RIGHT ON CRIME **Testimony**

July 13, 2021

Facial Recognition Technology: Examining Its Use by Law Enforcement

Testimony before the United States House of Representatives Committee on the Judiciary

by Brett Tolman, Executive Director

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee on Crime, Terrorism, and Homeland Security:

Thank you for the opportunity to testify today.

My name is Brett Tolman, and I am the Executive Director of Right on Crime, a conservative organization dedicated to the promotion of criminal justice policies that promote public safety, individual liberty, and whole communities. I have previously served as the United States Attorney for the District of Utah, as an Assistant United States Attorney, and as Chief Counsel for Crime and Terrorism for the United States Senate Judiciary Committee. The past decade I have also worked in private practice as the founder of the Tolman Group, focusing on government reform, criminal defense, and internal corporate investigations, and previously as a Shareholder and Chair of the White Collar, Corporate Compliance and Government Investigations Section of the law firm of Ray Quinney & Nebeker, PC.

I am encouraged by the Subcommittee's decision to hold a hearing today on the use of facial recognition technology by law enforcement entities. It is an area of increasing concern that is ripe for abuse and could stand to benefit from congressional attention and oversight.

The first issue to address is a concerning lack of transparency and basic information relating to law enforcement's use of facial recognition technology. Many of the fundamental questions that you likely want—and deserve—answers to are currently unanswerable. Questions such as: How many law enforcement entities use facial recognition? How often do they use it? Who is in their databases and why?

To the extent that we have partial answers to some of these questions, the facts are daunting. Recently, the Government Accountability Office revealed that beyond those federal law enforcement agencies one might suspect of using facial recognition, like the Federal Bureau of Investigation, there are a host of others with less apparent need who also use the technology. For example, the U.S. Fish and Wildlife Service and the Internal Revenue Service.[1] Nationally, one estimate placed the government market for facial recognition in this country at $136.9 million in 2018, with the expectation that it would nearly triple by 2025.[2] Another estimate suggested that as of 2016, at least 1 in 4 police departments had the option to run facial recognition searches, a number that has surely grown since then.[3]

Also discomforting are the sources of the photos supporting this facial recognition technology. In addition to drawing on pictures secured through the criminal justice process, the government utilizes millions of photos of law-abiding individuals collected for driver's licenses and passports.[4] Private technology companies that contract with law enforcement have harvested billions of photos posted by unsuspecting users on platforms such as Facebook, YouTube, and even Venmo.[5] This collection is an unprecedented invasion of privacy that places enormous, undue control in the hands of the government and Big Tech, two entities not always known for their light touch or responsible use of power.

1 https://www.gao.gov/assets/gao-21-518.pdf
2 https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251
3 https://www.perpetuallineup.org/
4 https://www.gao.gov/assets/gao-16-267.pdf
5 https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

continued

Mass surveillance compounds the issues surrounding mass collection. Walking out the door in the morning can be an exercise in skipping from one camera to another, as everywhere from the convenience store on the corner to the traffic camera at the light in front of it record our actions. To this perpetual passive surveillance, law enforcement can potentially add recordings from body-worn cameras or simply from the smartphone in an officer's pocket. In short, there are very few instances where law enforcement will *not* have the opportunity to subject a person of interest to facial recognition technology.

Inevitably, the first temptation will be to use facial recognition by default rather than necessity. Instead of limiting the practice to serious public safety risks or only after due process has been afforded an individual, officers may use—and have already used—the practice for run-of-the-mill interactions and minor cases.[6] Our Founding Fathers deliberately and prudently enshrined in the Bill of Rights proscriptions on the wanton search of Americans as a necessary bulwark for freedom. It is hard to square these notions and protections with the unfettered use of a technology that can instantaneously reveal an individual's identity as well as potentially their associations and prior movements. The unrestricted use of facial recognition bears little difference to allowing police to collect fingerprints or DNA from anyone and everyone they come across, an abuse that we clearly do not, and should not, tolerate.

The implications of such access to personal information become especially troubling when dealing with real-time interactions between law enforcement and members of the public. Americans have long prided themselves on our ability to refuse the government unless it has legitimate cause to interfere with our liberty. Our police, at least in the absence of reasonable suspicion of wrongdoing or additional judicial process, are supposed to rely on the consent of the citizenry in their interactions. Facial recognition has the power to stand this principle on its head and turn questions from law enforcement about personal information into mere rhetorical ones.

In addition to identifying individuals, facial recognition technology makes it much easier for law enforcement to track them. It can essentially automate surveillance across the network of cameras mentioned above, following individuals with minimal effort or oversight. It could also mean historical tracking. Once somebody lands on law enforcement's radar, there is little stopping officers from running their image through available videos and photos to reconstruct past days, their associations or affiliations, and other aspects of their life or routine.

Furthermore, we cannot ignore the risk that facial recognition technology will be used to target certain Americans. Facial recognition can instantaneously strip away the anonymity of crowds, and ultimately threaten our constitutional rights of assembly and association. Consider the chilling effect facial recognition could have if used to identify individuals at a political rally or government protest. This technology could be used to identify everyone who simply visits a gun store or any other place an individual is exercising a personal freedom or choice that a particular politician or other individual heading an agency considers undesirable.

This practice grossly lacks the necessary accountability. Right now, we have little more than vague assurances that we should trust the government to safely use the incredible power of facial recognition technology without such information or oversight. Not long ago, I was tasked with leading the effort in the Senate to reauthorize

6 https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251

the PATRIOT Act. We heard similar assurances years ago, by those leading the Department of Justice and the FBI about FISA and those surveillance authorities not being turned against honest Americans. We have seen how that worked out as outlined in the recent, and disturbing, Inspector General reports.

None of this is to say that law enforcement should *never* have access to facial recognition technology. While China's unconscionable use of facial recognition technology to enhance and accelerate its undemocratic control of its citizenry is a warning of the costs of failure, I do not believe it is the inevitable consequence of any use of facial recognition technology by law enforcement. Further, it is unrealistic to expect law enforcement officials to permanently deny themselves a tool that is increasingly prevalent in the commercial sector and which has such powerful capacity to improve public safety. It is easy to contrive a scenario in which we would very much want law enforcement to have facial recognition technology available—searching for a known terrorist loose in one of our cities presenting an imminent risk to the public, or seeking to identify a mass-murder suspect, for example. And while I harbor a conservative's healthy skepticism of government, I respect members of law enforcement and will always seek to support them and their mission to keep us all safe. However, acknowledging there are credible uses for facial recognition technology and voicing support for law enforcement is not the same as writing a blank check for power and then looking the other way.

In the past, members of this Subcommittee and others in Congress have proposed a moratorium on the use of facial recognition technology by law enforcement. Significant restraints might be necessary for privacy protections to catch up to the rapidly advancing capabilities of this technology. If nothing else, we need a reset in which law enforcement agencies must gain affirmative permission from relevant democratically elected representatives to use this technology prior to its use; that way transparency, accountability, and proper use guidelines can be established.

As it stands, it is difficult to see how the regular, widespread use of this technology can meet the high standards of our Constitution and its protection of civil liberties or the norms inherent in a democratic society. If one considers this technology as creating the ability to find a needle in a haystack, it seems entirely reasonable to demand the police to first know which needle they are looking for, rather than search every haystack in the off chance it contains a needle. Absent an emergency or other exceptional circumstance, some manner of reasonable suspicion should likely be a prerequisite to a facial recognition search. Likewise, we should be exceedingly cautious about the deployment of real-time facial recognition, which has more disturbing Fourth Amendment implications. Finally, we need transparency on when, how, and why every law enforcement agency is using facial recognition and which databases they are drawing from, and we should have particular reticence when it comes to the collection of images from unwitting, law-abiding individuals.

This is a pressing issue pertaining to all Americans' fundamental rights. As someone who has spent a great deal of time working on legislation in this arena and someone who fundamentally believes that smaller government is better government, I am encouraged that the Subcommittee is concentrating its focus on these concerns today. I expect that its resolution will require many conversations, careful balancing of tradeoffs, and potentially difficult decisions. I look forward to contributing however I can to that effort today. Thank you once again, Chair Jackson Lee, Ranking Member Biggs, and other Members of this Subcommittee.

ABOUT THE AUTHOR

Brett L. Tolman is the founder of the Tolman Group and the executive director for Right on Crime. He is dedicated to state and federal policy and advocacy, especially on criminal justice reform. Prior to entering private practice, Tolman was appointed by President George Bush in 2006 as the United States Attorney for the District of Utah and held that office for nearly 4 years from 2006-2009. As U.S. Attorney for Utah, he was responsible for cutting-edge cases addressing such issues as international adoption fraud, mortgage fraud, international marriage fraud, sex and human trafficking, terrorism, and breaches of national security. In 2009 he handled the prosecution of Brian David Mitchell, the convicted kidnapper of Elizabeth Smart. From 2008-2009 he was selected by Attorney General Michael Mukasey to serve as special advisor to the attorney general on national and international policy issues affecting United States attorneys and the Department of Justice. Prior to his appointment as U.S. Attorney, Tolman served as chief counsel for crime and terrorism to the United States Senate Judiciary Committee.

During his career, Tolman has testified multiple times in the United States Congress and assisted in drafting and passing many pieces of legislation affecting state and federal criminal justice systems. These include the First Step Act of 2018, the Corrections Act, the Sentencing Reform Act, the Justice for All Act of 2004, Protection of Lawful Commerce in Arms Act (2005), the Violence Against Women and Department of Justice Reauthorization Act of 2005, the USA Patriot Improvement and Reauthorization Act of 2005, and the Adam Walsh Protection and Safety Act (2006). He is a frequent contributor on Fox News, CNN, MSNBC, NewsMax and *No Spin News* with Bill O'Reilly.

About Right on Crime

Right on Crime is a national campaign of the Texas Public Policy Foundation, in partnership with the American Conservative Union Foundation and Prison Fellowship, which supports conservative solutions for reducing crime, restoring victims, reforming offenders, and lowering taxpayer costs. The movement was born in Texas in 2007, and in recent years, dozens of states such as Georgia, Ohio, Kentucky, Mississippi, Oklahoma, and Louisiana, have led the way in implementing conservative criminal justice reforms.

RIGHT ON CRIME

901 Congress Avenue | Austin, Texas 78701 | 512.472.2700 | www.TexasPolicy.com | www.RightOnCrime.com