

# A View from the CT Foxhole: Five Years after the Boston Marathon Bombing

By Nicholas Tallant

*William Weinreb stepped down as Acting United States Attorney for the District of Massachusetts in January 2018. He was the Lead Prosecutor of the 2015 investigation and trial of Boston Marathon bomber Dzhokhar Tsarnaev. In 2016, Weinreb received the Attorney General's David Margolis Award for Exceptional Service—the highest honor in the Department of Justice—for his role in investigating and prosecuting Tsarnaev. Weinreb previously served as First Assistant U.S. Attorney, Counsel to the U.S. Attorney, and Deputy Chief of the National Security Unit. He also served as the Coordinator of Massachusetts' Anti-Terrorism Advisory Council. He has served as an Assistant U.S. Attorney since 1995—in the District of Massachusetts since 2000 and in the District of Columbia in 1995-2000. Weinreb graduated cum laude from Harvard Law School.*

*Harold Shaw has served as the Special Agent in Charge of the Federal Bureau of Investigation's Boston Division since 2015. Shaw previously served as the Special Agent in Charge of the Counterintelligence and Intelligence Divisions of the New York Division. From 2011 to 2013, he served as Assistant Special Agent in Charge within the Counterterrorism Division of the New York Division. Shaw has served with the FBI since 1999, primarily in the New York Division. During his tenure at the FBI, he has investigated a variety of international and domestic terrorism matters, including the USS Cole bombing and the September 11, 2001, attacks. Shaw earned a Bachelor of Science degree from Norwich University. Prior to joining the FBI, Mr. Shaw served as an officer in the U.S. Army for more than nine years.*

*The views expressed in this article do not necessarily reflect those of the Combating Terrorism Center, United States Military Academy, Department of Defense, or U.S. Government.*

**CTC: April 15th marks the five-year anniversary of the 2013 Boston Marathon bombing. The term “Boston Strong” surfaced quickly in the attack’s aftermath to describe the unified response. Independent reports point to the well-developed and planned incident management procedures as a particular strength.<sup>1</sup> How have these preparations changed since 2013, whether in Boston specifically or for other similar events nationwide? And how does that relate to the broader changes in the nation’s counterterrorism capabilities since 9/11?**

**Weinreb (USAO):** We had been preparing for an event like the Boston Marathon bombing ever since 9/11. Boston was affected by 9/11 in a special way because two of the planes originated from here. As a result, many of the victims were from here. The chief lesson we learned from 9/11 was the importance of coordination, collaboration, information sharing, and being prepared to tackle the next

event together and work seamlessly.

One important change since 9/11 is that the U.S. Attorney's Offices around the country, particularly the larger ones, have increased their level of resources and expertise devoted to national security threats. When 9/11 occurred, we didn't have any attorneys in the Boston U.S. Attorney's Office whose expertise or whose responsibility was in anti-terrorism or other national security matters. Now we have seven full-time lawyers dedicated to just that one area. All of us are expected to be experts not only in counterterrorism but also in illegal export enforcement, espionage, misuse of classified information, and other areas. That's a big change.

When the Boston Marathon bombing occurred, there were already a number of us who were very experienced at doing counterterrorism cases. We immediately co-located with the FBI. We knew how to assist in the investigation, getting the information that was needed using the kinds of tools that only prosecutors have access to, like grand jury subpoenas, search warrants, and 2703(d) orders—orders that allow you to get certain telephonic or email communications. We were part of the investigation from the very first day and continued to be part of it even after the suspect was in custody.

**Shaw (FBI):** I was serving in the Counterterrorism Division at FBI Headquarters, as a lead detailee to the CIA, during the Boston Marathon bombing. When talking about the importance of the greater Joint Terrorism Task Force concept, in that capacity, I was briefing updates on the attack to the Director of the CIA on a daily basis. Looking at how we as the FBI and the greater Intelligence Community have evolved since 9/11, you now have an FBI agent, embedded in Langley, briefing the Director of the CIA on what was happening in Boston. You see how the world has changed in terms of information flow, interconnectedness, and interdependence.

