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

Engaging With Feds On Threats To Executives, Employees

By **Jordan Estes** (February 5, 2025, 3:47 PM EST)


Jordan Estes

We live in an increasingly polarized environment where companies and their executives are facing serious concerns about how to protect their executives and employees from dangerous threats.

It's important that they consider every resource at their disposal when reassessing security. This includes one often overlooked tool: engaging with federal law enforcement early, after the discovery of threats or harassment.

As a former prosecutor who has overseen threat and cyberstalking cases, I know firsthand that law enforcement can serve as an invaluable partner in managing and mitigating these threats.

Engaging with federal law enforcement has many advantages. Federal prosecutors have broad power to investigate and prosecute electronic threats of violence and electronic communications designed to harass and intimidate an individual.

They have greater investigative tools that can be used to more readily identify the source of a threat, such as grand jury subpoenas, search warrants and warrants that track cellphone location.

Federal agents are also well equipped to assess the credibility of threats, which can, in turn, help companies identify what additional security measures may be warranted.

Of course, it remains to be seen how the new administration will handle threat cases, and whether federal law enforcement will continue to have the resources to investigate and prosecute them.

But early indications suggest that threat cases will continue to be a focus. For example, news reports have already suggested that the U.S. Secret Service is considering charges against an individual who threatened President Donald Trump on social media.

This article addresses the federal criminal statutes that can be used to prosecute threats and harassment, as well as the variety of tools law enforcement officers have to address those threats.

It then discusses the benefits of engaging federal law enforcement, and provides recommendations on how to approach federal law enforcement about investigating specific threats.

It also discusses how these cases may be handled under the new administration.

Federal Statutes Covering Threats

Federal prosecutors have two principal statutes available to investigate and prosecute threats and harassment against private citizens: Title 18 of the U.S. Code, Section 875, which criminalizes interstate threats of violence; and Title 18 of the U.S. Code, Section 2261A, which criminalizes cyberstalking.

For communications with explicit threats, Section 875 makes it a crime to transmit in interstate commerce "any communication containing any threat …to injure the person of another."[1]

To satisfy this statute, the government must prove that (1) the defendant knowingly transmitted a communication in interstate or foreign commerce, (2) the defendant subjectively intended the communication as a threat, and (3) that the content of the communication contained a "true threat" to injure.[2]

In interpreting statutes with identical language, many courts have held that the interstate-commerce element of the statute can be satisfied by showing that the internet was used for the transmission.[3]

Other courts have interpreted that language to require more direct proof of the interstate nature of the threat, but that proof could be something as simple as showing that threats were transmitted to interstate servers across state lines.[4]

In other words, most online threats of injury fall within the scope of the statute.

The cyberstalking statute covers an equally broad spectrum of communications. The statute applies to a person who, "with the intent to kill, injure, harass, [or] intimidate," uses a computer to engage in a course of conduct that "causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress."[5]

Unlike the threat statute, this statute covers communications that do not expressly threaten injury. A pattern of online harassment is enough, so long as the prosecutor can show that it caused, or would reasonably be expected to cause, emotional distress.

Both statutes have been used to prosecute threats and harassment at companies. Some prosecutions concern external threats or harassment, such as the prosecution of Rickey Johnson, who was convicted in 2022 in the U.S. District Court for the Southern District of New York for threatening various Fox News hosts over social media.[6]

The statutes can also address internal threats and harassment. For example, the government prosecuted former K&L Gates LLP partner Willie Dennis for cyberstalking other lawyers at the firm by sending thousands of emails and text messages with harassing messages like "I will find you" and "sleep with one eye open."[7] He was convicted in October 2022.

For prosecutors, the most challenging aspect of these cases is proving the requisite intent — that the defendant intended a communication as a threat (for Section 875), or that the defendant intended to harass or intimidate (for Section 2261A).

But companies without such evidence should not let that deter them from bringing threats or online

harassment to the attention of law enforcement. The mere fact of a threat or pattern of harassment can be enough to trigger a federal investigation, and the investigation is likely to uncover evidence of intent, or a lack thereof.

Law Enforcement Tools in Handling Threats

Once a federal investigation is open, federal prosecutors and their law enforcement partners have many tools to investigate the threats.

If the perpetrator is unknown, prosecutors can issue grand jury subpoenas to email providers, phone companies and internet service providers to investigate who is behind the threat.

They can obtain search warrants for email, iCloud and social media accounts, which could shed light on the credibility of the threat and whether the perpetrator is also threatening others.

