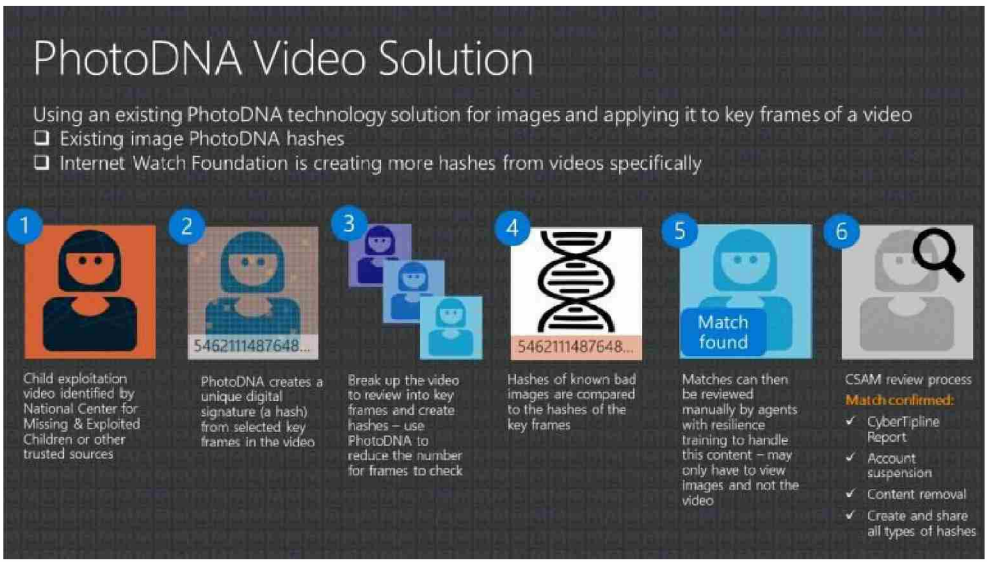
Microsoft has long been committed to protecting its customers from illegal content on its products and services, and applying technology the company already created to combating this growth in illegal videos was a logical next step.

"Child exploitation video content is a crime scene. After exploring the development of new technology and testing other tools, we determined that the existing, widely used PhotoDNA technology could also be used to effectively address video," says Courtney Gregoire, Assistant General Counsel with Microsoft's Digital Crimes Unit. "We don't want this illegal content shared on our products and services. And we want to put the PhotoDNA tool in as many hands as possible to help stop the re-victimization of children that occurs every time a video appears again online."

A recent survey of survivors of child sexual abuse from the Canadian Centre for Child Protection found that the online sharing of images and videos documenting crimes committed against them intensified feelings of shame, humiliation, vulnerability and powerlessness. As one survivor was quoted in the report: "The abuse stops and at some point also the fear for abuse; the fear for the material never ends."



The original PhotoDNA helps put a stop to this online recirculation by creating a "hash" or digital signature of an image: converting it into a black-and-white format, dividing it into squares and quantifying that shading. It does not employ facial recognition technology, nor can it identify a person or object in the image. It compares an image's hash against a database of images that watchdog organizations and companies have already identified as illegal. IWF, which has been compiling a reference database of PhotoDNA signatures, now has 300,000 hashes of known child sexual exploitation materials.

PhotoDNA for Video breaks down a video into key frames and essentially creates hashes for those screenshots. In the same way that PhotoDNA can match an image that has been altered to