



ASPEN TECH
POLICY HUB

POLICY



ANJANA RAJAN

Combating Domestic Terrorism

Empowering Witnesses to Fight White Supremacist
Extremism While Protecting Civil Liberties

EXECUTIVE SUMMARY

From the attacks at the Emanuel African Methodist Episcopal Church in South Carolina to the massacre at the Tree of Life Synagogue in Pittsburgh to the mass shooting of an immigrant community in a Walmart in El Paso, mass gun violence perpetrated by white supremacist domestic terrorists is an increasing national security threat. Many attacks such as these could have been prevented if the witnesses who observed the perpetrator's concerning behaviors prior to the attack had reported such behavior to law enforcement. Unfortunately, [nearly 60% of witnesses](#) prior to a mass shooting chose not to do so. Their reasons for not reporting included distrust of the police, loyalty to the perpetrator, self-doubt of their own risk assessment, and a desire for anonymity to protect their privacy and personal safety.

The FBI should endorse a two-point solution to address the low witness reporting rates: 1) a **cryptographic reporting escrow** to enable witnesses to report confidentially to a non-government third-party, such that the information is only revealed when the severity crosses a certain threshold, paired with 2) a nuanced **threshold-based risk model** that identifies white supremacist terrorist threats. This solution could fundamentally change the trust relationship between communities and law enforcement and ultimately save lives.



PROBLEM

Community witnesses have the ability to prevent terror attacks, yet that intelligence isn't being gathered effectively

Domestic terrorism is a rising threat. This is particularly true of violent white supremacist extremism, which since September 11, 2001 has been responsible for [more deaths on U.S. soil than jihadist terrorism](#). Fighting domestic terrorism is difficult because law enforcement agencies cannot use the same aggressive tools that they use for foreign terrorism. Under [Section 215 of the USA PATRIOT Act](#), the government can counter a designated foreign terrorist organization (FTO) using tools such as deploying electronic surveillance, delaying notification of a search warrant, and using orders to obtain business and bank records through the FISA Courts. Domestic terrorism cases, in contrast, do not have a federal statute to prosecute similar crimes; such terrorism is briefly defined in Section 802 of the USA PATRIOT Act, but the relevant provisions only apply to crimes affiliated with al-Qaeda, ISIS, or other officially designated FTOs.

This means that similar acts face divergent results under U.S. law. For example, if a U.S. citizen donated money to al-Qaeda, the federal authorities could take immediate action under laws that enable them to investigate those who provide illegal, material support to a foreign terrorist organization. However, if that same citizen donated money to a white supremacist organization, federal authorities could not investigate him or her unless there was evidence that force, coercion, or violence was being planned or had already occurred. This is because the PATRIOT Act only focuses on FTOs. Adversaries who commit acts of terror on behalf of groups that do not belong on the FTO list are exempt from surveillance and are protected under the First Amendment, which protects the citizen's privacy from prospective law enforcement examination. The perpetrators of the [2015 Charleston Emanuel AME church shooting](#) and the [2017 Unite The Right rally murder](#) were not charged with terrorism, but rather with firearms, attempted murder, federal hate crimes, and state criminal charges.



Because of these discrepancies, many [counterterrorism experts argue](#) that white supremacist groups should be designated as foreign terrorist organizations. They argue that there are noticeable similarities between white supremacist extremists and jihadists: both groups use violence to create a climate of fear and chaos; they rely heavily on propaganda to radicalize followers; they use technology platforms to recruit new members; and they utilize real-world war zones to learn physical combat. Congressman Max Rose recently authored the [Transnational White Supremacist Extremism Review Act \(H.R. 5736\)](#), which would direct the Department of Homeland Security to develop and disseminate a terrorist threat assessment of foreign, violent, white-supremacist extremist groups. This bill was endorsed by the Anti-Defamation League and was unanimously approved by the House Committee on Homeland Security.

Some have argued that Congress should pass a [more expansive domestic terrorism statute](#) that would allow federal agencies to prosecute these crimes equally. However, civil liberties groups cite [free speech concerns](#) about outlawing and surveilling extremist groups based on ideology. [The ACLU has strongly opposed](#) this legislative proposal, stating that an expanded terrorism statute would “undermine and violate equal protection, due process, and First Amendment rights.” Even [Michael McGarrity](#), head of the FBI’s Counterterrorism Division, said that “we probably would not want something that is similar to what we have on the international side, which is designating foreign terrorist organizations. Picking out particular groups that you say you disagree with their views is going to be highly problematic.”

