

**INTERNET TERROR RECRUITMENT AND
TRADECRAFT: HOW CAN WE ADDRESS AN
EVOLVING TOOL WHILE PROTECTING FREE
SPEECH?**

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE,
INFORMATION SHARING, AND
TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MAY 26, 2010

Serial No. 111-67

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpo.gov/fdsys/>

U.S. GOVERNMENT PRINTING OFFICE

63-091 PDF

WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

| | |
|--|-------------------------------|
| LORETTA SANCHEZ, California | PETER T. KING, New York |
| JANE HARMAN, California | LAMAR SMITH, Texas |
| PETER A. DEFAZIO, Oregon | DANIEL E. LUNGREN, California |
| ELEANOR HOLMES NORTON, District of Columbia | MIKE ROGERS, Alabama |
| ZOE LOFGREN, California | MICHAEL T. McCAUL, Texas |
| SHEILA JACKSON LEE, Texas | CHARLES W. DENT, Pennsylvania |
| HENRY CUELLAR, Texas | GUS M. BILIRAKIS, Florida |
| CHRISTOPHER P. CARNEY, Pennsylvania | PAUL C. BROUN, Georgia |
| YVETTE D. CLARKE, New York | CANDICE S. MILLER, Michigan |
| LAURA RICHARDSON, California | PETE OLSON, Texas |
| ANN KIRKPATRICK, Arizona | ANH "JOSEPH" CAO, Louisiana |
| BILL PASCRELL, JR., New Jersey | STEVE AUSTRIA, Ohio |
| EMANUEL CLEAVER, Missouri | VACANCY |
| AL GREEN, Texas | |
| JAMES A. HIMES, Connecticut | |
| MARY JO KILROY, Ohio | |
| DINA TITUS, Nevada | |
| WILLIAM L. OWENS, New York | |
| VACANCY | |
| VACANCY | |

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND
TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

| | |
|---|---|
| CHRISTOPHER P. CARNEY, Pennsylvania | MICHAEL T. McCAUL, Texas |
| YVETTE D. CLARKE, New York | CHARLES W. DENT, Pennsylvania |
| LAURA RICHARDSON, California | PAUL C. BROUN, Georgia |
| ANN KIRKPATRICK, Arizona | PETER T. KING, New York (<i>Ex Officio</i>) |
| AL GREEN, Texas | VACANCY |
| JAMES A. HIMES, Connecticut | |
| BENNIE G. THOMPSON, Mississippi (<i>Ex Officio</i>) | |

MICHAEL BLINDE, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
MEGHANN PETERLIN, *Minority Subcommittee Lead*

CONTENTS

| | Page |
|---|------|
| STATEMENTS | |
| The Honorable Jane Harman, a Representative in Congress From the State of California, and Chair, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment | 1 |
| The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment | 3 |
| The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security .. | 4 |
| WITNESSES | |
| Mr. Bruce Hoffman, Professor, Edmund A. Walsh School of Foreign Service, Georgetown University: | |
| Oral Statement | 6 |
| Joint Prepared Statement | 9 |
| Mr. Brian Michael Jenkins, Senior Adviser, The Rand Corporation: | |
| Oral Statement | 14 |
| Joint Prepared Statement | 16 |
| Mr. Anthony D. Romero, Executive Director, American Civil Liberties Union: | |
| Oral Statement | 19 |
| Joint Prepared Statement | 21 |
| Mr. John B. Morris, Jr., General Counsel, Center for Democracy and Technology: | |
| Oral Statement | 28 |
| Joint Prepared Statement | 30 |
| Mr. John Philip Mudd, Senior Research Fellow, Counterterrorism Strategy Initiative, New America Foundation: | |
| Oral Statement | 36 |
| Joint Prepared Statement | 38 |

INTERNET TERROR RECRUITMENT AND TRADECRAFT: HOW CAN WE ADDRESS AN EVOLVING TOOL WHILE PROTECTING FREE SPEECH?

Wednesday, May 26, 2010

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 10:04 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [Chair of the subcommittee] presiding.

Present: Representatives Harman, Carney, Green, Himes, Thompson (ex officio), McCaul, and Dent.

Ms. HARMAN. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on the question of "Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?" Let me say that again, "How Can We Address an Evolving Tool While Protecting Free Speech?"

