Understanding Encryption:
The Connections to Survivor Safety

For many survivors of domestic violence, sexual violence, stalking, and trafficking, having private and secure ways to communicate and store files electronically is a vital part of their safety. For victim service providers and other professionals working with survivors of abuse, using communication and storage tools that prioritize privacy and security help ensure they're supporting the survivor's privacy and safety. Strong encryption is a critical part of the solution.

What is Encryption and How Does it Work?

Generally, encryption is the process of scrambling information so that it can only be read by those who have access to the keys to unscramble it. This process of unscrambling is called decryption. Not all encryption is the same, and some communication and online storage platforms use weak encryption methods. To ensure survivors remain in control of their information, it's important that no third party have a key to access their communications or information stored in the cloud. **End-to-end (E2E) encryption** provides the strongest level of security and trust for communication technologies, because by design only the sender's device and the intended recipient's device hold the keys to decrypt the message. For the instances where sensitive data needs to be stored securely online, what is called "zero-knowledge" or "no-knowledge" encryption should be the standard. This level of encryption means that no one except the account holder can view the data.

Here are some examples of how E2E encryption and no-knowledge encryption can help mitigate the impacts of technology-facilitated abuse.

I. **Safety Planning & Relocating:**
End-to-end encryption can provide a secure channel for a survivor to make plans and communicate with trusted individuals, like when they are trying to relocate and secure housing and support. (This is particularly true when the abusive person does not have access to the

survivor's devices or accounts.)

II. **Protecting the Integrity of Evidence:**

Using E2E and no-knowledge encryption when storing and transferring digital evidence to law enforcement, prosecutors, or other professionals in the legal system helps maintain the integrity of that evidence. When digital evidence is passed through insecure sources or there is the possibility of interception, the integrity of the evidence can be diminished, increasing the likelihood that its authenticity will be called into question in a court of law.

III. **Protection Against Unauthorized Access:**

Unauthorized access to data can happen when a communication being sent (data in transit) is intercepted or when information stored in an online database or online file vault (data at rest) is breached. This is why it's critical that all data – that in transit and that at rest – be protected with the highest level of encryption. Information communicated without E2E encryption is at an increased risk of being breached by third parties. Furthermore, information stored without no-knowledge encryption is at increased risk of being breached. Both types of breaches can negatively impact a survivor's privacy, safety, and well-being by revealing sensitive information. This could result in their abuser finding them after they've relocated, or to the loss of evidence related to their pending court case, or to revealing personal information that could negatively impact their ability to secure or maintain housing or employment.

IV. **Seeking Help:**

E2E encryption allows survivors to communicate safely and securely when they decide to seek help. It helps protect against interception, deletion, and alteration. It helps ensure that private communications stay private, so that only the sender's and intended recipient's devices can access the messages.

Protect End-to-End Encryption to Protect Survivors

Strong encryption is a critical tool that helps protect the privacy and safety of survivors. Unfortunately, efforts to undermine E2E and no-knowledge encryption will also undermine survivor privacy and safety. Using weaker forms of encryption or creating backdoors to the most secure methods of encryption threatens the security of everyone who relies on it for private communication.

The best way to keep people safe online is to continue preserving uncompromised end-to-end and no-knowledge encryption practices, and to adopt and bolster strong encryption policies. Survivors of domestic violence, sexual assault, stalking, and trafficking deserve to know that their private communications remain confidential as they seek support, and that the evidence they collect can be preserved without risk of malicious tampering or deletion. When E2E and no-knowledge encryption-based technology is available to survivors, they are empowered with more options to find help, safety, and healing.

Learn more about the technical and human elements of encryption at www.internetsociety.org, and learn more about how to help survivors at www.techsafety.org. Follow our work on Twitter at @internetsociety and @nnedv.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.