I often use Massport [Massachusetts Port Authority] as an example of an agency that has evolved and adapted, specifically from being impacted by a terrorist attack. On a daily basis, Massport conducts a daily intelligence briefing tailored to threats with all of its critical stakeholders, including the FBI Boston Division. This began immediately following 9/11 and continues to this day. They understand the importance of information sharing, preparation, and consistently looking for what could have been missed. Are we as coordinated as we need to be? As for lessons learned from 9/11, they still live it today in terms of the importance of sharing information, specifically regarding the terrorism threat. That's what it takes to proactively get in front of an attack.

**Weinreb (USAO):** The U.S. Attorney's Office—along with all the other federal, state, and local law enforcement agencies that have a stake in terrorism prevention and response—had been coordinating closely and doing tabletop exercises, planning out how we would respond to the next event, since 9/11. When the Marathon bombing occurred, everything came together seamlessly. All the relevant

agencies and state and local law enforcement officers knew where to go and what to do. Control of the various crime scenes moved seamlessly from the first responders to state and local law enforcement, who were there immediately on the ground, to the FBI and federal law enforcement, who were responsible for the long-term investigation.

Every time you have an event like the Boston Marathon bombings, you see what lessons you can learn from it. We did do quite a number of after-action reports to see what we could learn and how we could improve. In many ways, the lesson we learned was that we had prepared well. We needed to keep doing what we had been doing.

**Shaw (FBI):** One takeaway is a term often used in the military—train as you fight. We rely heavily on the use of table-top exercises. In some instances, we conduct Command Post Exercises to ensure communications work and are coordinated as necessary. We ensure interconnectivity, not only with our databases and systems, but also by having the right people assigned and trained to support our Joint Intelligence Center or prepared to participate in an FBI or partner agency Tactical Operations Center. Within our office, any time we can capitalize on even a smaller scale operation, whether arrest or search, we make sure we are including our partner agencies as appropriate to get the greatest benefit. That has proven to really build the interconnectivity to be able to deal with larger scale events.

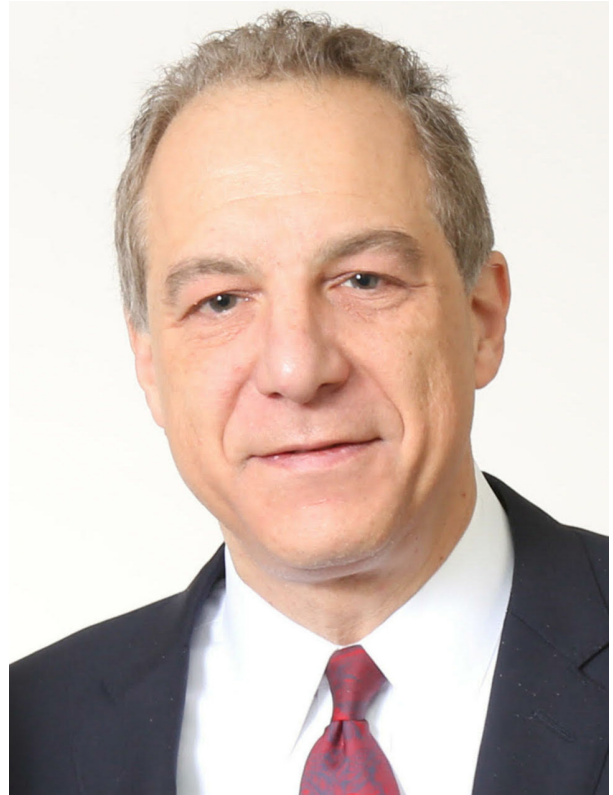
The other takeaway is the importance of intelligence. Prior to 9/11, it's not necessarily that the FBI didn't use and push intelligence, but we didn't do it well *enough*. In today's threat environment, we're really trying to stop something before it happens. The investigative side alone is not going to get you where you need to be. It's the ability to not only develop, analyze, and share intelligence but also to integrate intelligence into all of our operations—and efficiently move this information to fusion centers and other departments. Whether in the planning for the marathon or other special events, we share intelligence and develop an intelligence assessment—a Special Event Threat Assessment.

It's really critical to look both domestically and internationally. An example I often use is Manchester. What changed in terms of that attack? An attack on egress. Historically, law enforcement has done a very good job of hardening events in advance of the event itself, whether it be a playoff game at Gillette Stadium, fireworks on the Esplanade, or the Boston Marathon. The concern now is whether we're doing as good a job of assessing the threat post-event. Does everybody leaving the marathon getting on the "T" [subway] become vulnerable? Now, with changes in tactics, considerations need to be made and a plan implemented on how we're addressing crowds after the event. It's a potential vulnerability.

A final development after 2013 has been better engagement with the private sector and private security firms. Gillette Stadium has been a perfect example of this integration.

**CTC: How has the evolving terrorism threat influenced preparations for this year's marathon?**

**Shaw (FBI):** The planning starts almost immediately after the marathon for the following year. It's a synergy between federal, state, and local partners as well as the private sector. With the marathon, the Boston Athletic Association has embraced the need for and the significance of a good, coordinated security plan.



*William Weinreb, former Acting U.S. Attorney for the District of Massachusetts (USAO)*

A marathon has complexities in comparison to, say, Boston's 4th of July Esplanade fireworks celebration. Those are fixed and finite areas. There's a direct and practical way to harden them. Now, look at 26.2 miles for the marathon. A number of different departments—whether law enforcement, emergency management, fire, or private sector entities—all support the event in one way or another. Along a route of that expanse, it's a significant lift to not only secure but harden it. How do we appropriately disperse investigative and tactical resources? No one agency necessarily has the investigative, response, or tactical resources to cover 26.2 miles. We have developed a comprehensive plan, which is better integrated to more quickly respond to certain areas along the route. That all has to be worked out well in advance, whether it be emergency response, investigative, tactical, bomb, or evidence response.

One of the biggest changes in the past few years is the use of a vehicle as a terrorism device. In support of the marathon, more departments are bringing out heavy equipment and sand trucks to shut down access points or corridors potentially vulnerable to vehicular attacks. As part of the security planning process, a lot of time and effort goes into assessing potential weaknesses or vulnerabilities and how we best counter these threats. Specifically, those were lessons learned from attacks in Nice and New York.

As an emerging and developing threat, we are continually concerned about a potential attack through the use of a UAV [Unmanned Aerial Vehicle]. The FBI is consistently working with our partners on how to best determine what technologies are available and how we must coordinate with the FAA [Federal Aviation Administration] and others who manage airspace to best address the possible threat.



*Harold Shaw, Special Agent in Charge of the Federal Bureau of Investigation's Boston Division (FBI)*

**Weinreb (USAO):** The security for the Boston Marathon these days is absolutely first-rate. There are some legal mechanisms in place to prohibit UAVs in certain areas. The Coast Guard has the authority to prohibit UAVs in certain circumstances in areas within its jurisdiction. The FAA can prohibit them within areas within its jurisdiction. The law regarding UAVs is still evolving. If it becomes problematic, then we would press to make sure we have the legal authority to neutralize any threat.

**CTC:** Given the sheer number of marathon spectators in 2013, many people fleeing the area left bags, backpacks, and packages on the ground. How does that complicate incident response and evidence collection?

**Shaw (FBI):** The chaos needs to be managed as best as possible, but there is a process. First and foremost, we have to secure the area and assess the next threat. In some instances, the greater concern is not only the potential for a secondary or tertiary device; there have also been far more complex attacks seen globally, with everything from a VBIED [Vehicle-Borne Improvised Explosive Device] to an active shooter to separate suicide bombers. We have to factor all these in while moving as quickly as possible to render aid to the victims.

Initially, our goal is not necessarily the painstaking and detailed effort of evidence collection. It's ensuring the area is safe and secure. Even to allow our emergency first responders—whether EMS or fire—into the area, it has to be secured first. You want to evacuate the wounded as quickly as possible but want to do it in a fashion that isn't going to compromise or impact the crime scene.