I would like to welcome our witnesses.

Recent terror attacks and plots have taught us that the lonely, vulnerable, or disaffected are just a few mouse clicks away from terrorist recruiters. The anonymity of the internet and the sheer speed of communications across it make it an easy tool for recruiting and for streamlining terror group training and operations.

According to the FBI, the Christmas day bomber, Umar Farouk Abdulmuttalab, was recruited on the internet and trained in just 6 weeks.

A Philadelphia woman, Colleen LaRose, who assumed the name Jihad Jane on-line, apparently used YouTube and other websites to post communications about staging attacks in the United States, Europe, and South Asia.

The Fort Hood shooter, Major Malik Hasan, used e-mail to recontact an American cleric in Yemen, Anwar al-Awlaki, who just last weekend posted another internet video calling for the death of more civilians modeled after Hasan's point-blank assault of deploying service members in the medical units in Fort Hood. To remind us, Hasan killed 13 and wounded 31.

Hasan's family attended the Dar al-Hijrah Islamic Center in Falls Church, Virginia, where al-Awlaki was preaching in 2001.

Around the same time, two 9/11 hijackers worshipped at the mosque.

Najibullah Zazi, who was arrested last year when his plot to bomb the New York subway was uncovered, searched beauty salon and home improvement store websites on multiple occasions for chemicals to make a bomb. He also researched bomb-making instructions from internet sites.

Adam Gadahn, an American citizen from California, now serves as al-Qaeda's English language spokesman under the pseudonym Azzam al-Amriki. He has produced propaganda videos that are circulated over the internet which encourage Muslims join the global extremist movement and take part "in slitting the throats of the infidel."

The dilemma is that the internet is a forum for free speech and global commerce. But the underside is that it can also be a forum for violence and global terror. How to respect individual freedom and access and yet find those who abuse the internet and stop them before they act is a huge and difficult challenge.

Let me be clear, and many have heard me say this over and over and over again, liberty and security are not a zero sum game. We don't get more of one and less of the other. We get more of both or less. In fact, we must get more of both. Security without the liberties that our Constitution protects and Americans treasure is not security.

Our subcommittee has been wrestling with this problem for a while, and as many know, this is our third hearing on the threat posed to the U.S. homeland by violent extremism.

The purpose of today's hearing is to analyze the use of the internet as a facilitator for recruitment training and development of terror plots. The problem is the internet combines speed and anonymity in a way that complicates law enforcement and intelligence work exponentially.

I am very glad that Anthony Romero, the able Executive Director of the ACLU and well-known commentator on this issue, is here at my personal invitation to testify about how to guard the privacy and civil liberties of individuals who use the internet for the right reasons. I consult with Anthony regularly, and I thank him for being here.

But I also thank our other witnesses, also friends and colleagues, who have thought deeply and written extensively on these topics. Dr. Bruce Hoffman, a professor at Georgetown University, will discuss the evolving nature of the terror network tactics on the internet. Your testimony is excellent, Bruce.

Brian Jenkins, from California, a senior adviser at the RAND Corporation, will discuss his latest report, "Incidents of Jihadist Terrorist Radicalization in the U.S. Since 9/11."

Phil Mudd, who retired from the FBI this year as Associate Executive Director of the National Security Branch, will discuss U.S. efforts to conduct surveillance of internet communications and how the FBI currently intervenes.

We will also hear from John Morris, General Counsel for the Center for Democracy and Technology.

Welcome to you all.

As difficult and controversial as this subject is, we need to find the right way and place to intercept those who would do us harm. Developing a strategy around the internet is not optional. It has to be part of the equation.

I now yield 5 minutes to the Ranking Member for an opening statement.

Mr. McCAUL. Thank you, Madam Chair. Thank you for having this very timely and important hearing. I want to thank the witnesses on our distinguished panel. You are among the top experts in the country on this issue. Thank you for being here.

The threat of terror seen on the internet to recruit others and spread their ideology is very real. While I know there is debate about what we can do about it, I don't think anyone here could dispute the fact that terrorists are successfully using the internet to help spread their message.

The internet allows extremists the freedom to meet, work together, research and plan attacks, and inspire others to attack, without ever leaving their home. According to some estimates, over 5,000 jihadists websites and web forums are currently operational. This number continues to climb, with an estimated 900 more appearing every year.

Terrorists once had to travel to terror camps in Pakistan to receive indoctrination and training. Now, aspiring terrorists only need to open their laptop and connect to the internet. The internet and e-mail continue to play an integral role in recent terror plots. One example that Madam Chair underscored was the threat by Colleen LaRose, better known as Jihad Jane, a blonde-haired, blue-eyed, native-born American who actively solicited conspirators to travel abroad to commit terror attacks; and at Fort Hood, just north of my district in Texas, Nidal Hasan brutally murdered 13 innocent people after exchanging e-mails with the radical cleric in Yemen. Al-Awlaki's on-line lectures were cited as inspiring Shahzad, the bomber in the recent Times Square attack. Al-Awlaki has repeatedly posted messages and videos on-line encouraging the murder of Americans.

As we continue to debate how to attack and defeat this enemy, I believe the answer must include combating the jihadi propaganda so readily available on the internet. We must work with our private sector and community partners to counter the terrorist narrative. At a more basic level, if we are going to look seriously at terrorists' use of the internet, there are issues that must be addressed in order to protect the fundamental American rights guaranteed by the Constitution.

For instance, should the Government be monitoring jihadi websites and chat rooms, and how can that be done effectively while protecting Constitutional rights?

There is little expectation of privacy, in my judgment, on-line, especially when the internet is used to spread violent radical Islam or recruit others to participate in jihad. Similarly, there is a debate among many counterterrorism experts whether we should allow these websites to remain up and running. Does shutting them down turn off an important source of information for investigators? Or does it effectively disrupt terrorists' communications?

An attack was prevented in Dallas when FBI agents monitoring an extremist website forum noted violent messages being posted by al-Smadi and set him up in a sting operation. This shows there is value to monitoring these websites. But is there a point where it is of greater value to shut them down, and at what point does terrorist use of the internet cross the line from free speech to illegal activity?

Al-Awlaki's radical lectures available on the internet are known to inspire and incite terrorist acts. Are these lectures protected as free speech?

Another issue I hope to address is the responsibility of the private sector to self-monitor the content on their websites for danger, much like the street vendor in Times Square who saw something and said something to prevent an attack. At what point does the responsibility lie with the web host to identify and report potential threats? At what point does terrorist use of the internet cross the line from free speech to illegal activity?

Al-Awlaki's radical lectures available on the internet are known to inspire and incite terrorist attacks. Are they protected as free speech?

I believe this is similar to one of the issues raised in the Supreme Court cases as to whether yelling fire in a theater is covered under the First Amendment.

These are just a few examples of the complex issues that I look forward to exploring at this hearing, and let me once again thank Madam Chair for holding this important hearing. With that, I yield back.

Ms. HARMAN. Thank you, Mr. McCaul. The Chair now yields 5 minutes to the Chairman of the full committee for an opening statement.

Mr. THOMPSON. Thank you very much, Madam Chair, and I compliment you for this hearing. As you know, a number of things have occurred over the last 6 months that has put more light on this situation.

One of the most important messages this committee has worked to communicate is that the concept of homeland security is more than just the sum of many working pieces. Yes, homeland security is about stopping terrorist attacks. Yes, homeland security is about responding to disasters, both natural and manmade. But homeland security is also about giving the American public, our citizens, a sense of security and freeing them from fear.

Terrorists want nothing more than to shatter our security and make us fearful. Their acts by design are intended to create fear to draw attention to their message, regardless of whether that message is hatred for a particular group of people, a government, or a government policy. While we understand why terrorists use fear in that way, what we have struggled to understand is why individuals are drawn to participate in these kinds of acts. What leads an individual down the path from radical thought to violence?

Many of our homeland security-related policies are directed towards prevention of terrorist acts and overcoming the fear created by those acts themselves. However, very little of our focus is upon any kind of fear, the fear generated by what we do not understand.

Because we are seeing a trend involving cases of individuals move from radical thought to violent action, we already heard from just a few examples this morning an important part of helping us free from fear is to strive to understand and, if possible, disrupt the process.

As a communication tool, however, the internet is already used in many ways as an important piece of that process that we must work to understand. Because we are working to understand the recruitment and radicalization process, it is equally important that we understand the uses of which individuals undergo are encouraging this process with tools like the internet.

However, freedom from fear also means that people should also not fear their Government and, in particular, should not fear the homeland security and law enforcement organizations that are working to provide that security. A person should also be free from fear that their communication or free expression, both on-line and off, are not subject to improper law enforcement scrutiny. This is why it is so important that we have the conversation like the one we are about to have today.

To free us from fear, we must develop our understanding of terrorist recruitment and radicalization and the tools used to facilitate that process, but we also ensure that we are exploring the issues in a way that is protective of our rights to hold and express radical or unpopular ideas and privacy.

For that reason, I welcome this panel of witnesses. I hope you can help us shed some light on how we can go about managing this delicate balancing act.

Thank you, and I yield back, Madam Chair.

Ms. HARMAN. Thank you, Mr. Chairman.

Other Members of the subcommittee are reminded that under subcommittee rules, opening statements may be submitted for the record.

I now welcome our witnesses this morning.

Dr. Bruce Hoffman is a Professor of Security Studies at Georgetown University's Edmund A. Walsh School of Foreign Service and a member of the National Security Preparedness Group, the successor to the 9/11 Commission. Before working at Georgetown, Professor Hoffman held the corporate Chair in Counterterrorism and Counterinsurgency at the RAND Corporation in its Washington office. Between 2004 and 2006, Professor Hoffman was scholar in residence at the CIA, during which he served in a variety of advisory roles. He has conducted field work on terrorism in Afghanistan, Argentina, Pakistan, India, Northern Ireland, and Iraq, among others.

Our second witness, Brian Michael Jenkins, is Senior Adviser at the RAND Corporation and an expert on political violence and sophisticated crime. He, too, is very sophisticated, I should add. From 1989 to 1998, Mr. Jenkins was the Deputy Chairman of Kroll Associates, an international investigative and consulting firm. Before this he worked at RAND as Chairman of its Political Science Department. He also held the rank of Captain in the U.S. Army's Green Beret, serving both in the Dominican Republic and Vietnam.

Anthony Romero, as I mentioned, is the Executive Director of the ACLU. He took this position 4 days before September 11, and the

ACLU soon after launched the National Safe and Free Campaign to Protect Basic Freedoms in a Time of Crisis. He is a frequent commentator on virtually everything that has happened in the legal domain and policy domain since 9/11, and the ACLU has filed litigation on issues like the torture and abuse of detainees in U.S. custody. He has also presided over the most successful membership growth in ACLU history. During his tenure, the staff has doubled and the budget has tripled. Pretty impressive.

Mr. John Morris is the General Counsel at the Center for Democracy and Technology, CDT, and Director of CDT's internet Standards Technology and Policy Project. Prior to joining CDT in 2001, Mr. Morris was a partner at Jenner & Block, where he litigated ground-breaking cases in internet and First Amendment law. He was the lead counsel in the landmark case *Reno v. ACLU*, where the Supreme Court unanimously overturned the Communications Decency Act of 1996 and extended the highest level of Constitutional protection to free speech on the internet. In 2009, Mr. Morris was appointed to the Communication Security Reliability and Interoperability Council of the Federal Communications Commission to ensure civil liberties are considered in developing law enforcement communications technologies.

Finally, Phil Mudd. Mr. Mudd is a Senior Research Fellow for the Counterterrorism Strategy Initiative at the New America Foundation. Most of us have known him a long time, as he served as senior intelligence adviser at the FBI. In 2005, he was appointed First Deputy Director of the FBI's National Security Branch. He began his Government service when he joined the CIA in 1985, served there in a variety of roles, including Deputy National Intelligence Officer for Near East and South Asia and as CIA detailee to the White House National Security Council and ultimately Deputy Director of the Counterterrorism Center. He has received numerous awards for his Government service, including the CIA Director's Award, the George H.W. Bush Award for Excellence in Counterterrorism, and the first ever William Langer Award for Excellence in Analysis.

Without objection, your full statements will be inserted in the record.

We will now ask Dr. Hoffman to summarize his statement in 5 minutes, more or less. I do understand that you have some slides to show us.

Mr. HOFFMAN. Yes, actually videos.

