Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

School Swatting: Overview of Federal Criminal Law

October 27, 2023

In September 2023, school districts in several states—including Pennsylvania, New York, Utah, California, and North Carolina—were reportedly subject to threatening hoax communications characterized as swatting—that is, communicating a false emergency in an attempt to direct an armed police response to a certain target or location, often as a prank or means of harassment. Many school swatting incidents have involved false claims of active shooters on school premises. Others have involved bomb threats. Swatting incidents targeting schools have resulted in significant police activity and disruptions such as lockdowns. One study by an educational nonprofit found that there were at least 446 swatting incidents specifically involving active shooter hoaxes in the United States during the 2022-2023 school year. The FBI is reportedly maintaining its own database of school swatting incidents. The phenomenon of school swatting has garnered widespread media attention and has prompted statements from some Members of Congress and other public officials. At least one state has enacted new legislation aimed at swatting, and other legislative proposals have been introduced at the state and federal levels. This Sidebar provides an overview of several federal criminal laws that may be relevant to school swatting incidents, discusses potential complications when prosecuting school swatting that originates abroad, and concludes with some congressional considerations.

Select Federal Criminal Statutes Relevant to Swatting

Depending on the circumstances, a school swatting incident may violate one or more federal criminal laws. As one federal prosecutor has explained, "Swatting scenarios can vary greatly, and consequently, charging options are highly fact-dependent." This section provides an overview of several federal criminal statutes that may apply to making a swatting communication, including statutes governing threats, hoaxes, and cyberstalking. None of these statutes expressly mention swatting or schools, but each has been used to charge swatting incidents either in general or specifically involving schools. Apart from the communications themselves, tactics used by swatters may also violate federal law. For example, swatters may rely on unauthorized computer entry to obtain the information necessary for executing their plans. Such behavior could implicate federal laws such as the Computer Fraud and Abuse Act and the wire fraud statute, both of which are discussed in CRS Report R47557, *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*, by Peter G. Berris (2023).

Congressional Research Service
https://crsreports.congress.gov
LSB11063

Interstate Threats to Kidnap or Injure, 18 U.S.C. § 875(c)

The Department of Justice (DOJ) has used 18 U.S.C. § 875(c) to charge individuals who engaged in swatting, including at least one who allegedly targeted schools. Section 875(c) authorizes fines and up to five years of imprisonment for threatening to injure or kidnap another. To violate § 875(c), the threat must be transmitted "in interstate or foreign commerce." Generally, that requirement may be satisfied where "a communication actually crosses state lines, however briefly." This could occur, for example, where a threatening communication, such as a phone call, is made from one state to a recipient located in another. Alternatively, the commerce requirement may also be satisfied where the recipient is located in the *same* state as the person making the threat if, for example, the threatening communication is conveyed by a phone call or instant message routed through equipment or computers located in a second state. At least one federal appellate court has examined whether use of the internet without proof that the message crossed state lines could suffice for § 875(c) purposes given the inherent "cross-border nature" of the internet, but it declined to resolve the issue, which it observed has divided other circuits in related contexts.

In light of First Amendment speech protections, federal courts have interpreted § 875 as prohibiting only true threats—statements conveying "an intent to commit an act of unlawful violence to a particular individual or group of individuals." According to the Supreme Court, "True threats of violence are outside the bounds of First Amendment protection and punishable as crimes." In its 2023 decision in *Counterman v. Colorado*, the Court clarified that a conviction for conduct "falling within that historically unprotected category" requires at least proof of recklessness. In other words, prosecutors must, at a minimum, "show that the defendant consciously disregarded a substantial risk that his communications would be viewed as threatening violence." A number of federal courts have required an additional mental state requirement on the part of a defendant to violate § 875—that he transmit the threat knowingly.

Bomb Threats, 18 U.S.C. § 844(e)

School swatting incidents that involve bomb threats may also violate 18 U.S.C. § 844(e). That provision makes it a crime to, among other things, threaten to kill or injure any individual "by means of fire or an explosive." The statute also prohibits maliciously conveying false information about attempts to kill or injure others with fire or explosives if the defendant knows the information is false. Caselaw examining the relationship between the false information language and the rest of the provision appears scarce, but as a whole, § 844(e) covers threats even where there is no "present intention" to carry them out. For example, DOJ has used the provision to prosecute hoaxes. To establish a violation of Section 844(e), prosecutors must prove that the defendant communicated a threat or false information through "the mail, telephone, telegraph, or other instrument of interstate or foreign commerce, or in or affecting interstate or foreign commerce." Additionally, at least one federal appellate court has said § 844(e) applies only to willful conduct. As with § 875, "§ 844(e) proscribes only 'true' threats." At least one person involved in a swatting scheme has been charged under § 844(e). In that case, DOJ alleged that the defendant violated § 844(e) by placing a "hoax telephone call from Massachusetts to emergency services in or near Denver, Colorado, falsely claiming that he had taken hostages, was armed with explosives, and would detonate his bombs and kill his hostages and any law enforcement personnel who arrived at the location." According to charging documents, the call was part of a larger swatting scheme to harass a specific person. The defendant pled guilty and was sentenced to a prison term of 30 months.

Hoaxes, 18 U.S.C. § 1038

Given that swatting incidents generally involve false reports of emergencies, another potentially applicable statute is 18 U.S.C. § 1038, which broadly speaking "criminalizes hoaxes simulating various

other crimes." Violations of § 1038 may result in fines and imprisonment for up to five years—or more if bodily injury or death result.