For all those bags, backpacks, and packages, we do all that we can to identify the owners, as we know they are potential witnesses, victims, or even possibly subjects.

**Weinreb (USAO):** For every single item on the scene, at the time you're collecting it, you don't know whether it's going to be important evidence or not. So everything has to be collected in a certain

manner, catalogued, tagged, and so on. It's very labor-intensive and time-consuming. Of course, people will also want those things back, so then there is a process down the road to reunite people with their belongings.

**CTC:** About 72 hours after the bombing, the FBI released the pictures of two suspects, enlisting public help to identify the Tsarnaev brothers.<sup>2</sup> Can you address the trade-off between soliciting public help and working behind the scenes to identify suspects? How do you manage the immense outpouring of information from the public once help is solicited?

**Shaw (FBI):** It's a fine line. Oftentimes, we know it's not only the public watching, but also the subjects, conspirators, or facilitators. It's a balance to get information out and request public assistance for any information they may have. But, you're also potentially tipping off the perpetrators or the conspirators. Unfortunately, the more information that gets into the media, it's also providing intelligence for those conspirators to react. The other issue is—based on the way it's portrayed in the media—that it may cause a panic or concern within the community. Needless to say, a lot of thought, coordination, and discussion amongst your partners goes into how to manage the message and what is shared through the media.

After some great work, analysis, and exploitation, the pictures that we had of the subjects were crystal clear. However, as the case goes, the first time we fully identified Tamerlan Tsarnaev was after the quick-capture fingerprint at the morgue.

**Weinreb (USAO):** You always want to try to control the investigation to the extent possible. That often means holding information close. Particularly, you don't want to reveal any information that will taint witnesses. For example, if you release a picture of somebody you think is a suspect, a witness who might have seen the actual person might now think, "Oh, I must have seen it incorrectly because this is what the person looks like." Then, their memory becomes cloudy or may be affected by the picture you released. Generally speaking, you don't want to risk that.

In addition, we were concerned that if we released the photos, the bombers would know that we were on to them. They might decide the jig was up and that it was time to make a last stand. On the other hand, you don't want to go too long without making the pictures public and essentially crowd-sourcing the identification process. The ultimate goal is to determine who they are before they decide to regroup and commit another offense or flee the country or any number of things that would be bad for public safety. It's always a tough choice that involves balancing many competing concerns.

**Shaw (FBI):** There are competing interests. The team really didn't have a choice because the media was going to release them. When you have a large task force and are sharing information freely and transparently, information gets out.

There's always greater benefit to transparency. We've found that throughout the years. The real challenge is that we have to value and understand that different stakeholders have different responsibilities. As we are moving on the investigation, political leaders, governmental officials, and law enforcement representatives all have responsibilities to their communities. And, their communities are looking for information about what is going on. So, it's striking the appropriate balance on what needs to be disseminated in the best

interest of the community, public safety, and the investigation.

Another concern, especially today, is attacks that have spawned other attacks. While not necessarily copycats, we're mindful that successful attacks have the potential to motivate other individuals, who are on the path of radicalization, to react or mobilize to violence.

The Boston Marathon bombing, in particular, was one of the first really big cases where the FBI and our law enforcement partners were deluged with digital evidence. By the end of case, we had collected 28 terabytes of information. Specifically, after the pictures were published—within those first 24 hours—we had 10,000 online tips, 10,000 videos, and 113,000 images that were sent to us. In addition, there were 250 million visits to the FBI.gov website to look at the pictures. How did we handle that within a 24-hour period? We needed to triage it. We have a transfer system where we can intake information and get it down to our headquarters. There, 150 agents and analysts were standing by to exploit and analyze it. What pictures or images were relevant? What's a real video or still image that was actually taken at the scene?

You're not only looking at this information for lead or intelligence purposes, you're also looking at it for evidentiary purposes. Did you go through all of it? Is there information that helps you identify a co-conspirator? Is there information that might be exculpatory to individuals who may not have been involved? That was a huge lesson learned from the Boston Marathon bombing. Looking at a picture or a video, it's really some compelling evidence. Although scouring through digital media can be laborious and challenging on a number of accounts, it can be invaluable evidence and really move a case along.

**Weinreb (USAO):** When you are prosecuting a case with that quantity of information, the easiest and safest way to ensure the defense is getting any potentially exculpatory information is simply to share all that information with them. That way, they have everything. If there's exculpatory information in there, they have it. That was, by and large, what we did in this case. When it came to these massive quantities of information, like the hundreds of thousands of photos and all the videos, they were digitized. We put them on hard drives and shared them with the defense, so they had the same access to them that we had.

Of course, the government is just as interested in uncovering exculpatory information as in identifying inculpatory information. If we find any, we share it with the defense. I do believe that every single photo and every video was looked at by somebody on the investigative team at some point over the two years between the bombing and the trial. It requires a huge amount of resources, and it may not be necessary to obtain a conviction, but we'd rather have as much information as possible and get the evidence that is both inculpatory and exculpatory, rather than not have it at all.

**CTC: The manhunt for the Tsarnaev brothers throughout Boston was a particularly notable feature of the 2013 event. Some cite it as the first real test of post-9/11 interagency coordination. We witnessed a similar search for the San Bernardino suspects in 2015. How have procedures evolved since 2013?**

**Shaw (FBI):** The biggest difference between the Boston Marathon and the San Bernardino attack was the duration of the manhunt following the respective incidents. Once the threats were mitigated in

San Bernardino, the FBI and its partners could more quickly move from crisis management to investigative and evidence collection efforts. In Boston, there were a series of different crises that needed to be contended with, including the initial attacks, fugitive hunt, and follow-on attacks on a law enforcement officer and private citizens.

Interagency coordination has improved for a number of different reasons. First, all of our partners fully understand the threat, its "real" impact on the community, and that we're all on the front lines when defending the public we serve. Second, we depend on each other and value the skills each agency brings to the table. A great example is our bomb technicians go through the same FBI-sponsored training in Alabama. Now, with the same training, it's easy to interchange parts when you have a bombing issue, but more importantly, relationships are built from the ground up. We rely on the skills each brings to the table. I couldn't be prouder of the quality of the partnerships seen across the Boston law enforcement community. Having been attacked, facing the demands of crisis, and understanding the reliance we all have on each other's agencies has aided in fostering critical partnerships across the region.

One of the more important points is that all of our partners here in Boston fully recognize that we are going to "win or lose as a team." Especially during any post-incident assessment or after-action review, we all understand there is room for improvement without casting blame or fault. Was sharing as efficient as it could have been? What was missed? What could have been done better?

We all understand our roles, responsibilities, and how we can best leverage each other's capabilities. We, as a law enforcement community, also understand the importance of incident command and how to capitalize on the unified command structure in crisis. For example, if a significant attack or event were to occur right now in Boston, Commissioner Evans [Boston Police Department] is leading the response and crisis. I know my role. I'm standing side-by-side with him, supporting him, and bringing all my resources to bear. It does not matter whether it is a counterterrorism event or not, we will be there to assist. If, through the initial response and investigation, it looks to be a terrorism-related matter or other federal violation, the FBI will take the investigative lead but continue to work alongside the Boston Police Department as part of the unified command.

**CTC: A May 2017 CTC *Sentinel* article by Frank Straub discussed the unique risks faced by local patrol officers being the first to respond during terror incidents.<sup>3</sup> He focused on the San Bernardino and Orlando incidents, during which high-powered weapons and explosive devices played a role. Boston witnessed very similar patrol officer involvement during the search. Can you comment on those challenges, particularly when terrorism is suspected?**

**Shaw (FBI):** It's a timely question because over the last two weeks, we've had the FBI's On-Scene Commander for the Pulse nightclub shooting [Orlando] and the former Assistant Director in Charge of the Los Angeles Division who managed the San Bernardino attack meet with our law enforcement partners to discuss some of the challenges that they faced. From my perspective, it's one thing to share after-action reviews, it's another to bring those individuals who were part of the events to share and discuss the challenges they faced. It offers the opportunity—whether for our chiefs or tactical operators—to ask questions of those individuals that actually went

through it. Yes, it is more than likely a local problem first. They are the first responders. They are the first people that are going to have to address the threat. In both of these incidents—Pulse and San Bernardino—the threats were mitigated by the effective response by our state and local partners.

