ALM | LAW.COM

New York Law Journal

The DOJ Cracks Down on AI-Powered Crimes

By Christian Everdell and Marvin Lowenthal

March 29, 2024

Move over, crypto: artificial intelligence (AI) is the next frontier for the Department of Justice (DOJ). In recent public comments, Deputy Attorney General Lisa Monaco identified the emerging threat posed by AI as a top enforcement priority and announced that the DOJ will begin targeting crimes "made significantly more dangerous by the misuse of AI." To combat this threat, Monaco indicated that federal prosecutors will be using all means at their disposal to seek increased sentences for defendants in these cases, similar to those obtained in cases involving firearms.

Like the numerous criminal enforcement actions that followed the advent of cryptocurrency and digital assets, white collar practitioners can now expect a wave of indictments charging AI-powered crimes led by prosecutors with a mandate to seek tough penalties. But as Monaco recognized, it is not yet clear that existing statutes and Sentencing Guidelines enhancements will provide the DOJ with the tools they need to obtain the increased sentences they seek.

Courtesy Photos

Christian Everdell, left, and Marvin Lowenthal, right, of Cohen & Gresser.

Generative AI

The threat identified by Monaco is particularly acute with generative AI. Generative AI refers to a type of AI capable of creating (or generating) original content. Generative AI applications like OpenAI's ChatGPT/GPT-4, Google's Bard/Gemini and Anthropic's Claude are deep learning models that learn from being exposed to examples. After being trained on voluminous sets of raw data, these computer models can identify statistical patterns that enable them to create content that

is similar, but not identical, to the data on which they were trained.

Generative AI can even create original works that appear to have been made by specific people, such as an essay written in the style of a specific author or, more problematically, "deepfakes." Deepfakes can come in several forms, including fake audio recordings that sound exactly like a specific person or realistic but fictional images and videos that depict identifiable persons doing things they never did. These images, videos and audios have become so technically advanced that they are virtually indistinguishable from the real thing—and they are improving every day.

Not surprisingly, concerns have been raised over the criminal threat posed by increasingly realistic deepfakes, such as a widely reported phone scam in which parents received panicked phone calls in their children's voices saying that they had been kidnapped and would be harmed if the parents did not send money immediately. *See* Charles Bethea, "The Terrifying A.I. Scam That Uses Your Loved One's Voice," The New Yorker (March 7, 2024).

Generative AI can create original works that appear to have been made by specific people, such as an essay written in the style of a specific author or, more problematically, "deepfakes."

Monaco herself sounded the alarm about the use of deepfakes in the upcoming elections to impersonate trusted information sources and spread misinformation, noting that this already happened in New Hampshire where a deepfake of President Biden's voice was used in a robocall to discourage Democrats from voting in a primary. *See* Maggie Astor, "Behind the A.I. Robocall That Impersonated Biden: A Democratic Consultant and a Magician," The New York Times (Feb. 27, 2024).

ADOBE STOCKS

Monaco's Directive: Using AI Will Be Treated Like Using a Gun

Monaco outlined the DOJ's response to this threat in speeches at Oxford University in February and again at the 2024 National Institute for White Collar Crime in March. Touting both the potential benefits of AI for stopping criminals, terrorists and other threat actors and the potential risks AI poses to our collective security, Monaco declared that "[e]very new technology is a double-edged sword, but AI may be the sharpest blade yet." She expressed particular concern over the risks AI posed in a number of areas, including election integrity, theft of trade secrets and fraud.

Monaco's directive was clear: Deliberate misuse of AI technology that makes a crime "significantly more dangerous" or "significantly more serious" will be viewed by the DOJ as akin to using a firearm and will be dealt with harshly. In such cases, prosecutors will seek "stiffer sentences" to reflect the increased risks that AI poses to crime victims.

Monaco's reference to firearms signals the seriousness with which the DOJ regards the potential criminal threat of AI. The sentencing enhancements available for crimes involving firearms are some of the most severe that exist under federal law. For example, using a firearm to commit a crime of violence or a drug trafficking crime will result in a mandatory minimum sentence of five years, increasing to seven years if the firearm is brandished and ten years if it is discharged. *See* 18 U.S.C. §§924(c)(1)(A)(i)-(iii). The use of a firearm will also increase sentences for non-violent offenses, including fraud. *See* U.S.S.G. §2B1.1(b)(16) (two-level enhancement if the defendant possesses "a dangerous weapon (including a firearm) in connection with the offense").

