

The Opinion Pages

When a SWAT Team Comes to Your House

This Week in Hate

By ANNA NORTH JULY 6, 2017

This Week in Hate highlights hate crimes and harassment around the country since the election of President Trump.

Three families had to evacuate their homes in Florida in January after someone sent an anonymous email to a detective, claiming to have placed bombs at their addresses. The case, discussed at greater length in This Week in Hate on Wednesday, was unusual in that the only apparent connection between the victims was their surname, Gonzalez. But it was also an example of a kind of harassment that's become disturbingly common: a practice called swatting.

In a swatting, someone makes a fake report of a bomb or shooter at a victim's address, hoping to draw law enforcement officers, such as a SWAT team, to the house. This can be terrifying and sometimes dangerous, as heavily armed officers arrive at the home of an unsuspecting person. In 2015, a 20-year-old man in Maryland was shot in the face with rubber bullets by police after someone allegedly reported a fake hostage situation at his house.

The FBI has estimated that about 400 cases of swatting occur nationwide every year, but anecdotal reports suggest the numbers are far higher than that, according to Rep. Katherine Clark, Democrat of Massachusetts, who introduced an anti-swatting bill in Congress in 2015. In addition to the physical risks, swatting also wastes law enforcement time and money — some cases have cost police departments as much as \$100,000, Ms. Clark said.

It's not clear why the Gonzalez families in Florida were singled out for swatting. But swatters have targeted a variety of people for a variety of reasons, going after celebrities and micro-celebrities (the creator of the “Damn Daniel” meme was swatted last year), video game developers, politicians and ordinary people they met online. Women and girls are more likely than men to be the target of severe online abuse like swatting, Ms. Clark noted.

After she introduced the bill, Ms. Clark herself was the victim of swatting. She was watching TV with her husband when police cars pulled up to her house; when she walked outside, she saw officers with long guns on the lawn. Even though she knew all about swatting, she felt a “moment of terror about what was unfolding.”

For the majority of victims, who have never heard of swatting before, the experience can be confusing and chaotic. “Because the homeowners know things are safe in their house, they don't understand who they are seeing outside their windows,” she said.

Finding a potential victim's address is easy for would-be swatters. If you marry, divorce, buy a home, register to vote, get a driver's license or start a business, your address can become part of a public records database. Data brokers like Spokeo and Intelius scour these databases and make the information available online, some of it for free. While users can ask to have their information removed, the process can be laborious; there are hundreds of data brokers, and some require a government-issued ID to remove personal information. A few online safety groups offer advice for removing personal information from data broker sites. Even when removed, however, the information can crop up again.

If swatting is relatively easy, investigating and prosecuting it is hard. Swatters often mask their real phone numbers, IP addresses and even their voices, and

tracking them down can be expensive and time-consuming. One detective sergeant in Georgia estimated that he spent 1,000 hours investigating a swatting outside Atlanta, according to a report in The New York Times Magazine.

Swatting also presents jurisdictional problems. If a call or email is placed from one state but the victim lives in another, it may not be clear who should investigate or prosecute the case. If the swatter lives outside the United States, the case becomes even more complicated. The perpetrator in the Atlanta case turned out to be a teenager in Canada who went by the pseudonym Obnoxious and boasted on Twitter that he could not be extradited — he was arrested by Canadian police nearly a year after the Georgia incident, after he had executed several more swatting attacks. In that case, the F.B.I. agreed to help with the investigation, but only because the suspect had made dozens of swatting calls. In the case of a one-time threat that appears to pose no physical danger, the bureau may decide its limited time and money are better spent elsewhere, said Anthony Roman, a security expert.

Representative Clark's 2015 anti-swatting bill did not get a vote, but in June, she introduced a new bill called the Online Safety Modernization Act that includes anti-swatting provisions. The bill would solve some of the jurisdictional issues associated with swatting by making it a federal crime. "It would no longer matter if the crime was called into Massachusetts but the person happened to be calling from Utah," Ms. Clark said. The bill would also impose stiff penalties for swatting, including up to 20 years in prison if someone is seriously hurt as a result of a swatting attack.

"I think this is the type of bill that we can build bipartisan support for," she said of anti-swatting legislation, "even in a Congress where that can be difficult to do."

If you have experienced, witnessed or read about a hate crime or incident of bias or harassment, you can use this form to send information about the incident to This Week in Hate and other partners in the Documenting Hate project. The form is not a report to law enforcement or any government agency. These resources may be helpful for people who have experienced harassment. If you witness harassment, here are some tips for responding. You can contact This Week in Hate at weekinhate@nytimes.com.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion),

and sign up for the Opinion Today newsletter.

© 2017 The New York Times Company