Section 1038 has been used to prosecute conduct such as reporting false bomb threats to law enforcement. The statute makes it a crime to engage in "any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation" of one of a number of other federal criminal provisions, including those governing terrorism and firearms. One underlying statute included in § 1038 may be particularly relevant to swatting schemes involving false claims of an active shooter: 18 U.S.C. § 924(c)(1)(A), which provides enhanced criminal penalties for, among other things, using or carrying a firearm "during and in relation to any crime of violence." In one case, DOJ used § 1038 to charge the defendant for placing hoax telephone calls to emergency services in California "falsely claiming that he had taken hostages, was armed with explosives and firearms, and would detonate his bombs and shoot hostages and any law enforcement personnel who arrived at the location" of his intended victim. DOJ asserted that, had these claims been true, the underlying conduct would have violated § 924(c)(1)(A).

Cyberstalking, 18 U.S.C. § 2261A(2)

DOJ has also used 18 U.S.C. § 2261A(2) to prosecute swatting schemes, including at least one that involved a threatening communication to a school. Section 2261A(2) imposes criminal penalties for, among other things, using the internet, social media, websites, emails, texts, or other similar technologies to "engage in a course of conduct" that:

- places a person "in reasonable fear of the death of or serious bodily injury" to that person, "an immediate family member," a "spouse or intimate partner," or a person's "pet, service animal, emotional support animal, or horse;" or
- "causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress" to a person or that person's "immediate family member" or "spouse or intimate partner."

Penalties for § 2261A(2) violations generally include fines and up to five years of imprisonment, but Congress authorized higher penalties in cases involving dangerous weapons, resulting in injury or death, or where the victim is a child. Section 2261A(2) includes two important statutory limitations. First, as indicated, it applies only when the defendant engages in a course of conduct—that is, "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose." Second, § 2261A(2) requires proof that the defendant intended "to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person." These requirements suggest that § 2261A(2) may be most relevant to school swatting if the threatening communication targeting the school is actually part of a broader scheme to harass a particular individual. For example, in 2023, a defendant pled guilty to numerous cybercrimes, including a § 2261A(2) violation, stemming from swatting calls targeting an individual. Although some of the defendant's calls were intended to cause a police response at the victim's personal address (and succeeded in doing so), in others he impersonated the victim in swatting messages transmitted "to a high school, a restaurant, and a sheriff's department."

Prosecuting Swatting Originating Abroad

Swatting communications received in the United States can originate abroad, and some recent reporting suggests that this may be true of numerous school swatting incidents. DOJ has charged foreign individuals in connection with swatting schemes. The cyberstalking prosecution described above is one example: The defendant (a citizen of the United Kingdom) was arrested in Spain and extradited to the

United States, where he pled guilty and was sentenced to five years of imprisonment. One pending case is that of a Peruvian national arrested in September 2023 by Peruvian law enforcement based on a criminal complaint filed in the Southern District of New York, which alleges that he violated federal criminal statutes including §§ 875 and 1038. Among other things, federal prosecutors assert that the defendant emailed bomb threats to multiple school districts in Pennsylvania. To the extent the perpetrators of swatting targeting schools in the United States are located in other countries, domestic prosecution may turn less on the legal scope of the relevant statutes and more on practical considerations and matters of foreign relations. As another CRS product explains, investigating and prosecuting criminal conduct originating in other countries raises questions of national sovereignty and may involve "legal, practical, and often diplomatic obstacles that can be daunting." For example, the United States lacks extradition treaties with some countries, which may make domestic prosecution of criminals residing in those countries challenging.

Congressional Considerations

As discussed, school swatting may already violate a number of federal criminal statutes depending on the circumstances. The nature of swatting calls—which may cross state borders or employ technologies such as telephones and the internet—can run afoul of statutes such as 18 U.S.C. § 875(c), which focuses on threatening communications transmitted in interstate or foreign commerce, or 18 U.S.C. § 2261A(2), which requires the use of technologies like the internet to engage in a threatening course of conduct. These characteristics of swatting also provide potential constitutional authority for Congress to enact additional criminal laws on the subject pursuant to its power to regulate interstate and foreign commerce. Several bills have been introduced on the topic of swatting in general or school swatting specifically, including at least one in the 118th Congress. Select examples include:

- The **Preserving Safe Communities by Ending Swatting Act of 2023**, H.R. 3913, 118th Cong. (2023), would expand the federal hoax statute (18 U.S.C. § 1038) to criminalize engaging "in any conduct with intent to convey false or misleading information" by "using the mail or any facility or means of interstate or foreign commerce, under circumstances where such information may reasonably be expected to cause an emergency response and the information indicates that conduct has taken, is taking, or will take place that constitutes a crime under State or Federal law or endangers public health or safety or the health or safety of any person."
- The **Anti-Swatting Act of 2019**, H.R. 156, 116th Cong. (2019), would have, among other things, amended a federal statute governing robocalls to include a criminal penalty for violations with "the intent to trigger an emergency response in the absence of circumstances requiring such a response."
- The **Stop Swatting in Our Schools Act of 2016**, H.R. 4804, 114th Cong. (2016), would have directed the FBI to establish a task force to investigate swatting and refer incidents for prosecution.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer