TESTIMONY OF EDWARD F. DAVIS III, FORMER COMMISSIONER OF THE BOSTON POLICE DEPARTMENT and FOUNDER OF THE EDWARD DAVIS COMPANY

EMERGING THREATS AND SPENDING OVERSIGHT SUBCOMMITTEE
UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

APRIL 26, 2023

Chairwoman Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, I would like to thank you for the opportunity to testify at today's hearing to examine the lessons learned in the 10 years since the Boston Marathon Bombings and the many security advancements that have been made to protect the United States.

The impact of the terrorist bombing and resulting investigation at the Boston Marathon, on Patriots Day that took the lives of three people, Lu Lingzi, Krystle Campbell, and Martin Richard, at the scene and injured hundreds of others forever changed the City of Boston. The 2013 Boston Marathon bombing also significantly strengthened how law enforcement, the media and the community respond to these grave incidents and the way we conduct terrorist investigations.

I believe it's important to focus on the advancements and pivotable changes that technology has provided to investigations of this magnitude. Improved technology, including communication technology; video and photographic evidence; the use of social media; and the rapid evolution of machine learning and more recently, AI, have contributed to expediency, accuracy, and protection of the American public throughout the last ten years.

Since 2013, the government has made significant improvements in the realm of security measures, including cyber security, border security, and emergency response planning. These improvements include more advanced technologies, more comprehensive, planning, and increased public education and awareness supported by many private-public relationships and innovative companies. As I discuss some of these companies and their impact on public safety, I recognize there is always more work to be done. The advancement of technology will require strong consideration of privacy rights and protections lead by Congress, research, and funding priorities for technological resources impacting the landscape of policing and investigations.

As I testified in 2013, during the Boston Marathon Bombings cell network capabilities dropped for all of those in the direct vicinity of the attacks. Overwhelming numbers of phone calls, texts, and internet searches rendered voice communications practically useless for everyone, including the police officers on scene and those responding. With a lack of a secure network, communications between municipalities, local and federal law enforcement were impeded and change was critically important.

As a member of the Board of Advisors for AT&T and the company's FirstNet platform, I've seen the public private partnership of FirstNet take on this challenge and improve first responders' ability to communicate on scene. The development of FirstNet was conceived by Congress following 9/11 and came to fruition in 2012 when Congress created the "First Responder Network Authority" after over 10 years of public safety advocating. And I thank Congress for this critical legislation. In 2018, the network finally launched "The FirstNet Core, a physically separate and highly secure infrastructure that creates a differentiated experience for first responders. The Core is essential to providing many of the vital functions and capabilities public safety relies on to support their mission-critical work. The goal of FirstNet is to provide law enforcement and first responders the ability to access a highly secure and completely reliable service network during times where commercial servers become overwhelmed, exactly when it is needed most. FirstNet could have increased police capability and potentially impacted the lives of many of today's survivors. Additionally, while it was not a concern at the time of the bombings, the external threats to first responders' communications is a problem we face today. FirstNet ensures an encrypted, end-to-end communication network for law enforcement. Another aspect of technology that has seen great improvement is the proliferation and AI capabilities of video and photo surveillance, both private and public.

It has been well documented that the use of video surveillance from Boylston Street restaurants and photos provided by spectators that were at the scene of the attack led to the identification of the two suspects and provided a timeline of their movements after the attacks, leading to their apprehension. Law enforcement combined video with analytic resources available quickly and effectively.

That said, one of the most significant advantages of new AI-driven imaging devices is in the ability to transform traditional video surveillance systems into real-time data sources and proactive investigative tools. Today's cameras and coordinated systems have the potential to provide analytics in real time; identify possibly dangerous items, as well as react and pivot based on crowd dynamics such as abnormal movement patterns or gathering. Video analytic companies can also provide proactive solutions to crime problems. For instance, Genetec has sophisticated cameras that leverage radar and

LiDAR capabilities combined with machine learning. They use AI software like Vintra that can learn from normal activity and notify operators of approaching threats and of anomalies. This solves manually searching the overwhelming amount of data produced by use of thousands of cameras. Another company, Altumint, uses proprietary AI networks designed to detect and process traffic violations. This innovative tool allows for data driven traffic calming tactics and allows law enforcement to shift limited resources to other priorities.

Reliance on this data, however, presents its own challenges. There is so much information and data that it can be used to interfere in ongoing investigations. As has been noted, the FBI and law enforcement agencies had to sift through thousands of photos minute by minute and authenticate them. The public used those same tools to doctor photos. They photoshopped a suspicious person on a roof near the attacks and photoshopped a bag at the attack site in another photograph. These edited photos added an additional challenge necessitating us to verify and rule out fakes from the public, complicating the monumental task already at hand.

Ten years later, as artificial intelligence continues to mature, these capabilities grow exponentially more dangerous. AI can now create realistic, false images of people and voice replication. These "deep fakes", when used to interfere or disrupt an investigation pose a distinct challenge to law enforcement that Congress and legislation must anticipate and prepare for. Laws and regulations need to be formulated to safeguard this profound technology advancement as it continues to expand. Nefarious use of AI presents a clear and present danger to the safety of the American public.

At the time of the bombings, law enforcement agencies also faced the issue of wading through and verifying information being pulled from the scene, tips from the public, and witnesses while also coordinating inter-agency decisions on how and when to share verified information with the public. The Boston Marathon Bombing was one of the first incidents where law enforcement utilized the tools of social media, such as Twitter, to communicate directly with the public and media agencies. This was the Boston Police Department's most effective way to share pertinent safety information to the masses in real-time. As was published in a white paper I helped pen for the National Institute of Justice's Harvard Executive Sessions on Policing and Public Safety in March 2014[1], "[*The Boston Police Department] successfully used Twitter to keep the public informed about the status of the investigation, to calm nerves and request assistance, to correct mistaken information reported by the press, and to ask for public restraint in the tweeting of information from police scanners. This demonstrated the level of trust and interaction that a department and a community can attain online.*"

[1] Davis III, Edward F., Alejandro A. Alves, and David Alan Sklansky. "New perspectives in policing." (2014).

"One of the lessons of the marathon bombing investigation is that a police department that has worked to earn the public's trust can use social media to disseminate information directly to the public without the traditional intermediary of commercial news operations. This is the power of publishing: the ability of the police, with reasonable effort, to be the source for accurate, timely information that seizes the public's attention and contributes to public awareness and understanding in critical ways."

The landscape for social media has grown exponentially since April 2013 and must be capitalized on by law enforcement entities as one of our lessons learned. I'd like to credit the Department of Justice and the COPS office for their insight to provide guidelines and considerations for law enforcement to use social media in both community building and tactical responses over the last 10 years. One of the immediate takeaways from over ten years ago was the need to manage public involvement and perception. The community plays one of the biggest roles in providing investigative leads. The Pew Research Center has reported that in May of 2013, approximately one month after the bombings, 61% of Americans reported using at least one social media platform, that number has risen to 72% in February of 2022, and importantly, eight-in-ten U.S. adults (86%) say they "often" or "sometimes" get news from a smartphone, computer, or tablet". The use of hand-held devices and the social media applications associated with them greatly increases the immediate access and obvious need for information to be provided quickly, accurately, and effectively.

Lastly, since 2013, technological advancements have reshaped police response to tactical situations and should be availed to law enforcement agencies across the nation. The technology that changes policing decisions both in response to and review of incidents are seemingly endless. Body-worn cameras allow for an enhanced review of tactical situations. License-plate readers allow the tracking and identification of suspects, as well as datapoints to provide travel behavior. Gunshot detection systems allow for a speedy and streamlined response.

Technology advancements have also allowed us to take the police officers out of the line of danger as was faced in Boston and Watertown. Robotic development since 2013 has been rapid and exceptional. The use of drones and robotic technology, surveillance and inspection can be done with tools to share real-time video and data communication from a distance. Companies like Prepared also provide the technology to allow officers to receive immediate information prior to being in physical proximity to danger. Prepared allows the 911 caller, by touching a single text link to live stream video, share locations, and text with the dispatchers. This improves situational awareness. And in turn, allows dispatchers to understand the need comprehensively, allocate the required resources, and direct officers or mental health professionals in a more effective and safe

process. The ability to share data directly with first responders in real time is crucial, allowing those first to respond to the scene better prepared than ever before.

The private sector is utilizing these tools extensively. However, United States policing still lags woefully behind in the implementation of many of these important technologies. This is due to a lack of resources on the public side, a lack of information on how these tools can be utilized, and a hesitance to implement potentially controversial techniques. Clarity on privacy concerns and acceptable police procedures to investigate perpetrators of these terribly violent acts needs Congress-led debate, legislative authorization, and funding. Technology will save lives.

Further, there is an element of training now available that can prepare officers for work that would have never been possible in the past. Virtual reality training is now possible that can put officers in training safely accomplished only by using virtual reality. We can recreate harrowing incidents such as the shoot out in Watertown that was ultimately responsible for the death of BPD officer, Dennis Simmonds and the prior assassination of MIT Officer Sean Collier in Cambridge and practice aspects for tactical training purposes. Optimal designs promote situational awareness and the likeness can invoke the true dynamics of the incident, reducing mismanaged situations, improving de-escalation tactics, and limiting blue on blue and civilian shooting tragedies.

In closing, while these advancements have improved the environment for law enforcement and agencies to respond to crimes, the level of danger and sacrifice that police throughout our nation face should not be understated. As new technology becomes available to law enforcement, it is also available to criminals and terrorists. New threats, both physical and cyber are presented daily. Police will continue to adapt and overcome. With that, I would like to thank all of our law enforcement and intelligence community partners for their dedication to protect our nation. And I thank you all for providing me the opportunity to reflect and share these important lessons learned since the Boston Marathon tragedy ten years ago.