

Facial recognition could stop terrorists before they act

BY ADONIS HOFFMAN, OPINION CONTRIBUTOR — 03/09/20 11:30 AM EDT

America lost another piece of its soul when two homemade bombs exploded on Patriots Day, 2013, at the Boston Marathon. That act of home-grown terrorism killed three spectators and wounded hundreds of others. With it, the innocence of a celebrated event, and others like it, became forever lost.

In the seven years since the Boston Marathon bombing, there have been successive acts of domestic terrorism: 14 dead and dozens wounded in San Bernardino, 2015; 49 dead in the 2016 Orlando night club shooting; 8 killed in the 2017 New York City pickup truck incident; 22 killed in the 2019 El Paso Walmart shooting, And three sailors killed in the Pensacola Naval Air Station shooting last December.

All of these crimes were committed by men with deeply extremist views. Most documented their hate on social media postings prior to doing the deed. And some even showed up in a law enforcement database. Regrettably, none of this information was used to prevent their horrific acts.

Today, local police and national law enforcement agencies have a greater chance to identify, anticipate and preempt terrorist actions through new artificial intelligence — AI — tools. Among other things, AI facial recognition technology allows the authorities to clearly identify any individual, compare them against billions of public images culled from well-known sources and investigate what that person may be up to today. Facebook, Google and Microsoft, and smaller companies too, have been researching facial recognition technology for years, aided by work at leading universities.

A newcomer and early leader in this technology is Clearview AI. It is a small company whose groundbreaking — but controversial — facial recognition app has been favorably adopted by hundreds of state and federal law enforcement agencies as a crime-fighting tool. Success in solving several crimes has led law enforcement to embrace and endorse the app. There is little doubt the technology has the potential to change the paradigm. It would seem that its best and highest use would be to anticipate bad actions by bad people before they happen.

But not so fast.

Privacy advocates, policymakers and civil liberty proponents around the world have criticized the company and its technology for breaking the social compact on personal privacy. The critics contend that facial recognition applications pierce too far into our private space and can be hijacked for nefarious purposes, including racial profiling and unlawful surveillance. All valid concerns, to be sure.

The same conclusions, however, might be reached on other technologies, as well. Although technology is supposed to be neutral, its application, use and deployment determine whether it becomes a value or a vice to society. For example, a predictive modeling application used by big banks might be used to either reward or redline entire demographic groups, depending on how it is applied. Certain healthcare applications used by insurance companies can mean the difference between acceptance and denial, depending on how the apps are configured.

The biometric, banking, geolocation, social media, and advertising applications companies that we now rely upon leverage our personal data to deliver goods and services. These technologies not only are innovative and disruptive but are invasive and disturbing as well. Some have gone too far, and yet they persist with no public interest purpose to speak of, let alone protections of individual privacy.

That alone should distinguish the use of artificial intelligence and facial recognition for public safety and law enforcement purposes. If managed and regulated responsibly, this could become one of the most powerful weapons in the fight against global crime and terror.

In an age of isolated and seemingly random acts of terrorism, policymakers must balance competing interests — personal privacy protections on the one hand against public safety protections on the other. This, of course, is no easy task. The mandate for a comprehensive privacy regimen is both present and compelling, particularly a federal privacy statute that preempts the growing number of inconsistent state privacy laws. Whatever regime the U.S. develops should be harmonized and coordinated with Europe, Asia and the rest of the world.

Congress should be careful not to overreach. In their zeal and earnest desire to protect individual privacy, policymakers run the risk of stifling innovation and stemming investment in future AI applications. While unintended, such a consequence could shift the leadership and momentum from the U.S. to Asia, where there is tremendous interest and investment in the further development of AI technology.

Looking ahead, the commercial market for AI is poised for significant growth. In 2019 alone, \$27 billion in new investment was committed to research and development, with 39 percent going to American companies and 13 percent going to China. These levels are sure to increase with rising demand from financial institutions, insurance and other sectors beyond law enforcement.

In the meantime, our world is becoming more dangerous every day. As we stand on the doorstep of this new frontier, policymakers should err on the side of public safety, but build in guardrails to protect our privacy.

While AI cannot undo the terrorism of the past, it could mean the margin between success and failure, life and death, security and danger for us all in the future. In that context, our society faces a Sophie's Choice, where either privacy or security will become the lesser casualty. Only time and the next incident will tell if we made the right choice.

Adonis Hoffman is CEO of The Advisory Counsel, Inc., chairman of Business in the Public Interest, Inc. where he leads the Responsible Technology Initiative, and founder of yourprivacymatters.org. He is a former chief of staff and senior legal advisor at the FCC and served in legal and policy positions in the U.S. House of Representatives. He has also served as an adjunct professor at Georgetown University. Hoffman has no business, equity, financial or lobbying interests in any of the companies mentioned in this article. Follow him on Twitter @AdonisHoffman.