Testimony before the House Foreign Affairs Committee

Subcommittee on Terrorism, Nonproliferation, and Trade

January 27, 2015

The Honorable Mark D. Wallace

CEO, Counter Extremism Project

Chairman Poe, Ranking Member Keating and members of the Subcommittee, thank you for the opportunity to appear before you today to discuss what could be the most pressing public safety and national security issue today: the hijacking and weaponization of social media platforms by extremist groups to radicalize and recruit new members, and plan violent attacks against innocent people around the world. The evidence of social media's reach can be seen in the thousands of citizens from Western countries who continue to pour into Syria and Iraq in response to unrelenting and slickly produced propaganda by ISIS and other radical extremist groups; and the grim aftermath of lone wolf attacks, most recently in Canada and Australia, that bear witness to the power of social media to radicalize and encourage violence against Western targets.

The Counter Extremism Project (CEP), is a not-for-profit, non-partisan, international policy organization whose mission is to combat the growing threat from extremist ideology. Led by a renowned group of former world leaders and former diplomats, including former U.S. Homeland Security Advisor Frances Townsend and Senator Joseph I. Lieberman, CEP's mission is to combat extremism by pressuring financial support networks, countering the narrative of extremists and their online recruitment and calls for terror, and serving as a resource for best practices laws, policies and regulations.

CEP is assembling what we hope will be the world's most extensive research database on extremist groups and their networks of support, mapping the social and financial networks, tools and methodologies and providing an indispensable resource to governments, media, NGOs and the public. Modeled in part on advocacy efforts to counter Iran's efforts to acquire nuclear weapons, CEP exposes shadowy channels of financial support to extremist groups and brings to bear private and public sector pressure to disrupt them.

We use the latest communications tools to expose the threat of extremists and to mount a global counter-narrative to directly counter extremist ideology. Our efforts are focused

particularly on young people in communities across the globe vulnerable to extremist messaging and recruitment.

We commend this Subcommittee for recognizing the importance and the timeliness of this issue – an issue on which our Western allies, especially Great Britain have led.

We hope that this hearing can lead to a better understanding of the growing problem of social media abuse and hopefully, to a more coordinated and cooperative relationship between technology companies like Twitter and those of us who want to stop extremists from anonymously abusing social media platforms to expand their power and propel their declared war on Western society, institutions, values and culture.

Over the past two decades, the United States has led the world in advances in online technology and social media. We are the country that invented Google, Twitter, Facebook, YouTube and Instagram – all of which have revolutionized the way we communicate with each other globally, the way we share knowledge and ideas, and the way information is spread. These digital platforms have been a colossal force in empowering individuals and shining a light on abuses of power.

Unfortunately, these open platforms are also the tools of choice to spread messages of hate, creating a dark playground for extremist groups like ISIS to propagandize, radicalize, recruit new members and commit cyber jihad in the form of broadcasted beheadings, stoning's, cyber-attacks and encouraging DOS attacks and data hackings.

The reality is that extremists have been more agile, aggressive and insidious in their use of social platforms than governments have been in tracking, stopping and preventing them from hijacking the online world.

The Wilson Center's "New Terrorism & New Media" report found that 90 percent of terrorist activity taking place online today utilize social networking tools: 90 percent. According to the report, "these forums act as a virtual firewall to help safeguard the identities of those who participate, and they offer subscribers a chance to make direct contact with terrorist representatives, to ask questions, and even to contribute and help out the cyber-jihad."

Social media provides extremists with easily accessible and far-reaching platforms through which to deliver their dangerous messages. Their use of digital media has been so successful, so widespread and so encouraged that leading jihadist forums al-Fida and Shumukh al-Islam published the following regarding cyber-jihad:

> *Any Muslim who intends to do jihad against the enemy electronically, is considered in one way or another a mujaheed, as long as he meets the conditions of jihad such as the sincere intention and the goal of serving Islam and defending it, even if he is far away from the battlefield.*

That statement is emblematic of the new and troubling chapter in the sophisticated use of digital technologies by extremist groups, allowing them to spread far beyond discrete physical geographies to reach broader audiences worldwide.

During the past year, ISIS in particular has deployed an incredibly sophisticated social media campaign to radicalize and recruit new members and to call for acts of terror around the world. A major focus of CEP's work is to combat the rampant extremist recruitment, rhetoric and calls for acts of terror online, starting with Twitter. Through a rigorous research and crowdsourcing campaign called #CEPDigitalDisruption, we have identified and reported hundreds of extremists to Twitter. To be clear, our standard is incitement of violence and direct threats rooted in our American constitutional jurisprudence on free speech. Over the past three months, we've monitored hundreds of accounts and exposed the violent calls to action and instances of direct threats against individuals that jihadis are propagating on Twitter.

Even with our sacred protections of speech, our legal system does not protect certain forms of speech that crosses lines of public safety, and national security. Regrettably, as extremists have hijacked and weaponized social media platforms we are at a moment of collision between the good and thoughtful people who seek an unfettered and uninhibited right to speech through social media and similarly good and thoughtful people who seek to protect us from those who use social media platforms as an essential tool of terror.

We have seen these collisions before of course. Inevitably, public outrage over the terrible acts of the relative few who employ protected rights for perverse reasons leads to limitations through laws and regulations.

Private enterprise and businesses that profit from new technologies can either be a partner or an adversary. The question now before us is whether or not companies like Twitter will thoughtfully partner to combat those extremists who hijack and weaponize social media for terror.

As a private-sector non-profit organization whose mission is combatting extremism, we have reached out in the spirit of cooperation to Twitter in an effort to stop extremists who encourage and instruct in the ways of murder and terror, from abusing the platform.

And yet the response we get from Twitter is dismissive to the point of dereliction. We have written three letters describing the problem and requesting a sit-down between Twitter and CEP leadership. Twitter has ignored all but one letter, and its reply, simply put, was dismissive at best.

Twitter's dismissiveness on the issue of violent extremists who have hijacked and weaponized its platform can be best summarized in a quote given to Mother Jones magazine by a Twitter official: "One man's terrorist is another man's freedom fighter." Of course this statement is insipid and unserious, particularly in the context of al Qaeda, ISIS and many others. We strongly disagree with Twitter. The hijacking and weaponization of its platform is a dangerous and growing problem. We believe social media sites have a responsibility to more than protect their bottom line -- they have a responsibility to act against abuse. They provide the means for violent extremists and there should be appropriate accountability.

A great example of Twitter's failure to combat the threat of violent extremism online can be seen in a man named Mohamed Abdullahi Hassan – an American born jihadi from Minneapolis, Minnesota who is under federal indictment in Minneapolis and wanted by the FBI for joining a terrorist organization. He goes by the alias Mujahid Miski on Twitter. Miski is not only one of the most influential jihadis using Twitter to spread propaganda and recruit, he has also been responsible for tweeting some of the most heinous, violent content we've seen – including threats to behead our organization's President, Fran Townsend, and calling for every Muslim to kill one Jew in order to eradicate the Jewish people.

He boasts in his Twitter biography that he's been suspended from Twitter 20 times and keeps coming back, yet Twitter does nothing to monitor or remove his new accounts, despite the fact that each is similar to the one preceding it. As a result of Twitter's bad practice, we have been playing a never-ending game of whack-a-mole. We've raised these issues to Twitter through various channels – we've reported Miski's account over and over, we've written letters, gone to the press, and yet Twitter has not taken further action to end his abuse of its platform.

I respectfully request that the committee accept as part of this hearing's record a copy of the tweets we've reported over the course of our Digital Disruption campaign.

I would like to clarify why our focus is on Twitter versus other social media networks. When discussing the problem of drug abuse, Marijuana is often referred to as a gateway drug. In the case of jihadis online – Twitter is the gateway drug. This is where vulnerable individuals (usually young people) are first exposed to propaganda and radical content. This content is extremely accessible and public and Twitter is the introductory point to this world. From there, the conversation moves to a platform like AskFM where those being recruited can ask more in-depth questions -- for example, "What life will be like as a part of ISIS?" and "How can I get to Syria?" From there, the conversation moves to private chat applications like Kik or WhatsApp. By the time the conversation gets to the point of Kik/WhatsApp and even AskFM in many cases, it's too late. We need to stop recruitment at its gateway, and without question, Twitter is that gateway. This scenario is not fictional, it is exactly how three Denver girls were radicalized and were almost successful in joining ISIS in Syria.

In the past four months, there have been terror attacks carried out in Canada, the United States, Australia and France in the name of radical Islam. In two of these cases, Canada and

Australia, there is undisputed evidence that the attack was perpetrated by a jihadi who was using social media – either to spread content pushed out by others, or to leave messages and post justifications for his actions. If this isn't direct evidence of the extreme danger that comes from allowing these activities to take place uninhibited online, then we are simply hiding our heads in the sand.

This problem cannot be overcome by wishing it away. The number of Twitter abusers is admittedly very small in relation to the number of users, which is an even more powerful and compelling justification for taking action.

We believe strongly that there are very concrete actions that can help prevent extremists from using online tools for terror. Our goal cannot simply be to investigate, draw conclusions and count the bodies after the carnage has already taken place. Our goal should be to prevent murder, injury and destruction. And more broadly, there is a challenge for many parties in providing a counter-narrative that is more compelling and empowering than the hatred we're discussing today. But as a practical matter, while we go after the extremists, we cannot simply pretend that social media companies are helpless. They are not. They should — and they must — take a more active role in preventing extremist access to their platforms, pulling down accounts of extremists and keeping them down. We should all urge and as necessary compel social media companies to act responsibility.

If Twitter can beef up its policies as it relates to bullying and harassment of women, why does it show such dismissiveness when it comes to those promoting and glorifying terror? We stand ready to work with the Congress, the Administration and any company in finding the right mix of remedies that effectively attacks this growing problem, while protecting our values and liberties. But it must be attacked – and now.

The war against ISIS Al Qaeda and other extremist actors has many fronts – and an important one is online. While we undertake air strikes and other military responses to combat them, nothing is being done on a large scale to counter the narrative of extremists and fight back against them online.

Our concern is that we've seen a real evolution in the sophistication of methods utilized by ISIS and other extremist groups in the past year. Many ISIS members, sympathizers and supporters are young people. They've grown up in a digital world. They are digital natives, and they know how to use digital media to their advantage. They prey on at risk youths in the same way that gangs prey on at-risk kids in bad neighborhoods. And their tactics are escalating.

Several months ago, CEP as well as a large number of our supporters were targeted by a malware attack. More recently, a U.S. newspaper, and a Maryland television station were taken over by supporters of ISIS, as was the Twitter page of U.S. Central Command. This is completely unacceptable. We have called several times for the establishment of a National Cyber Terrorism Center – and we were pleased with President Obama's call during the State of the Union address for Congress to pass legislation to deal with this same issue. But cyberattacks

are but one part of the issue – we need to deal with the abuse of technology platforms directly and effectively as part of a broader effort to combat violent extremism rooting and spreading online.

There is an urgent need for social platforms to take action to stop extremists from abusing their sites to spread terrorist propaganda, recruit new members and kill innocent civilians. Government, private organizations like CEP, and companies like Twitter must work together to identify and counter the violent narrative of extremists and their recruitment efforts.

We have outlined below three clear and immediate changes that Twitter could make that would go toward stemming some of the issues outlined in this testimony:

- **Trusted Reporting Status on Twitter** – one of the problems we've encountered in the #CEPDigitalDisruption campaign is that accounts we report go into a long queue and are not immediately addressed. By giving CEP, as well as other agencies like the State Department, trusted reporting status and opening a direct line of communication between CEP and social networks, we can more easily and swiftly identify and remove the most notorious extremists online.

- **Streamlined Reporting Process** – Our campaign relies in part on our audience to report accounts along with CEP. A roadblock we run into is that the reporting process on Twitter is long and cumbersome, and weeks can pass before action occurs. Twitter has recently begun a new reporting process for women who are being harassed online, so those complaints are dealt with more quickly, but when we try to take down a violent extremist, the request falls into a catchall category that includes reporting spam. We believe that a new reporting protocol should be added for users to report suspected terrorist/extremist activity as a way to speed the process.

- **Clear, Public Policy on Extremism** –While each organization will have to take a somewhat different approach to combat the unique ways extremists are using each platform, we believe that showing a united front among America's most important tech companies is of critical importance to fighting violent extremism. This includes a clear, public, policy statement that extremist activities will not be tolerated, and that organizations like Twitter and Google, along with CEP, will work tirelessly to identify and remove content. All social networks and technology companies should actively identify these persons and ban them swiftly.

- **Verified Accounts** – Extremists flaunt even the minimal efforts Twitter has made to enforce its own standards. Once banned, they come back minutes later with new accounts, like Miski has done over and over. They often self-identify as ISIS, jihadists and terrorists, and use names similar to their deactivated accounts to make it easier to

recreate their networks in short order. Twitter already has a system where people can verify their accounts, meaning they have self-identified and those carry a small blue visible check mark. We believe this concept can be the foundation for a tiered system whereby unverified accounts are restricted and subject to a streamlined system of review for prohibited content.

- **Technology as the Solution** – Those of us who believe in free speech, pluralism, peace and tolerance will not abide forever a circumstance where the right to freely and anonymously threaten, incite, and coordinate terror is protected to a higher degree than the lives of innocent victims. I do not have any problem with someone criticizing me in an intemperate way on Twitter. I don't like it, mind you, but it's a right I respect and defend. But when someone threatens to kill, or urges countless other anonymous individuals to do so, that crosses the line into abuse of the platform. There is a technological solution out there that I think most Twitter users would accept as a fair tradeoff for lives saved. Whether the solution to this problem is defined by Twitter or defined for Twitter is not the most important question. The most important question is will this come in time to prevent an attack in the U.S. like we just saw in France?

- **The Bright Spotlight of Transparency on the Most Egregious Extremist Accounts** -- When the United Kingdom's Chanel 4 revealed that one of the most influential and pro-ISIS Twitter accounts, ShamiWitness, belonged to Bangalore, India businessman Mehdi Masroor Biswas, it shook up the cyber-jihadi network. Once revealed, Biswas immediately stopped his egregious online support for Syrian and Iraqi Jihadis. The ShamiWitness Twitter account had 17,000 followers, including many of the Islamist foreign fighters active on social media. We believe that Twitter should reveal detailed information – including names -- of the most egregious of the cyber-jihad terror actors who are the foundation of the online jihad architecture. The bright spotlight will assuredly have a further disruptive effect on other cyber-jihad account holders like ShamiWitness. By calling out these seed accounts, Twitter can play a crucial role in shutting them down. Of course, the most aggressive defenders of the anonymous and "right to tweet" will chafe at such a suggestion and they should be heard. But surely, we can collectively agree that these most egregious of cyber-jihadis do not deserve anonymity or the right of free hate and incitement of terror speech through the use of Twitter.

CEP is also developing concepts that we hope with the advent of new technologies will make it much more difficult for the worst of extremists to hide in the anonymity of the online world. Our focus is that the worst actors can be brought to justice while protecting the rights of the many users of such platforms who employ them for legitimate expressions of free speech. We have faced such challenges before and have employed technology to confront them.

What many social media companies overlook is that the business imperative for them to act cooperatively is great. With each successive and horrific misuse of social media the outcry for limitations will be greater and greater. Working in an adversarial way is not only morally wrong but will also increase the cost of doing business.

CEP is not alone in calling out social media companies to do more in this area. In a recent article in the Guardian, English Prime Minister David Cameron issued a plea to US internet giants to accept they have a social responsibility to help fight terrorism by allowing Britain's intelligence agencies access to the data and content of online communications between terror suspects. And in a subsequent interview with ITV News, Mr. Cameron said he would ask President Obama to step up pressure on web companies such as Twitter and Facebook to do more to cooperate with the intelligence agencies as they seek to track terror suspects.

I would point out that while Twitter has been non-responsive, other Internet and social media companies like YouTube have instituted reforms – such as instituting trusted reporting status for government agencies – as a means of combatting serious instances of abuse without interfering with or inconveniencing subscribers.

Successfully combatting extremist activities online need not be an insurmountable challenge. The Federal Bureau of Investigation shut down Silk Road, an online "Darknet" market trading in Bitcoin (BTC) currency, primarily used for selling illegal drugs, but also for child pornography, weapons, counterfeit passports and money, and even for contract killers to solicit clients. Silk Road users could browse and trade anonymously (to a very high degree), with a very low risk of detection. But the FBI pinpointed the foreign server that ran Silk Road despite its use of anonymity software to protect its location, and obtained records from the server's hosting provider.

That is one success story, but there are others involving investigation and prosecution of online drug distribution, child pornography, tobacco sales, and sex trafficking.

This is a quote from FBI agent Gilbert Trill following a successful sting operation into online sex trafficking.

"Some child predators mistakenly believe the anonymity of cyberspace shields them from scrutiny. In fact, their use of the Internet gives us new tools in our efforts to investigate this insidious behavior."

I am convinced that if we can make progress against these types of criminal activities, there are strategies that we can bring to bear on those who attempt to hijack and weaponize social media. We must join Prime Minister Cameron, along with our other allies around the world in recognizing the impact of this activity and implementing ways to stop it.

As I said earlier, all of these marvelous communications tools were invented in the United States. We have a duty to lead in finding ways to ensure the safety and security of our nation and our allies.

Thank you Mr. Chairman, Ranking Member Keating and all the members of this subcommittee.