Ms. HARMAN. Videos to show us.

STATEMENT OF BRUCE HOFFMAN, PROFESSOR, EDMUND A. WALSH SCHOOL OF FOREIGN SERVICE, GEORGETOWN UNIVERSITY

Mr. HOFFMAN. Madam Chair, Mr. Chairman, Members of the committee, thank you for the opportunity to testify today.

Twice in the past 6 months, the United States was just minutes away from another tragedy of unmitigated horror. Once again, terrorists had breached our security and nearly succeeded in killing and harming Americans in the skies of our country and on its streets.

In both instances had it not been for the malfunctioning of the terrorist's explosive devices and the quick and effective intervention of our fellow citizens, America would have fallen victim to the worst terrorist attack since September 11, 2001.

These two incidents appear to be part of an emerging pattern of terrorist threats in the United States. During 2009, a record 10 jihadi or jihadi-inspired plots or incidents and one tragically successful attack occurred. Furthermore, at least two dozen persons were indicted in the United States on terrorism charges last year, another record.

Thus far, in 2010, there have been four incidents. It is therefore difficult to be complacent when an average of one plot is now being uncovered per month for the past year or more, and perhaps even more are being hatched that we don't know about.

While it is easy to dismiss as amateurish many of these plots, incidents, and failed attacks, we do so at our peril. In point of fact, what appears to be amateurishness, such as the most recent abortive car bomb plot in New York City's Times Square and the attempt last Christmas day to affect the in-flight bombing of a Northwest Airlines passenger jet, may be more of a reflection of the attack having been rushed.

Fears that a would-be attacker might be identified and interdicted by authorities may thus account for what appears to be a more compressed operational tempo or faster soup-to-nuts process by which a recruit is deployed operationally.

The sheer diversity of the perpetrators and nature of their plots is also remarkable. But as disparate and diverse as they may appear, the one thing that the majority of them had in common was the role that the internet played in their respective plots and often in their radicalization.

Terrorism has often been understood to be a violent means of communication. Communication is essential for a terrorist movement, not just for the obvious purposes of summoning publicity and attention through their violence acts but also to ensure their longevity and very survival.

Given this constellation of requisite sustainable resources, motivated minions, energized recruits, along with generous sympathizers and supporters, it is not surprising that the weapons of terrorism today are no longer simply the guns and bombs they have always been but now include computers, the internet, and the world wide web.

Because of the internet, the art of terrorist communication has now evolved to a point where terrorists can effortlessly and effectively control the communication of their ideology of hate, intolerance, and violence, determining the content, context, and medium over which their message is projected and towards precisely the audience or multiple audiences they seek to reach.

The recent Times Square plot involving a naturalized American citizen of Pakistani descent is a wake-up call. The wishful thinking that the American melting pot provided a firewall against the radicalization and recruitment of American citizens along with U.S. residents arguably lulled us into a false sense of complacency that homegrown terrorism couldn't happen here. By stubbornly wrapping ourselves in this false security blanket, we missed a rare

chance 3 years ago to get in front of this issue and potentially fully understand how Americans might be radicalized and recruited to terrorism.

In 2007, the Chair of this subcommittee introduced House Resolution 1955, the Violent Radicalization and Homegrown Terrorism Prevention Act, which would have established a National commission to study domestic terrorism. Although the bill passed the House, it never came to a vote in the Senate.

Given that the terrorist threat has changed so appreciably since the 9/11 Commission concluded its work 6 long years ago, we require the same fresh look and new approaches that would have been this commission's remit. In this case, such a body would have provided a baseline assessment of terrorist radicalization recruitment processes and make policy recommendations about how to counter them by drawing on a comprehensive survey of the experiences and best practices of other countries.

Instead, 10 years into the war on terrorism, important questions remain unanswered. The two most salient, in my view, are who, in fact, is responsible in the U.S. Government to identify radicalization when it is occurring and then to interdict attempts at recruitment? Most critically, have terrorists discovered our Achilles heel in that we currently have no strategy to counter this type of threat or to interdict radicalization and prevent terrorist recruitment?

Thank you, Madam Chair. May I show these two videos?

Ms. HARMAN. Yes. Without objection, yes. Please show them. They are not very long, are they?

Mr. HOFFMAN. No, and you can feel free to cut them off because the message I think will be very clear in the first 15 to 30 seconds. The first video is very much the kind of thing that you would see on MTV.

[Video shown.]

Mr. HOFFMAN. It ends with an image of the World Trade Center collapsing.

[Video shown.]

Ms. HARMAN. Is this video still on the website someplace?

Mr. HOFFMAN. It is readily available. It has been on the web for 6 years now. You can see it is geared to an audience of people that are aren't terribly religious, but it hooks them with an MTV-like presentation and a catchy beat. The second one is more religious. It is a capella, so there is no music. It is a traditional nasheed.

Ms. HARMAN. Thank you.

Mr. HOFFMAN. If I may say, the singer in that is an American citizen, someone named Omar Hammami, who is from Alabama, who was featured. If you saw the New York Times Magazine article in January, by Andrea Elliott, he was the jihad next door.

[The statement of Mr. Hoffman follows:]

PREPARED STATEMENT OF BRUCE HOFFMAN*

26 MAY 2010

Twice in the past 6 months, the United States was just minutes away from another tragedy of unmitigated horror. Once again, terrorists had breached our security and nearly succeeded in killing and harming Americans in the skies above our country or on its streets. In both instances, had it not been for the malfunctioning of the terrorists' explosive devices and the quick and effective intervention of our fellow citizens, America would have fallen victim to the worst terrorist attacks since September 11, 2001.

These two incidents are part of an emergent pattern of terrorist threats in the United States. During 2009, a record ten jihadi or jihadi-inspired plots or incidents and one tragically successful attack, at Fort Hood, Texas that claimed the lives of thirteen persons, occurred.¹ Furthermore, at least two dozen persons were indicted in the United States on terrorism charges last year²—another record. Thus far in 2010 there have been four incidents. It is therefore difficult to be complacent when an average of one plot is now being uncovered per month over the past year or more—and perhaps even more are being hatched that we don't yet know about.

While it is easy and perhaps also comforting to dismiss as “amateurish” these plots, incidents, and failed or foiled attacks, we do so at our peril. In point of fact, what appears as “amateurishness”—such as the most recent abortive car bomb plot in New York City's Times Square and the attempt last Christmas day to effect the in-flight bombing of a North West Airlines passenger jet—may be more a reflection of the attack having been rushed. Terrorists, we often forget, play the odds and pin their faiths and hopes on eventually simply getting lucky. Over a quarter of a century ago, the Irish Republican Army famously taunted then-Prime Minister Margaret Thatcher after a bomb failed to kill her at the 1984 Conservative Party conference in Brighton, England: “Today we were unlucky, but remember we only have to be lucky once. You will have to be lucky always.”³ Our terrorist enemies today doubtless embrace the same logic.

Indeed, at a time, for example, when the capability of the Tehrik-i-Taliban or Pakistani Taliban, (TTP)—whom both the U.S. Attorney General Eric Holder and senior Obama administration counterterrorism adviser John Brennan have gone on record as stating was behind the Times Square plot, having provided money and direction to the hapless bomber, Faisal Shahzad⁴—and al-Qaeda in Pakistan are being relentlessly degraded by the U.S. drone attacks, both groups as well as allied and associated organizations may feel pressed to implement an operation either sooner or more precipitously than they might otherwise prefer. Fears that a would-be attacker might be identified and interdicted by authorities may thus account for what appears to be a more compressed operational tempo or faster “soup to nuts” process by which a recruit is deployed operationally.

The complaint sworn against Shahzad in Federal court, for instance, reveals a very fast 4-month process from planning to training to Times Square.⁵ He reportedly only received 3 to 5 days of bomb-making training. The TPP, al-Qaeda and other terrorist groups may thus be prepared to accept this trade-off between shorter training periods leading to accelerated operations in order to dispatch “clean skin” recruits before they can be identified and detected. Indeed, this likely represents a reasonable trade-off and excellent return on a very modest investment. The terrorists groups have expended little effort and energy training alleged “walk-ins” like Shahzad who present terrorist organizations with a low-cost opportunity to strike in the United States.