The reality is that none of us are ever going to have the resources to do it all on our own. For a protracted event, such as Pulse [Orlando], additional teams were brought in, such as FBI negotiators, and were prepared to take over as needed. Anytime there is a suspicious package, that's a collaborative effort. It's not only the Boston Police Department or Massachusetts State Police bomb squads rolling out. There's an immediate interface with the FBI Special Agent bomb technicians that there's a potential device out there. Based on the initial assessment, we'll provide the necessary resources, whether it be bomb, evidence, or JTTF investigative support.

It's probably the most difficult job when you, as a patrol officer, come across the information that a person may be a subject of interest following a terrorism incident. They were possibly involved in committing a terrorist attack, so what do they have to live for now? Believe me, the FBI is keen to provide any and all available intelligence—whether photos, identifiers, or license plates—to the regional fusion centers, JTTF partners, and respective departments.

**CTC:** There were reports in the press that the Tsarnaev brothers and Pulse nightclub shooter were all known to law enforcement. Similar reports have surfaced following terror attacks overseas as well. Can you discuss the challenges faced in preventing attacks?

**Weinreb (USAO):** Many of the challenges will be quite familiar. We live under a legal system in which people cannot be restrained. You can't restrain their liberty or take away their rights just because you fear that they may commit a crime.

When we get wind of the possibility that somebody is a potential terrorist, we investigate it to the extent the law allows. The FBI has some pretty elaborate sets of rules that limit to what degree they can pry into somebody's life—to what degree they can investigate them—based upon the mere suspicion of terrorist activity. The degree to which they can investigate is commensurate with the information that they have and the nature of the threat. It's somewhat the same for us in the U.S. Attorney's Office. We have certain legal tools that are available to us only if we have probable cause to believe that the person has committed a crime, and oftentimes, we don't have probable cause.

A couple of the investigative challenges we face that have been in the news recently are encryption and the inability of law enforcement to get into locked cell phones. Another challenge is people who are on the internet or in other forums espousing radical extremist beliefs of one type or another. We can't take action against people merely because of their beliefs, even if experience has shown that people with those beliefs sometimes later commit terrorist acts. People can think and say what they want. Only when they mobilize and actually begin to plot and plan or actually prepare to engage in an attack can you step in and do something about it.

**Shaw (FBI):** Relative to these instances, even when the FBI does have information about certain individuals, it doesn't necessarily mean that we can mitigate the potential threat via an arrest. Intelligence can often drive a case, as can sophisticated techniques used throughout the investigative process. We are continually discerning

the degree of threat, building evidence, working with our U.S. Attorney's Office, and devising strategies on how best to mitigate that threat through arrest or other means. We are continually looking for the most efficient and effective way to address the threat. In some instances, it might be through an interview; in others, leveraging the capabilities of a local police department. It's an ongoing struggle to stay in front of the threat and find the best ways to prevent incidents from occurring.

Ongoing assessment is key. We are bound by the rule of law and our Constitution. After investigating and assessing the threat with some individuals, you may not necessarily have enough to continue with a case. Cases are built on predication, and we don't keep cases open indefinitely. We're not only focused on protecting and securing the country from terrorist threats. We're equally as concerned about protecting and maintaining the civil liberties and protections of the American people. If the intelligence or the evidence developed does not support the continuation of an investigation, we will move to close that investigation and will reassess if new intelligence or information develops.

**Weinreb (USAO):** Unlike the 9/11 attack, which was preceded by a lot of planning and preparation and a lot of communication among the people that were involved, these days people often radicalize and then mobilize to violence extremely quickly without much communication with others—sometimes with no communication with others—with few resources and with little planning. There are not that many opportunities to apprehend them.

One of the best ways to find out if people are up to something is, believe it or not, to just go and ask them. If you talk to them, a lot of people will voluntarily tell you things. One thing will lead to another, and you'll find out useful information that can really benefit you in an investigation. These are completely voluntary interviews called "knock and talks."

**Shaw (FBI):** One major change that came out of FBI Boston was routine and periodic reassessments of past counterterrorism cases. During high-threat periods—whether an upcoming special event, significant holiday, a domestic attack, or an attack overseas—we'll conduct comprehensive assessment scrubs. We go back and revisit some of these assessments—which are previous reporting of suspicious activities or threats that do not reach the threshold of a fully predicated investigation. The threat has become more dynamic and ever-changing, and unfortunately, the "flash-to-bang" or radicalization-to-mobilization period has shortened for many of these subjects. We continue to reevaluate if world events or some other catalyst will drive somebody to mobilize to violence? Based on past attacks, someone usually knows something, sees something out of the norm, or—as a by-stander—may have a critical piece of information.

Modes of radicalization have dramatically shifted over the past 10 to 20 years. As of recent times, many of the individuals prone to supporting terrorist causes or potentially involved in future U.S. attacks do not even have to travel overseas. At one point, travel was a critical tripwire that helped us discern if somebody was truly committed to joining or supporting al-Qaeda, AQAP, al-Shabaab, ISIS, or Hezbollah. Now, the new dynamic is that the same radicalization can occur simply through online correspondence. Overseas travel is still an important indicator, especially now with foreign fighters who may be leaving Syria or Iraq. However, just as concerning are those individuals that don't need to travel to conduct jihad or be

involved in jihad. They can do it by engaging with like-minded folks online.

**CTC:** Once Dzhokhar Tsarnaev was apprehended, some public debate surrounded the decision to read Tsarnaev a Miranda warning. Some questioning occurred before the Miranda warning under the warning’s “public safety exception.” Can you discuss the Miranda “public safety exception” and the impact of that determination?

**Weinreb (USAO):** The “public safety exception” reflects a balancing of individual rights under the 5<sup>th</sup> Amendment against the needs of the public for public safety. What the Supreme Court said was that the 5<sup>th</sup> Amendment “right to remain silent”—just like every Constitutional right—is not absolute. Sometimes, it has to give way to a compelling government interest. When a terrorist attack occurs, the danger may not be over. There may be other terrorists, other bombs or other people who were part of the plot who may be ready to continue once the suspect has been captured. When the circumstances suggest that is possible, then there is a compelling public interest in getting answers to those questions that overrides the person’s 5<sup>th</sup> Amendment rights. That’s the basis of the public safety exception.

One of the difficulties of doing a public safety interview is knowing how many questions you can ask before you have to stop—when the Supreme Court would say that you have asked enough questions to safeguard the public such that the person’s 5<sup>th</sup> Amendment rights once again outweigh the public’s need to know. In order to make the decision correctly, you need input both from the investigators—in this case, the FBI were most familiar with the facts and what the dangers to the public were—and the lawyers, the NSD [National Security Division], and parts of the Department of Justice that are experts in this area. This ensures that this is a proper situation in which to do “un-Mirandized” questioning and helps identify what questions are permissible to ask and how long the questioning can go on. It’s absolutely an area where you would want to have input from as many people with knowledge and expertise as possible.

**Shaw (FBI):** “Quarles”<sup>a</sup> or the public safety exception is used solely to obtain information on an ongoing threat. Our goal at that point in time is to get any needed information to stop an ongoing threat to life. It’s very limited in scope. It doesn’t necessarily go into the greater history of the case. Once it leaves that sphere of what’s still a threat, it stops. Miranda kicks in.

I can still remember back to Faisal Shahzad, the Times Square bombing, and being part of that. With any bombing or terrorist attack, the bigger issue will be determining what other devices are out there. Does the threat continue? Are there other attacks planned? For example, did the individual booby trap the residence in which he was staying? Does the car he drove have an explosive device? Are there co-conspirators who have a follow-on attack planned? That is the scope.

**CTC:** Tsarnaev was successfully convicted in 2015 of using a

weapon of mass destruction in addition to 29 other counts. This successful prosecution is another distinct feature of this event. How does that particular WMD charge change the nature of the case if at all? And are there other notable features of the case’s prosecution?

**Weinreb (USAO):** Using a weapon of mass destruction is not a crime that is charged every day. Even when it’s charged, it is not often that the case goes to trial. And it’s usually only at a trial where the fine points of the law and what the requirements are for proving a violation of it are hashed out.

That was particularly true of another of the statutes that we charged a violation of—one called “bombing a place of public use.” That was a statute that, I believe, had been charged only a couple of times before, and none of those cases had gone to trial. That was one where we had to make new law when it came to what that statute required us to prove.

The case involved another law—called “using a firearm or explosive device during and in furtherance of a crime of violence resulting in death”—that is not often charged. In a situation like this, you have a combination of bombs and guns, and you have people not just getting hurt, but actually being killed. That raised some novel legal questions as well.

This case really combined many elements that are not often found together in a criminal case. You had a crime that affected thousands and thousands of people. Hundreds were injured. Seventeen were maimed. Four were killed. It involved terrorism. It involved the use of weapons of mass destruction. Because it was a capital case, it implicated all the issues that were involved in capital cases, of which there are many.

There was a challenge to the venue of the case—whether it could lawfully be tried in Boston or not. That was a major issue during the pre-trial proceedings. There were witnesses who were all over the world who had to be found and safely brought to the U.S. to testify on behalf of the defense. That was a particular feature of the case. There were really a lot of interesting and difficult challenges in this case from a prosecutor’s standpoint.

**Shaw (FBI):** From the law enforcement side—whether us in the FBI or our partners on the JTTF—our role and responsibility is conducting a full and comprehensive investigation, the collection of evidence, and the timely sharing of intelligence. We will process, analyze, exploit and collect as much information as possible to advance that case or support a potential prosecution. We’ll have to attest to that evidence at trial. It’s the U.S. Attorneys that make the determination on how the case is going to be charged based on the information developed through the course of our investigation.

**Weinreb (USAO):** Most challenging was making sure we did the right thing by the victims, that we gave them an opportunity to tell the world what had happened to them, and that we got the full accounting out. There had been so much in the press that was heard by people in bits here or bits there. Very few people understood how it really all unfolded from beginning to end or really understood the magnitude of the harm that it did to people who were victimized by it. We felt a real special responsibility to tell that and to allow the victims to tell it in their own words.

**Shaw (FBI):** The victims of these horrific crimes are always with us. We seek to bring justice to those who have been impacted through

<sup>a</sup> *New York v. Quarles* was a 1984 decision by the United States Supreme Court regarding the public safety exception to the Fifth Amendment requirements of the Miranda warning.

compassion, sensitivity, and diligence in our work. As tragic as the Boston Marathon bombings were to this city, our country, and our friends around the globe, it was a seminal moment for those of us within the Greater Boston law enforcement team. It made us better, more connected, and driven to stop the next potential attack from happening. Our workforce, JTTF, and partners could not be more committed to proactively identifying the next threat and mitigating

it with speed, thoroughness, and through lawful means. We take the threat of terrorism personally. We've been attacked, and we know how it feels. When you've been through it, you also understand the importance of working together, the reliance on sound and trusting partnerships, and the need to efficiently share information with the goal of stopping an attack before it occurs. **CTC**

## Citations

- 1 Herman Leonard, Christine Cole, Arnold Howitt, and Philip Heymann, "Why Was Boston Strong? Lessons from the Boston Marathon Bombing," Program on Crisis Leadership and Program in Criminal Justice Policy and Management, Harvard Kennedy School, April 3, 2014.
- 2 "Remarks of Special Agent in Charge Richard DesLauriers at Press Conference on Bombing Investigation," Federal Bureau of Investigation Boston, April 18, 2013.
- 3 Frank Straub, Jennifer Zeunik, and Ben Gorban, "Lessons Learned from the Police Response to the San Bernardino and Orlando Terrorist Attacks," *CTC Sentinel* 10:5 (2017).