Section 2B1.1(b)(10) provides for a two-level enhancement if the defendant committed a fraud offense using "sophisticated means."

The issue facing the DOJ is that, unlike firearms, there are no statutory penalties or Sentencing Guidelines enhancements specifically designed for crimes committed with AI—the technology is simply too new. Monaco acknowledged this potential problem when she stated that the DOJ will seek reforms if it determines that "existing sentencing enhancements don't adequately address the harms caused by misuse of AI." This leaves the open question: What tools can the DOJ use now and will they be adequate to the task?

Potential AI Sentencing Enhancements and Their Limitations

Let's consider these questions in the context of a hypothetical financial fraud offense, one of the areas that Monaco highlighted as particularly susceptible to the risks of AI. In this hypothetical, the defendant creates a sham crypto token and uses a publicly available generative AI application to create a deepfake audio recording of a well-known celebrity or sports figure (we'll use LeBron James) endorsing the new token. Investors are duped by the life-like recording and buy the token. They find out later that they have been scammed and the defendant has stolen their money.

The DOJ would likely view this as an example of a defendant making a garden variety token fraud "significantly more serious" by "deliberately misusing" generative AI to take advantage of James' celebrity to reach a wider audience of potential victims and potentially damaging James's own reputation in the process. But what are the available options for the DOJ to enhance the defendant's sentence for misusing the deepfake audio in connection with the fraud?

Aggravated Identity Theft

We begin with possible statutory penalties. As mentioned, there is no direct analogue to the firearm penalty enhancements in 18 U.S.C. §924(c) that would apply to AI-enhanced fraud. However, the aggravated identity theft statute—18 U.S.C. §1028A—offers a possible, but not perfect, option.

Section 1028A prohibits "knowingly transfer[ing], possess[ing] or us[ing], without lawful authority, a means of identification of another person" to commit certain enumerated offenses including wire fraud. 18 U.S.C. §1028A(a)(1). The term "means of identification," as relevant to this discussion, means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any… unique biometric data, such as fingerprint, voice print, retina or iris image or other unique physical representation." 18 U.S.C. §1028(d)(7)(B).

At first blush, Section 1028A seems to fit the bill. First, the deepfake audio is almost certainly a "means of identification" of LeBron James. The definition of the term includes a "voice print" of a specific individual. Although voiceprint technology pre-dates generative AI, it uses similar machine learning AI models to analyze samples of a person's voice to generate a unique voice identifier for that person. Moreover, any slight technical differences would likely be immaterial as courts have recognized that "means of identification" is "defined broadly" and the list of illustrative examples in the statute is non-exhaustive. *See, e.g., United States v. Dumitru*, 991 F.3d 427, 432 (2d Cir. 2021) (*per curiam*); *United States v. King*, 861 F. App'x 490, 496 (2d Cir. 2021).

Second, the defendant used James's voice "without lawful authority." To be sure, the defendant did not "steal" LeBron James's voice. Countless publicly available recordings of James speaking exist on the internet that could have been used to train the generative AI that created the hypothetical deepfake. Nevertheless, numerous courts have recognized that the "means of identification" does not need to be stolen as long as it was misused in some way. *See, e.g., United States v. Reynolds*, 710 F.3d 434, 436 (D.C. Cir. 2013) ("[U]se without lawful authority easily encompasses situations in which a defendant gains access to identity information legitimately but then uses it illegitimately—in excess of the authority granted" (internal quotation marks and alterations omitted)).

Finally, if the DOJ wants to obtain "stiffer sentences" for AI-related crimes, Section 1028A has real teeth. It imposes a mandatory two-year term of imprisonment that must be served *consecutively* with the sentence imposed on the underlying crime. 18 U.S.C. §§1028A(a)(1) & (b)(2). If the defendant is convicted of multiple counts of aggravated identify theft—for example, by creating additional deepfakes of Lionel Messi and Patrick Mahomes to endorse the token—the two-year terms will be stacked on top of each other, unless the judge decides to run them concurrently. 18 U.S.C. §1028A(b)(4).

