LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Harsher Penalties For AI Crimes May Work In Practice

By **Jennie VonCannon** (March 20, 2024, 4:02 PM EDT)


Jennie VonCannon

On Feb. 14, Deputy Attorney General Lisa Monaco, the second in command at the U.S. Department of Justice, announced to an audience at Oxford University a key development in how the DOJ and its prosecutors plan to address the dangers posed by artificial intelligence technology.

Calling it the "ultimate disruptive technology," she expanded her remarks about criminals' use of AI in the commission of crime, in San Francisco on March 7 at the American Bar Association's 39th annual meeting of the National Institute on White Collar Crime.

Monaco has likened the use of AI to commit a crime to the use of a weapon, calling it a "sword," and characterizing its misuse as "dangerous."

She has stated that "like a firearm, AI can also enhance the danger of a crime" by enabling criminals to "supercharge their illegal activities" and cause "especially serious risks to their victims and to the public at large."

Characterizing AI as "the sharpest blade yet" that can be wielded by criminals who would use it to commit crimes ranging from election fraud to corporate crime to cyber warfare, Monaco announced in February that DOJ prosecutors may now seek sentencing enhancements for crimes committed using AI technology.

Federal prosecutors have long been required to calculate proposed sentences by consulting the U.S. Sentencing Commission's Guidelines Manual, or USSG,[1] as the first step in recommending a sentence for convicted criminals. The guidelines provide a mathematical framework within which to calculate a criminal defendant's potential sentencing exposure by assigning numerical values to factors such as the nature of the crime, its impact on the defendant's victims, the defendant's role in the crime vis-à-vis any co-conspirators, and the defendant's criminal history — to name just a few.

The guidelines contain certain numerical enhancements that can be added to a base offense level for each federal crime, which means that the range of months that undergirds the foundation of a federal prosecutor's recommended sentence for a particular defendant will be higher should such enhancements be applied.

Monaco referenced enhanced penalties that can be sought for the use of a gun in the commission of a

crime when explaining that prosecutors may now seek similar enhancements when AI is used to commit a crime.

While there currently do not exist any enhancements in the sentencing guidelines specifically referring to the use of AI, prosecutors currently could potentially seek an enhancement using USSG Section 2B1.1(b)(1)(10)(C) for use of "sophisticated means." This enhancement would increase the defendant's offense level by two levels and, if their resulting offense level is less than Level 12, would set the floor of the defendant's offense level to 12.

In addition, prosecutors could also recommend that a court impose a more severe sentence for an AI-using defendant who also:

- May have used a special skill that is not possessed by members of the general public, such as being an AI programmer or having a Ph.D. in computer science, under USSG Section 3B1.3 — resulting in a two-level increase; or

- "[M]ay have misused special training or education to facilitate criminal activity," as outlined in USSG Section 5H1.2 — which does not include a level increase but rather may result in special conditions for probation or supervised release to protect the public from the defendant's misuse of AI technology by "restricting activities that allow for the utilization of a certain skill."

Monaco also stated in February that if existing advisory sentencing enhancements are deemed inadequate to address the harms caused by AI, the DOJ is committed to "seek reforms to those enhancements to close that gap." In doing so, DAG Monaco appears to have acknowledged that the current sentencing guidelines regime may prove to be inadequate to address what the DOJ considers to be the grave danger posed by the misuse of AI technology.

Since the U.S. Supreme Court's 2005 ruling in United States v. Booker that the sentencing guidelines calculations are advisory rather than mandatory,[2] courts are no longer required to hand down sentences within the range set forth by the USSG manual. Accordingly, federal prosecutors, defense attorneys and district courts alike must consider the factors set forth in Title 18 of the U.S. Code, Section 3553(a), in advocating for, in the case of the attorneys, and determining, in the case of the courts, a sentence for any federal crime.

