Published on *The National Law Review* https://natlawreview.com

The Era of Retail Biometric AI Crime Has Begun

Article By:

Theodore F. Claypoole

Each new technology seems to offer creative tools for both criminals and law enforcement. Telegraphs and telephones spawned wire and phone fraud. The era of digital networking ushered in the age of hacking. Digital banking allowed distance identity theft.

As machine learning and artificial intelligence push deeper into our society as useful tools, their utility to criminals increases as well. Technically sophisticated criminals have been writing self-learning algorithms for decades that probe for system weaknesses, search out vulnerable information, and breaks poorly designed passcodes. Today's applications go deeper and are more shocking to the public. But we have reached the time where software's ability to fool our eyes and ears is passing into the criminal toolkit.

A recent and shocking example of this trend is the use of video deepfakes by a Pennsylvania mother to discredit her daughter's rivals on a high school cheerleading squad. According to multiple news reports, she targeted three teenagers in a Bucks County cheerleading program, harassing and attempting to implicate them with altered videos and spoofed phone numbers.

According to a New York Times story, anonymous messages sent to the girls, their parents and the owners of the gym where they practiced "contained doctored images and videos that attempted to incriminate the teenagers with fake depictions showing some of them nude, drinking alcohol or vaping. At times, the text messages took an even darker turn, telling at least one girl to die by suicide." Two weeks ago, the mother of one of their squad rivals was arrested and charged with using deepfake technology "to add likenesses of the girls to incriminating images."

Deepfake technology allows the user to take a still image of someone's face and map that face onto an existing video to make is seem like the target is committing a crime, a sexual act, or otherwise behaving in a compromising manner. The technology had been famously used in the recent past to map the faces of celebrities or ex-lovers on pornographic videos. Now it has become so prevalent to move to crimes involving neighborhood cheerleading rivalries. The Times article quoted the Bucks County district attorney as saying "This technology is not only very prevalent, but easy to use. This is something your neighbor down the street can use, and that's very scary."

If the amateur criminals can use this technology, imagine what the professionals will do with it. Two years ago a set of European criminals used AI voice software to perpetrate a most sophisticated version of the "email-from-your-boss" scam. They used software to mimic the voice of a CEO, leaving a message to tell his subordinate to send a large sum of money to an account that turned out to belong to the criminals. The money was quickly moved from the Hungarian bank account to Mexico and distributed elsewhere from there.

As told in a Wall Street Journal article the CEO of a U.K. based energy company thought he was speaking on the telephone to his boss, the CEO of the German parent company, who asked the U.K. man to urgently send $243,000 to a Hungarian supplier. He was told the payment must be made within the hour. No suspects had been identified at the time the WSJ article was written.

A representative of the victim’s insurance company talked to Forbes, telling them that the criminal “called the company three times: the first to initiate the transfer, the second to falsely claim it had been reimbursed, and a third time seeking a followup payment. It was at this point that the victim grew skeptical; he could see that the purported reimbursement had not gone through, and he noticed that the call had been made from an Austrian phone number.”

According to a 2020 study from University College London, fake audio or video content was ranked by experts as the most troubling use of artificial intelligence in terms of its potential applications for terrorism and crime. The study’s authors say “fake content would be difficult to detect and stop, and that it could have a variety of aims — from discrediting a public figure to extracting funds by impersonating a couple's son or daughter in a video call. Such content, they said, may lead to a widespread distrust of audio and visual evidence, which itself would be a societal harm.” They note that digital crimes can be easily shared, repeated and even sold, which would allow the tools to be marketed “and for the crime to be provided as a service,” therefore outsourcing the most technically difficult aspects of the crime.

We have seen a proliferation and democratization of hacking tools, and the hackers sell access to their most profitable tech. There is no reason to expect such services would not be built around voice and data artificial intelligence.

Note that not all is lost. Artificial intelligence and machine learning can also be used by law enforcement and private companies to challenge this technology, as it already is being successfully used to battle fraud. The financial industry has used AI for years providing real-time attack recognition and to isolate transactions likely to be fraudulent.

As the technology to digitally manipulate voices and faces becomes more readily accessible, easier to use, and better at fooling listeners and viewers, we will see more crimes committed using it. We will need to learn to question digital proof more often and to train ourselves not to believe our own ears and eyes.

National Law Review, Volume XI, Number 75

Source URL:https://natlawreview.com/article/era-retail-biometric-ai-crime-has-begun