Data shattering is a technique where the data is split into small little pieces and moved in various ways across the Internet to eventually the offline database. The data will then be reassembled and encrypted to be used by the pattern recognition software. The purpose behind the data shattering is to ensure the safety of the data from hackers whom may attempt to tamper or steal. By doing so we also ensure the security of the user and the accused.

The most fundamental fact of the PACTS software and ideology is that we own the data. To give away the rights to it is against our beliefs and is not an option. With that said, though, we are willing to work with companies to best utilize the data. Meaning that arraignments can be made so that its not just PACTS will provide special accommodations for the company. The most useful accommodation would be unique data handling methods. (I think maybe a sentence could be said about saying that the goal is still at the end of the day to find predators, but that is up to you)

The software has built in methods to ensure anonymity of both the accused and accusing. The first and most important is encryption methods, which, for example, ensure that names put in the pacts database will not be the same. The next method is the data shattering which protects against hackers from being able to get at the whole data. The third is the offline database; once the data has made it to the offline database it is impossible to be reached by hackers. The reason being is that since it is offline remote access will not be possible. These are but three ways the PACTS software ensures the security of both the data and the users. These methods, and others, also prevent slander from occurring before the PACTS software has had a chance to sift through the data.

The other risk of slanderous charges is once the PACTS software has scanned through the data. The pattern recognition itself will not only search for patterns which point to sexual assault, but also to those that appear to have been faked. This is but one way the software works to ensure that those who have done nothing wrong are not damaged. The software will also go through the data looking for inconsistencies to ensure that the only data kept will be from real victims and not those looking to needlessly damage others. These methods are based off of doctors and other professionals who helped ensure the software’s integrity. The goal is to find predators, not falsely identify them; PACTS succeeds without issue in this.