In the absence of comprehensive legislation to counter white supremacist terrorists, there are still ways to help improve how such incidents are identified, prevented, and prosecuted. One such possibility is to elevate the role of witnesses and better enable them to report what they know. There is evidence that witnesses can play a critical role in preventing acts of mass violence. According to an [FBI study on the pre-attack behaviors of active shooters between 2000 and 2013](#), there



were, on average, three distinct witnesses who observed concerning behaviors by the shooter. While the severity of these behaviors varied, 56% of the time the behavior observed was “leakage,” a term coined by the FBI that is defined as the communication to a third-party of an intent to harm someone. Unfortunately, nearly 60% of those witnesses chose not to inform law enforcement. There are many reasons why witnesses choose not to report: they distrust law enforcement; the perpetrator is a person they care about and the witness does not want to get them in trouble; they are uncertain about whether their assessment of the risk is accurate; and they have a desire to remain anonymous in order to protect their privacy and personal safety. This low reporting rate means we are losing a valuable source of intelligence that could help prevent these deadly attacks.

Community-based counterterrorism programs to encourage witness reporting have been attempted before, but not without controversy. Following the July 7, 2005 London bombings, the UK created [Pre-vent](#), a subset of a national counterterrorism program that focuses on educating communities about the risk of radicalization and staging interventions before a crime has been committed. However, [critics of the program](#) argue that this type of program is discriminatory, particularly against Muslim communities.

There needs to be a witness-centric, ideology-agnostic system that can build trust with community witnesses in three ways. First, witnesses must trust that there is a safe and confidential way to report. Second, witnesses must trust that their actions will lead to a de-escalation of violence. Finally, witnesses must trust that their actions will lead to a calibrated and compassionate response.



SOLUTION 1

A cryptographic reporting escrow

The problem of low witness reporting rates can be best understood as a [game theory](#) problem. Simply put, this means that there is a first-mover disadvantage for a witness who has observed a concerning behavior to report to law enforcement without knowing if their observation meets a credible threshold of risk. Additionally, they may only want their observation to be seen by law enforcement if they believe that other witnesses have observed concerning behaviors, too. Therefore, ordinary channels for reporting to law enforcement can present significant privacy and civil liberties risks for both the accuser and the suspect.

A third-party [cryptographic reporting escrow](#) is an ideal solution for situations in which somebody should report something in order to protect society, but may be reluctant to come forward on their own. Such an escrow would be a trusted third-party system (that the government does not own or have direct access to) that allows witnesses to report concerning behaviors. The report is only unlocked and given to law enforcement if and when a threshold of severity is met.

Cryptographic escrows build trust in a fundamentally new way. Four key principles define such systems:

- ▶ **Threshold-based:** One witness's record stays locked until a threshold of risk is met by one or more people;
- ▶ **Zero-Trust Network:** The data stored in the escrow is protected from both [outside and inside threats](#);
- ▶ **Human Legal Firewall:** The record is unlocked by a person who can establish privilege and block false accusations; and
- ▶ **Multiple Calibrated Options:** Witnesses have several options for how they choose to take action.



Below is an example of how a cryptographic escrow might work in a counterterrorism use case:

A witness submits a report into an encrypted, third-party, non-government reporting platform, providing details about themselves, the suspect, and the observed concerning behavior.

That entry stays encrypted so that nobody (not law enforcement, and not even the escrow provider) can see the details of the record unless one or more other witnesses report the subject's risky behavior. The records in the escrow would only be unlocked if a threshold of risk is observed by one or more people. This creates a low-risk environment for a witness because nobody can see the accusation unless a credible threshold of risk is met.

A second record is created about the same suspect. Once this happens, the escrow automatically transmits the decrypted records to a legal counselor. This attorney provides free confidential counseling to the witness(es) about their reporting options. The legal counselor provides two firewalls: first, as a lawyer, they can establish attorney-client privilege and protect their conversations against a subpoena. Second, they can filter out false accusations by malicious actors before they are escalated to law enforcement.