However, Section 1028A may not be available in every AI-related fraud and may be vulnerable to limitations imposed by courts wary of extending the statute's reach. Just last term, a unanimous Supreme Court held that a defendant's "use" of a means of identification must be "at the crux of what makes the conduct criminal" to prevent the use of Section 1028A "well beyond ordinary understandings of identity theft." *Dubin v. United States*, 599 U.S. 110, 115, 131 (2023).

Dubin built on prior opinions from the U.S. Court of Appeals for the First, Sixth and Ninth Circuits that expressed concern about the statute's seemingly unlimited scope and the possibility that mandatory two-year sentences could be imposed far outside the heartland of identity theft cases. *See United States v. Miller*, 734 F.3d 530, 541-42 (6th Cir. 2013); *United States v. Medlock*, 792 F.3d 700, 705-07 (6th Cir. 2015); *United States v. Berroa*, 856 F.3d 141, 156 (1st Cir. 2017); *United States v. Hong*, 938 F.3d 1040, 1050-51 (9th Cir. 2019). These courts found that, under the circumstances presented, the defendant did not "use" a means of identification under Section 1028A because he did not try to "pass himself off" as the person whose identity was stolen or "purport to take some action" on that person's behalf. *Id*.

In our hypothetical example, the defendant's use of the deepfake audio is seemingly "at the crux of what makes the conduct criminal." However, if the court were to apply the reasoning

of *Miller*, *Medlock*, *Berroa* and *Hong*, the outcome is not so clear. The defendant is not passing himself off as LeBron James—*i.e.*, he is not trying to make his victims believe that *he* is, in fact, LeBron James—nor is he necessarily trying to "take some action" on James' behalf like obtaining a credit card in his name. He is merely coopting James's voice to mislead his victims that the real LeBron James endorses his token. Hence, prosecutors may not be able to use Section 1028A to enhance penalties for AI-related offenses in every court and in all circumstances. The DOJ may also feel constrained to charge Section 1028A narrowly to avoid further curtailment of the statute by skeptical courts.

Sophisticated Means and Use of Special Skill

Apart from statutory enhancements, the Sentencing Guidelines offer some familiar avenues for obtaining increased penalties for the deliberate misuse of AI, but again, not without complications. Section 2B1.1(b)(10) provides for a two-level enhancement if the defendant committed a fraud offense using "sophisticated means," which means "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." U.S.S.G. §2B1.1(b)(10) & cmt. Note 9(B).

Similarly, Section 3B1.3 provides for a two-level enhancement if the defendant committed the offense using "a special skill," which means "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing" such as "pilots, lawyers, doctors, accountants, chemists, and demolition experts." U.S.S.G. §3B1.3 & cmt. Note 4.

On the surface, these enhancements appear to be tailor-made to apply to the misuse of generative AI. Generative AI models are unquestionably sophisticated and were developed over several years by highly trained computer scientists and engineers. But what was once the exclusive province of technologists is now at the fingertips of anyone with access to the internet.

Indeed, someone with no "special skills" whatsoever, like our hypothetical token scam defendant, who does nothing more "sophisticated" than typing a simple prompt in a publicly available generative AI application can create a high quality deepfake of LeBron James's voice that can easily defraud countless victims. Will the "sophisticated means" and "special skill" enhancements apply under those circumstances? Defense lawyers will certainly have a credible argument that the answer is no.

Conclusion

The DOJ has staked out a new target and Monaco has issued a clear warning to would-be criminals: AI-generated deepfakes are the digital equivalents of loaded guns and if you deliberately misuse AI technology to commit your offenses, you will suffer the consequences. Whether the existing sentencing enhancements will apply broadly enough for the DOJ to obtain "stiffer sentences" for defendants in all circumstances, however, remains to be seen.

Christian Everdell *is a partner and* **Marvin Lowenthal** *is counsel at Cohen & Gresser.*