WRITTEN TESTIMONY OF KEVIN METCALF
National Child Protection Task Force (NCPTF)
House Bill 223 & Senate Bill 192 – Facial Recognition Technology

Thank you for the opportunity to provide this testimony. Since February 2011, I have been a Deputy Prosecuting Attorney at the Washington County Prosecutor's Office in Arkansas, where I prosecute felonies. I am also the founder and Chief Executive Officer of National Child Protection Task Force (NCPTF). The NCPTF is a non-profit organization with approximately 50 volunteers that include active-duty law enforcement officers who volunteer their time to help state, federal, and international law enforcement agencies investigate online child abuse, recover exploited children, and hunt sexual predators and human traffickers.

The members of the NCPTF help provide detectives, analysts, and officers access to investigative expertise and resources that are unavailable or underfunded in most law enforcement organizations. For example, the NCPTF brings together recognized experts in facial recognition technology, strategic legal applications, open-source intelligence, cellular mapping and analysis, dark-web investigations, and cryptocurrency to aid law enforcement agencies everywhere. Through my work as a prosecutor and with the NCPTF, I have assisted with the recovery of hundreds of missing and exploited children and helped identify and apprehend hundreds of sexual predators in multiple states and countries.

Open-source intelligence is a critical component in the timely identification and rescue of these young victims of violent crimes. In fact, without the ability to effectively process open-source intelligence, our success in these cases would be tragically impaired. I could give you hundreds of examples of children who were being sexually exploited or raped and were rescued solely because of access to open-source intelligence, but most cases follow the same general fact pattern. Law enforcement officers find videos and photos on the dark web of children being raped -- many are produced by parents, siblings, or other close family members. Law enforcement knows nothing about these children other than the fact that they are being raped and that their videos and photos are being traded or sold on the dark web.

Using traditional investigative techniques, law enforcement officers have to carefully scrutinize every second of these rape videos hoping that the perpetrators will make a mistake and reveal a clue, such as a street sign, identification card, or receipt that could give investigators a lead. On the dark web, predators maintain manuals of changes in the law, technological advances, and the methods investigators use to identify other pedophiles. The ready availability of these how-to manuals means that predators make fewer mistakes that investigators can use to track them, and children continue to be exploited and raped.

Most of the time, law enforcement only has images of helpless children's faces with no way to identify them or bring them to safety. It is fruitless to run the faces of child rape victims, many of whom are prepubescent, through traditional law enforcement facial recognition programs because these programs are typically limited to booking photos. Sometimes, the faces of predators are present, but that is still a long shot as many of the abusers have managed to avoid arrest.

We must use open-source intelligence to identify these victims and these perpetrators. And the best source of this intelligence is publicly available data and images from the internet. But as you can imagine, the vastness of the public internet makes it impossible to effectively search it by a single human investigator or even a team of investigators. It requires working collaboratively with companies that aggregate public data and publicly available images. The data they provide is data that I or any investigator in the world would already have lawful access to, but it would take months, even years, to effectively search it manually. These young victims don’t have months or years, some don’t have hours, before they are violated again, so there is a real urgency in the need to quickly identify the victims and suspects in these cases. The use of modern, high-performing facial recognition technology and aggregated public data and images are crucial to our continued success.

This technology and publicly available dataset helps protect children who would otherwise slip through the cracks -- children who have not been reported as missing or abused and are being raped by their parents, family members, or others close to the child.

Example of Locating Child Using FRT

In one case here in the U.S., a predator was posting images of the sexual abuse of very young children; the images indicated he had access to children and was actively raping and abusing them. However, one of the pictures he posted included the face of a young teenage girl. Using technology with an open-source database, investigators were able to identify the girl from an old Instagram account she no longer used. This allowed law enforcement to find her and identify the predator, who was actively abusing very young children. This teen's face would not appear in a driver's license database or booking photos.

MVA Database and Mug Shots Severely Limit Effectiveness of FRT in Child Exploitation Cases

Despite the misinformation out there on this subject, high-performing facial recognition technology is extremely accurate, and when used within appropriate procedures and guidelines is very effective. Facial recognition offers unprecedented capabilities to identify stalkers, rapists, child abusers, and other online predators and could facilitate identification of previously unknown child victims depicted in child sexual-abuse material proliferating online. However, limiting the data set to only that provided by the motor vehicle administration (MVA) is extraordinarily limiting. This will not help identify a deceased child, a minor victim, or a suspect traveling through the state that is not in the MVA data set. The issues related to limiting law enforcement's data set are infinite. Limiting the dataset to only MVA images and mug shots significantly increases the likelihood of misidentifications and completely omits the important work being done with facial recognition to identify children who are abused and whose images appear online.

Open-source data has been a game changer for rescuing and identifying victims such as children and identifying violent criminals that are from other states and countries. Law enforcement has significantly increased the rate of identifying child victims of sexual abuse online using platforms of aggregated publicly available data and images. In fact, limiting datasets has many unintended consequences, aside from severely limiting its use in child exploitation cases. Restricting a law enforcement agency to look for perpetrators in criminal datasets such as mug shots is inherently biased in itself. It encourages the resolution of crimes that point to repeat offenders and discourages resolution of investigations involving unknown persons that are not in the typical local data set. Citizens should be concerned if the only data its law enforcement is permitted to use is that of its own communities.

In many investigations, but more so related to children, time is never on the side of law enforcement. While reasonable and effective policies and procedures are critical for law enforcement's use of facial recognition technology, limiting the databases or creating a complicated process where it could take days, weeks or months to use the technology could mean another child is lost. Trafficking and crimes against children move quickly. A child being sex trafficked could be in one location and then moved to another state the following day (or even that same day). If law enforcement cannot use facial recognition technology promptly because an investigator has to place multiple requests, has to obtain approval from another agency or department, and then waiting for days for a search to be returned – it will be too late, the child will be in another location.

Without facial recognition technology that uses a database of publicly available data and images, we will lose the ability to save hundreds of children from continuing to be raped, and these recordings shared on the internet for the world to see. Further, limiting law enforcement's ability to use facial recognition technology and limiting it to the MVA dataset will significantly curtail the success of law enforcement in cases where the children are victims.

Thank you for your time.

Kevin Metcalf