St. Dominic Racine, WI
- Sisters of St. Francis of Clinton
- Sisters of St. Francis of Colorado Springs
- Sisters of St. Francis of Dubuque
- Sisters of St. Francis of Mary Immaculate
- Sisters of St. Francis of Philadelphia
- Sisters of St. Francis of Redwood City
- · Sisters of St. Francis of the Providence of God
- · Sisters of St. Francis Rochester, MN
- · Sisters of St. Joseph of Baden
- · Sisters of St. Joseph of Carondelet
- Sisters of St. Joseph of Chestnut Hill Philadelphia
- Sisters of St. Joseph of Cluny, USA & Canada Provinces
- Sisters of St. Joseph of Concordia, KS
- Sisters of St. Joseph of Orange
- Sisters of the Blessed Sacrament
- Sisters of the Divine Savior
- Sisters of the Good Shepherd
- · Sisters of the Holy Cross
- Sisters of the Holy Family
- Sisters of the Holy Fulling
- Sisters of the Holy Names of Jesus and Mary
- Sisters of the Humility of Mary
- · Sisters of the Precious Blood
- Sisters of the Presentation of the Blessed Virgin Mary
- Sisters of the Sacred Hearts
- Sisters of the Sorrowful Mother
- Society of the Divine Savior
- Society of the Holy Child Jesus
- Society of the Sacred Heart
- Southern CA Partners for Global Justice
- St. Mary's Institute of O'Fallon
- Tri-State Coalition Against Human Trafficking & Slavery
- · U.S. Ursuline Sisters of the Roman Union