And, significantly, they can obtain a warrant for cellphone tracking information, which they can then use to locate the perpetrator of the threats and confront or arrest the perpetrator.

Benefits of Engaging Law Enforcement

Some of the benefits of engaging law enforcement are obvious: They have more far more tools to investigate threats, and they have the power to arrest and prosecute individuals.

But there are even more benefits. A federal investigation may reveal if the perpetrator of the threat is behind threats to other individuals, or if the perpetrator has taken steps to act on those threats.

If the perpetrator has taken steps to act — such as by surveilling a target, hacking into a target's social media or email accounts, or visiting the target's office — the investigation may reveal weaknesses in the company's executive security measures that can then be cured.

Law enforcement officials can even end ongoing threats short of prosecution: A visit from an FBI agent or a deputy U.S. marshal is often enough to stop a perpetrator in their tracks.

Recommendations for Approaching Law Enforcement

Federal agents and prosecutors have limited resources, so it is important to approach them with the right information to get them to investigate and act with speed.

Explicit threats of violence will get their attention. But many threats are more veiled. In those situations, the company should be prepared to illustrate why the threats merit federal investigation.

For example, company counsel presenting to prosecutors could emphasize the large volume of concerning communications, because thousands of messages, even without explicit references to violence, may show that the perpetrator was intending to harass or intimidate the victim and cause them emotional distress, thus falling within the federal definition of cyberstalking.

Likewise, company counsel could focus on the escalation of communications from the perpetrator, which could suggest that the next level of escalation is concrete action.

Threat Cases Under the Trump Administration

Under the previous Trump administration, prosecutors routinely brought threat cases, including cases involving threats against political opponents of Trump.

For example, in 2019, an Arizona man was charged with violating Section 875(c) for threats against then-Rep. Adam Schiff, D-Calif., at the time Schiff was involved in Trump's impeachment inquiry.[8]

While it remains to be seen how threats with a political angle will be handled under the new administration, there is no indication there will be any deemphasis on nonpolitical threats. One of Trump's early executive orders — Executive Order No. 14164 on capital punishment and public safety, signed on Jan. 20 — states that the "Attorney General shall appropriately prioritize public safety and the prosecution of violent crime," which presumably encompasses cases involving threats of violence.[9]

However, the investigation and prosecution of threat cases also hinges on resources within the U.S. Department of Justice.

In some U.S. attorney's offices, such as the Southern District of New York, threat cases are often handled by the office's more junior prosecutors, while more senior prosecutors handle cases involving actual violence. A prolonged hiring freeze could affect the resources available to investigate and prosecute those cases.

Conclusion

Companies should proactively approach federal law enforcement after the discovery of online threats or harassment, so that federal law enforcement officers can investigate those threats with search warrants, subpoenas and cellphone tracking orders.

To prompt investigative action, companies should be prepared to emphasize explicitly violent communications, the volume of communications or the escalating nature of communications.

Jordan Estes is a partner at Gibson Dunn & Crutcher LLP. She previously served as an assistant U.S. attorney, the co-chief of the General Crimes Unit, and a senior member of the Securities and Commodities Fraud Task Force in the U.S. Attorney's Office for the Southern District of New York.

Disclosure: In her role as the co-chief of the Southern District of New York's General Crimes Unit, Estes supervised the prosecution in U.S. v. Dennis.

[1] 18 U.S.C. § 875(c).

[2] See United States v. White, 810 F. 3d 212, 220-21 (4th Cir. 2016).

[3] See United States v. Lewis, 554 F. 3d 208, 214-15 (1st Cir. 2009) (interpreting 18 U.S.C. §2252(a)(2) as it existed at the time); United States v. Runyan, 290 F. 3d 223, 239 (5th Cir. 2002) (interpreting 18 U.S.C.

§2251); United States v. Macewan, 445 F. 3d 237 (3d Cir. 2006) (interpreting 18 U.S.C. § 2252A as it existed at the time).

[4] See United States v. Sutcliffe, 505 F. 3d 944, 953 (9th Cir. 2007).

[5] 18 U.S.C. § 2261A(2)(B).

[6] United States v. Rickey Johnson, 21 Cr. 194 (S.D.N.Y.).

[7] United States v. Willie Dennis, 20 Cr. 623 (S.D.N.Y.).

[8] United States v. Jan Peter Meister, 19 Cr. 2738 (D. Ariz.).

[9] Exec. Order 14164, dated January 20, 2025.