Victims of Violence & Privacy

Since community-based programs began serving victims of domestic violence, sexual assault, and stalking, privacy and even secrecy have been considered a crucial component of a victim’s safety. This is why many emergency domestic violence shelter locations are still confidential and why many states have laws that prohibit publishing the names of rape victims. Many states have address confidentiality programs for victims of domestic and sexual violence and stalking so that survivors do not have to give out their home addresses. Survivor privacy is so critical to their safety, that several federal laws include privacy and confidentiality provisions and most states prohibit the disclosure of victim information.

Despite state and federal laws, in this age of advanced technology, increased data collection, and increased data sharing, it has become more difficult than ever for survivors to limit the sharing of their personal information. Despite strict state and federal laws and advocacy prioritizing survivor privacy, sensitive information can be exposed, leaving survivors either in danger, unwilling to disclose their abuse and get help, or unable to do something as simple as buying a house.

The World of the Internet

We live in the world of internet search engines where information about anything and anyone can be obtained in less than a second. We also live in a time where things that are shared offline are increasingly getting posted online. A quick search on a public tax mortgage site can reveal exactly who owns the home, where the house is located, property value, and, depending on the community, even more personal information about the homeowner. This has prevented many survivors from purchasing homes, fearing that a stalker or abuser whom they have fled will be able to find them.

An online search of a person’s name can pull up a wealth of information, including: social media accounts; references to them online, which could include
news stories or even pictures posted by an organization; data broker sites that sell personal information, including addresses (current and former), financial records, background checks, and so much more. Public records, including court records, are also increasingly being published online. In some cases, survivors’ testimony of their assaults has been published online.

Impact to Victims
Survivors are finding it increasingly difficult to maintain any form of privacy. They need to learn how their information could possibly be shared and be proactive about preventing it or limiting it, knowing that in many cases, it is just not possible. Once information is posted online, it is nearly impossible to remove it. For one victim of revenge porn, the victim and her mother spent thousands of hours trying to remove the intimate images that were distributed online by an ex-boyfriend. NNEDV has spoken with an advocate working with a rape survivor whose testimony during her trial was published online by a law firm, and they are desperately trying to remove it.

The result is that survivors are making decisions that no one should have to make. Some survivors are so fearful of someone finding them that they choose to be homeless to “stay off the radar.” One survivor with whom NNEDV spoke explained that she “couch surfs” via craigslist postings, just so she does not have to sign any lease. Another survivor refused to have any official government ID because she worries that if her name gets into any government database, her abusers will find her. This results in her being unable to participate in activities that require an official ID, including flying and even accessing some social services. For other survivors, the lack of privacy when seeking services creates a chilling effect, causing them to choose not to call the police or ask for help.

Some survivors believe that they can maintain their privacy and safety by changing their names. However, this can create even more problems. Despite changing their names, they can still be found because there is simply so much information available; the two names may inevitably be connected. Survivors who change their names may have more trouble getting jobs or housing (because
previous employment and tenancy were in their old names); they may lose professional credentials, because their education, professional licenses, and certifications were in their old name; and may have a difficult time replacing important identification documents, such as birth certificates and driver licenses. Inevitably, for these reasons and so many more, survivors end up having to disclose that they used to go by another name, thereby connecting both identities, eliminating the reason for the name change in the first place.

**How to Increase Survivor Privacy**

1. **What is the goal for sharing or publishing this information?**
   First, it is important to identify the reasons for why information needs to be collected, compiled, or shared. Second, weigh those goals against the potential safety and potential danger it could pose for the victim if information is disclosed. Despite the benefit of sharing, if releasing information could put someone in danger, it might be better to not share that information. Instead, there may be other ways to share information that minimizes privacy risks and potential danger.

2. **What is the privacy impact for victims?**
   Any publication of individual data, but specifically victim data, should include a discussion on how that publication could impact the privacy, and therefore safety, of victims. Victim privacy experts should be included in these discussions to ensure that the experiences of survivors are at the center of these conversations. Keep in mind that for many victims of violence, privacy can have a direct correlation to their safety. For some survivors, knowing that they are not able to maintain privacy can result in them not seeking services or requesting help.

3. **Is there notice or consent for the release of information?**
   At minimum, survivors should be informed of what information is being collected and who will have access to that information. Survivors’ lives are complex and they know best what might compromise their safety. Knowing
the potential risks will help them determine their next steps. Best practice is allowing survivors to decide when, what information, and to whom their information is shared.

4. **Can the information be identifiable?**

In this age of increased data sharing, simply removing the name will not de-identify the data. A lot of other information can be identifying, such as location, the perpetrator’s name, or a combination of age and race. In addition, certain information—in combination or in context—can be identifying. For example, data regarding a 13-year old, African-American, female rape victim from a specific neighborhood, can be quite identifying, even if her name and exact address are not provided. Finally, be aware of the mosaic effect, wherein the information by itself is not identifying but combined with other data sets could re-identify individuals.

5. **If information must be collected and shared, does it follow Fair Information Practice Principles?**

The Fair Information Practice Principles are guidelines that help organizations determine how to collect and share personally identifying information while considering individual privacy. These guidelines include transparency, participation of the individual whose information is being collected, specifying the purpose for collecting and using the information, minimizing the data that is being collected, limiting the use of the data, ensuring data quality and integrity, having security safeguards, and demonstrating accountability when collecting personal information. Best practices exist that allow the sharing of information while ensuring privacy.