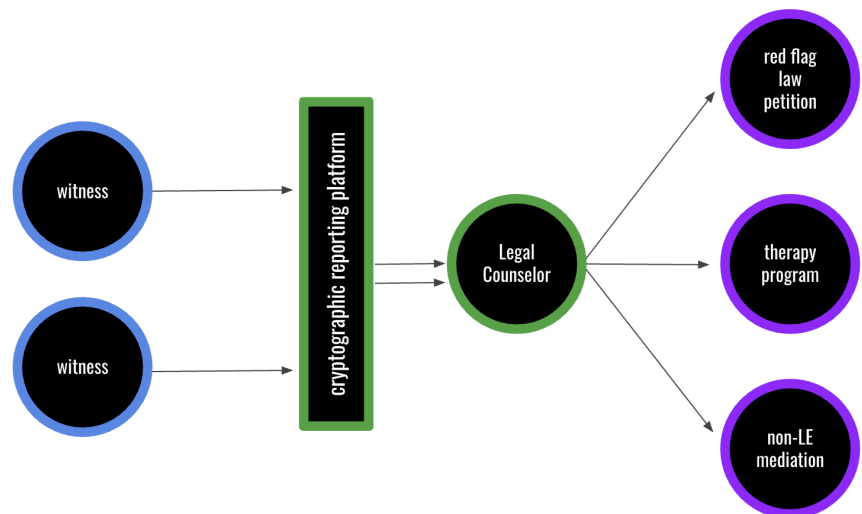
The counselor then explains a variety of calibrated actions a witness can take. It is critical that witnesses have a range of options to choose from because less severe evidence requires a less severe response. By having more compassionate options for intervention that go beyond informing law enforcement, the process enables the witness(es) to see that reporting will not just get somebody they might care about in legal trouble, but could also help somebody they care about get help.



In addition to reporting to law enforcement, the actions available to witnesses could include helping the suspect enroll in therapeutic programs that provide wrap-around support and social services. Examples include:

- ▶ Cognitive behavior therapy;
- ▶ Mentoring;
- ▶ Family counseling;
- ▶ Drug and alcohol counseling;
- ▶ Pro-social activities (i.e. team sport);
- ▶ Vocational rehabilitation; and
- ▶ Life-skills training.

Witnesses could also file a [red flag law petition](#) (also known as an extreme risk protection order) to confiscate weapons from the suspect. A red flag law is a gun control law that allows family members and police to petition a state court to have [weapons temporarily removed](#) from a person deemed at risk of causing harm to themselves or others. While [red flag laws](#) exist only on the state level and vary state-by-state, they have proven to be effective. A [study](#) of the efficacy of extreme risk protection orders in Connecticut shows that, for every 10 to 20 risk warrants issued, one life is saved. Under extreme or immediate cases of imminent violence or abuse, the counselor would be obligated to report directly to law enforcement.





SOLUTION 2

Threshold-based risk model

Perhaps the most complex question to be answered is, how do we define what behaviors are risky, and what is the threshold of risk that should unlock the escrow? The risk threshold component is particularly complex in counterterrorism cases because a crime has not yet been committed. Therefore, it is important that the threshold is designed thoughtfully and built correctly. On one hand, the risk model should prevent false negatives that avoid missing signs of mass terror. On the other hand, the risk model should also prevent false positives in order to avoid stereotyping based on race or religion.

The risk model proposed in this project looks at four key elements as inputs:

- ▶ **Element 1:** Relationship proximity between the witness and the suspect;
- ▶ **Element 2:** Concerning behaviors observed by the witness about the suspect;
- ▶ **Element 3:** Multiplicative impact of concerning behaviors and active gun possession; and
- ▶ **Element 4:** A defined threshold of risk to unlock the escrow.

A separate technical white paper with more details about how these were selected and measured can be found [here](#).



ASPEN TECH POLICY HUB

POLICY

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

CONCLUSION

The tumultuous events of 2020 have underscored that eradicating mass terror caused by white supremacist extremists continues to be an urgent crisis that requires a multidisciplinary approach. In just the last six months, white supremacist groups reportedly have planned to [car bomb a hospital](#) and discussed using the coronavirus as a [bioweapon](#); [gun sales have increased](#) significantly during the pandemic; [domestic violence has increased](#), widespread police brutality and systemic racism have drastically [broken public trust in law enforcement](#), and [fringe extremist groups](#) have weaponized disinformation about COVID-19 and infiltrated peaceful protests with acts of violence.

There is an opportunity, amidst the chaos of this current moment, to reimagine what public safety looks like, and develop solutions that protect our communities from violent extremism, protect civil rights and liberties, and elevate compassionate and calibrated de-escalation channels in lieu of traditional law enforcement. A privacy-preserving solution, such as a threshold-based risk model and a cryptographic reporting escrow, could help strike the balance of pursuing our national security goals while protecting our civil liberties.



**ASPEN TECH
POLICY HUB**

Combating Domestic Terrorism