Monaco's remarks indicate that federal prosecutors will be considering, among other things, the following Section 3553(a) factors that are relevant to whether a criminal will face stiffer penalties due to the misuse of AI technology:

- The nature and circumstances of the crime, including whether and how AI technology was used to commit the crime and heightened risks suffered by their victims or the public as a result;

- The need for the sentence to reflect the seriousness of the crime, promote respect for the law, and provide just punishment for the crime;

- The need for the sentence to deter the defendant from recidivating (specific deterrence) and to deter other would-be criminals who may be contemplating using AI technology to "supercharge" their crimes (general deterrence);

- The need for the sentence to protect the public from further crimes of the defendant; and
- The sentencing guidelines range, which will likely be higher as calculated by the DOJ as a result of federal prosecutors seeking enhancements for criminals aided by AI technology.

Consider a real-life example of how sentences could differ in light of the DOJ's new AI sentencing policy.

In February, the South China Morning Post reported that employees in the Hong Kong office of an unidentified multinational firm were tricked into sending over $25 million to scammers who used deepfake technology to impersonate the company's chief financial officer and other company personnel in a videoconference call where participants were convincing digital representations made possible by AI technology.[3]

Assuming that the ringleader of this scam was successfully convicted of wire fraud by a DOJ prosecutor, the sentencing guidelines calculation would begin with a base offense level of 6 per USSG Section 2B1.1(a)(2), plus a 22-level increase for causing over $25 million of loss, per USSG Section 2B1.1(b)(1)(L), resulting in an offense level of 28.

Assuming no other enhancements apply and that the defendant has little to no prior criminal history — i.e., is in Criminal History Category I — their resulting guidelines range would be 78 to 97 months of imprisonment.

If the DOJ prosecutor applied the "sophisticated means" enhancement of USSG Section 2B1.1(b)(1)(10)(C) because the defendant used AI technology to convince the victim employees that the company's CFO was ordering them to wire the $25 million, the defendant's range would increase to 97 to 121 months of imprisonment — meaning the use of AI technology alone would increase the defendant's sentence by 19 to 24 months.

And if the defendant personally created the deepfake videos by leveraging their computer science training, that same prosecutor may be able to convince a judge that the "special skill" enhancement also applies, which results in an additional two-level offense level increase per USSG Section 3B1.3. The resulting advisory sentencing range would increase to 121 to 151 months of imprisonment — about four years more than if the defendant in this scenario had not used AI at all.

Of course, this example illustrates Monaco's point: Without the deepfake AI technology, the malicious actors may not have been successful at convincing the employees that their CFO wanted them to wire $25 million — which is why the DOJ considers the misuse of AI technology as posing a particularly serious risk to victims.

Given that the sentencing enhancements for the misuse of AI technology can result in significantly higher sentencing guidelines ranges, attorneys for federal defendants should at the outset ascertain whether the defendant or any of their co-conspirators, if any, used AI to carry out the crime. It remains to be seen how tenuous the use of AI connection needs to be before a federal prosecutor refrains from seeking a sentencing enhancement, but it is safe to assume that it will be a very fact-specific inquiry that will behoove defense attorneys to get ahead of.

If such enhancements are applied, defense counsel will need to advise their clients about the potential for higher sentences, larger fines, and more stringent supervised release terms that could possibly severely restrict their clients' ability to use AI technology for a period of time.

And attorneys should remember that the sentencing guidelines calculations are only the beginning of the analysis that prosecutors, defense attorneys and district courts need to conduct in fashioning a sentence that is sufficient but no greater than necessary to address the crime. The Section 3553(a) factors are ultimately going to carry the day, so it is important for defense attorneys to understand the AI technology and how it was used to commit the crimes so that they can persuasively advocate for their clients within that framework.

Jennie Wang VonCannon is a partner at Crowell & Moring LLP. She served for over 11 years as a federal prosecutor, most recently as deputy chief of the Cyber and Intellectual Property Crimes Section of the National Security Division in the U.S. Attorney's Office for the Central District of California.

[1] Available at https://www.ussc.gov/guidelines/2023-guidelines-manual-annotated.

[2] United States v. Booker, 543 U.S. 200 (2005).

[3] Kong, Harvey, "'Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting," South China Morning Post, Feb. 4, 2024 (available at https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage).