Testimony before the House Committee on Oversight and Government Reform

Subcommittee on National Security

October 28, 2015

The Honorable Mark D. Wallace

CEO, Counter Extremism Project

Chairman DeSantis, Ranking Member Lynch and members of the Subcommittee, thank you for the opportunity to appear before you. It has been a year and a half since ISIS declared itself a caliphate. It has been more than a year since we launched the Counter Extremism Project – a non-profit, non-partisan, international policy organization aimed at addressing the threat of extremist ideology. It has been one year since we launched #CEPDigitalDisruption – a campaign and research effort to expose and quantify ISIS's exploitation of social media. And it has been nearly 10 months since I first testified before the House Foreign Affairs Committee's Terrorism, Nonproliferation and Trade Subcommittee on this very same critical issue.

Let me say in no uncertain terms – in that period of time, little has changed when it comes to thwarting the use of social media by terrorists. ISIS's presence on social media is a cancer. It continues to metastasize, largely unaddressed by government, the private sector, or social media companies. One of the most pressing public safety and national security issues we face today is without a doubt the hijacking and weaponization of social media platforms by extremist groups to radicalize, recruit new members, and plan violent attacks against innocent people around the world.

We commend this Subcommittee for recognizing the importance and the timeliness of these difficult issues – with which the U.S., as well as our allies, continue to struggle. 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.

It is time for us to respond – and not just by deepening our understanding and awareness of the problem, but also by actually doing something about it. And I will offer our own ideas today about how to do just that.

Over the past two decades, the United States has led the world in advances in online technology and the development of social media. We are the country that gave birth to 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 bright light on abuses of power.

Unfortunately, these open platforms are also the tools of choice for spreading 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, stonings, cyber-attacks and encouraging Denial of Service attacks and data hackings.

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

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. On September 11, CEP released profiles of 66 Americans who have joined or allegedly attempted to join the Islamic State of Iraq and Syria (ISIS), as well as other Americans accused of planning attacks on U.S. soil, providing financial assistance to extremist entities, or propagandizing on their behalf. I invite you to read their profiles. These individuals have very different backgrounds and experiences, but the one characteristic they seem to share is active participation on social media. In addition, we will soon release profiles on 54 of the most prolific social media propagandists.

Since its creation, 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. There are at least 43,000 active pro-ISIS Twitter accounts, sending approximately 200,000 tweets a day, amplifying and endlessly repeating ISIS's messages of hate and terror.

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, we respect and honor our American constitutional traditions of free speech; our standard for reporting an account is incitement of violence or direct threats.

Over the past year, 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. In June, we expanded our campaign to include monitoring of Twitter accounts in French, Italian, German and Turkish.

I would note that even with our sacred protections of free speech, our legal system does not protect certain forms of speech that cross 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 horrific acts of the relative few who abuse protected rights for perverse reasons leads to modifications through laws and regulations.

Private enterprise and businesses that profit from new technologies can either be partners or adversaries in this process. The question before us is whether or not companies like Twitter will choose to thoughtfully partner with us to combat those extremists who hijack and weaponize social media for terror or stubbornly refuse to acknowledge the problem and their responsibility.

As a private-sector, non-profit organization whose mission is combatting extremism, we have reached out repeatedly 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 that platform.

Unfortunately the response we've gotten 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 indifferent at best.

Worse, last month CEP co-hosted the first ever Global Youth Summit Against Violent Extremism with support from the White House and the State Department. The event brought together nearly 100 young people from 40 countries who are actively fighting extremism in their communities. Facebook and Microsoft both presented at the summit on best practices and tactics to fight extremism. While CEP, the White House, the State Department, Facebook and Microsoft united, Twitter decided to instead launch a PR campaign to distract from the reality that their platform has been weaponized by ISIS extremists.

Twitter's dismissiveness on the issue of violent extremists who have hijacked and weaponized its platform can be best summarized in a quote provided 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 other violent extremist groups. We strongly disagree with Twitter. The hijacking and weaponization of its platform is a dangerous and growing problem. We believe social media companies have a responsibility to do more than protect their bottom lines -- 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 is a woman named Sally Jones (known on Twitter as Umm Hussain al-Britani), a British ISIS operative who has used social media to propagandize, recruit members and incite Westerners to violence. Jones was the wife of Junaid Hussain a.k.a. Abu Hussain al-Britani, the deceased British computer hacker formerly in charge of recruiting new hackers to ISIS. Over the last year, we witnessed Jones and her now deceased husband return to Twitter with slightly altered monikers dozens of times. The type of content they push out is insidious. Most recently, in September, Jones issued a "kill list" of 100 U.S. servicemen. She was designated as a Specially Designated Global Terrorist and placed on the United Nations Security Council Sanctions List later that month. And yet, Jones has continued her threatening activity on Twitter. In October 2015, Jones incited violence against two additional U.S. veterans via Twitter: Navy Seal veteran Robert O'Neill and Dillard Johnson, a former army sergeant.

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 extremists 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 into this world. From Twitter, the conversation often moves to a platform like AskFM or Askbook 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/Askbook in many cases, it's too late; the radicalization has passed a point of no return, as thousands of heartbroken families around the world know all too well. We need to stop recruitment at its gateway, and without question, Twitter is that gateway. By the way, the scenario I have just described is not fictional, it is exactly how three Denver girls were radicalized and were almost successful in joining ISIS in Syria.

In the last year, there were terror attacks carried out in Canada, the United States, Australia, Denmark, Israel 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, but that 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 prevention of 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.

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 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 carry out air strikes and other military responses to combat extremists who have declared war against us, 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.

ISIS alone has produced and posted online at least 900 videos that show them projecting power and invincibility. These videos, at least 150 of which are focused on executions, are sophisticated and are designed to turn terror into a popular cultural product.

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 five clear and immediate changes that all social media companies could make that would go toward stemming some of the issues I have outlined today:

- **Trusted Reporting Status** – One of the problems we've encountered is that many social media companies place accounts that have been reported into a rolling queue. By giving CEP, as well as other agencies like the State Department, trusted reporting status and opening a direct line of communication, 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 reporting accounts along with CEP. A roadblock we run into is that the reporting process on Twitter and other social media sites 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. 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 organizations 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 perpetrators and ban them swiftly.

- **Shine 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.

- **Pro-Active Content Monitoring** – At this time, many social media sites including Facebook and Twitter only monitor and remove content that has been reported to them. Instead, each should spearhead internal efforts to find content and remove it without relying on the public to police the platform for 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 become greater and greater. Working in an adversarial way is not only morally wrong but will also ultimately increase the cost of doing business.

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. While no social media company has been able to solve the problem completely, companies like Google and Facebook are at least willing to have a conversation and take steps to address the issue.

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, illegal 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 platforms.

The majority of social media companies are U.S. companies, but online misuse has global consequences. It is time that social media companies like Twitter take responsibility for the global implications of their platforms and their lack of action.

Ambassador Mark D. Wallace Biography

Ambassador Mark D. Wallace serves as the Chief Executive Officer of the Counter Extremist Project (CEP) and United Against Nuclear Iran (UANI). He is also the COO of The Electrum Group, LLC.

CEP launched in September 2014, as a not-for-profit, non-partisan, international policy organization whose mission is to combat the growing threat from extremist ideology. CEP is led by a renowned group of former world leaders and former diplomats, including Frances Townsend and Senator Joseph I. Lieberman. CEP confronts the extremist threat by exposing and holding accountable their financial and other support; by serving as a best-in-class database of information about extremist groups and their supporters to governments, the private sector, the press, NGOs and other interested parties; by conducting a sophisticated media campaign to counter extremist ideology, and disrupt their messaging and recruiting; and assisting governments in the formulation of policies to degrade and stop extremist movements.

Wallace founded UANI in 2008 with the late Ambassador Richard Holbrooke, former CIA Director Jim Woolsey and Middle East expert Dennis Ross. Under his leadership, UANI has launched dozens of successful business and corporate campaigns that have called on such multinational firms as General Electric, Huntsman, Caterpillar, Ingersoll Rand, Porsche, Hyundai, Huawei, Royal Dutch Shell, Terex and Siemens to end their business dealings in Iran. UANI played a key role in pressuring SWIFT to end its provision of services to Iran's banking system. UANI's "Auto Campaign" has successfully focused on the lucrative Iranian Automobile Industry that is controlled by the regime and the Islamic Revolutionary Guard Corps. UANI has called on international automobile manufactures to leave Iran including, among others, Nissan, Fiat, Peugeot, GM and Hyundai.

UANI has authored and supported a variety of federal and state legislative and regulatory initiatives designed to enhance Iran's economic isolation. The organization's model legislation has been incorporated into both federal bills and state bills, including the *Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010* (CISADA), the *Iran Transparency and Accountability Act* (ITAA), the *Iran Financial Sanctions Improvement Act of 2012* (H.R. 4179 as introduced by Chairwoman Ileana Ros-Lehtinen and Congressman Brad Sherman), California's *Iran Contracting Act of 2010* (AB1650) and New York's *Iran Divestment Act of 2011* (A08668) among others. UANI's legislative and regulatory efforts have focused on banking, insurance and reinsurance, disclosure and debarment and shipping.

Wallace is a frequent media contributor and has been featured in news outlets around the world including *The Wall Street Journal*, *The New York Times*, the *Financial Times*, *CNN*, *Fox News*, the *Huffington Post*, *Voice of America* and *CNBC*.

Wallace served previously as United States Ambassador to the United Nations, Representative for U.N. Management and Reform. While at the U.S. Mission to the U.N., he was the lead U.S. negotiator to the world body on matters relating to reform and budget, and he led U.S. oversight into matters relating to U.N. mismanagement, fraud and abuse. During his tenure as Ambassador, Wallace most notably sought to uncover corruption in UN programs in such places as North

Korea. He exposed the "Cash for Kim" corruption scandal in North Korea, revealing that the United Nations Development Programme (UNDP) had funneled millions of dollars in hard currency to North Korea with little assurance that North Korea's dictatorship would use the money to help the North Korean people instead of diverting it to illicit activities. In addition he led the U.S. delegation's "no" vote against using UN money to pay for the 2009 "Durban II" conference. He opposed the 2008-2009 UN Biennium Budget for its "ad hoc" and "piecemeal" approach that ensured spending increases in the UN general budget that far outpaced the general budget increases of member states. While at the UN, Wallace launched the UN Transparency and Accountability Initiative (UNTAI) that focused on eight areas of reform related to member states' access to UN financial documents, ethics, financial disclosure, oversight mechanisms, IPSAS accounting standards and administrative overhead.

Upon his departure from the U.S. State Department, *The Wall Street Journal* editorial board compared Wallace to a list of "distinguished" Americans who tried to make the United Nations live up to its original ideals including Daniel Patrick Moynihan, Jeane Kirkpatrick and John Bolton.

Prior to his work at the United Nations, Wallace served in a variety of government, political and private sector posts. He served in the United States Department of Homeland Security (DHS) as Principal Legal Advisor to the Bureau of Immigration and Customs Enforcement and as the Principal Legal Advisor to the Bureau of Immigration and Citizenship Services. Prior to serving in the DHS, Wallace served as the General Counsel of the INS as it transitioned into the DHS as part of the Homeland Security Act of 2002 reorganization. He served as General Counsel of the United States Federal Emergency Management Agency (FEMA) where he oversaw and managed all aspects of the FEMA Office of General Counsel which, among other areas of responsibility, acted as counsel to the FEMA-led New York and World Trade Center recovery effort in the aftermath of the September 11, 2001 terrorist attacks.

During the 2004 Presidential campaign, Wallace served as President George W. Bush's Deputy Campaign Manager where in addition to his day-to-day responsibilities of the management of the national campaign, he was the campaign's lead at the Republican National Convention in New York City, the campaign's representative in debate negotiations, and he led the campaign's debate team at each of the Presidential and Vice-Presidential debates. During the 2008 Presidential campaign, he was a senior advisor to Senator John S. McCain and led the debate preparation team for Governor Sarah Palin in her vice-presidential debate with then-Senator Joseph Biden.

While in the private sector, Wallace worked as a commercial attorney. He was the General Counsel of the State of Florida's City of Miami Emergency Financial Oversight Board. He has served on various for profit, and not-for-profit boards of directors, including the Liberty City Charter School Project, Florida's first Charter School.