This is part and parcel of an al-Qaeda strategy that it also has pushed on other groups. It is a strategy that is deliberately designed to overwhelm, distract, and exhaust the terrorists' adversaries. There are two components to this strategy: one

* My affiliation with Georgetown University is for identification purposes only. This testimony presents the views of the witness only and does not nor is it meant to reflect those of Georgetown University.

¹ See Brian Michael Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001* (Santa Monica, CA: RAND Corp., 2010), pp. 13–17.

² One source puts this figure at 41 persons. See Steve Kroft, “Homegrown Terror,” *60 Minutes*, CBS News, 9 May 2010 accessed at: <http://www.cbsnews.com/video/watch/?id=6470178n&tag=contentMain,cbsCarousel>.

³ Quoted in Peter Taylor, *Brits* (London: Bloomsbury, 2001), p. 256.

⁴ Anne E. Kornblut and Karin Brulliard, “U.S. blames Pakistani Taliban for Times Square bomb plot,” *Washington Post*, 10 May 2010.

⁵ *United States of America v. Faisal Shahzad*, Defendant, Case 1:10-mj-00928-UA Filed 4 May 2010.

economic and the other operational. In terms of the economic dimension, al-Qaeda has never claimed it could or would defeat U.S. militarily. Instead, it seeks to wear us down economically through increasing expenditures on domestic security and overseas military commitments. Given the current global economic downturn, this message arguably now has greater resonance with al-Qaeda's followers and supporters and indeed perhaps even with new recruits. The operational dimension seeks to flood already stressed intelligence and law enforcement with "noise": low-level threats from "lone wolves" and other jihadi "hangers on"—e.g., the "low hanging fruit" are designed to consume the attention of law enforcement and intelligence in hopes that this distraction will permit more serious terrorist operations to go unnoticed and thereby sneak in "beneath the radar" and in fact succeed.⁶

The sheer diversity of the perpetrators and nature of their U.S. plots is also remarkable. These have included highly trained al-Qaeda operatives like Najibullah Zazi, the Afghan-born U.S. resident who sought to replicate the 7 July 2005 suicide attacks on London transport in Manhattan; motivated, but less competent, recruits like Shahzad and the five youths from a Washington, DC suburb who last December sought training in Pakistan to fight in Afghanistan but, had they been successful in establishing contact with a Pakistan-based terrorist group, could just as well have been deployed back to United States; dedicated sleeper agents like the U.S. citizen David Headley whose reconnaissance efforts on behalf of Lashkar-e-Taiba (LeT), a longstanding al-Qaeda ally, were pivotal to the November 2008 Mumbai, India attack's success; bona fide "lone wolves" like Major Nidal Hasan, the Fort Hood shooter, and other individuals with murkier terrorist connections like Abdulhakim Muhammad (nee Carlos Bledsoe), an African-American convert to Islam who returned from Yemen last year and killed a U.S. military recruiter and wounded another in Little Rock, Arkansas and has now claimed in court to have done so on behalf of AQAP—the same group responsible for Christmas day plot; and, finally, the incompetent, wannabe terrorists who are easily entrapped and apprehended such as the four parolees and converts to Islam who attempted to bomb 2 Bronx synagogues and an upstate air national guard base, the Jordanian national who overstayed his U.S. tourist visa and plotted to bomb a downtown Dallas office tower last September, and another convert who wanted to blow up a Springfield, IL Federal building that same month, among others.

Well over a year ago we became aware of radicalization and recruitment occurring in the United States when Somali-Americans started disappearing from the Minneapolis-St Paul, Minnesota area and turning up in Somalia with an al-Qaeda affiliate called al Shabab ("the youth"). Administration officials and others believed it was an isolated, one-off phenomenon. But it was not restricted to a small number of individuals in one place as the grand juries that have been sitting in Minneapolis-St Paul and San Diego, California attest along with the on-going FBI investigations in Boston and two locations in Ohio, among other places. The number of Somali-Americans who left the United States to train in Somalia was also far higher than initially believed (numbering upwards of some 30 persons) and furthermore once they were in Somalia they were in fact being trained by a senior and long-established al-Qaeda commander.

In sum, the case of the Somali-Americans thus turned out to be a Pandora's box. By not taking the threat of radicalization and recruitment actually occurring in the United States more seriously and sooner we failed to comprehend that this was not an isolated phenomenon, specific to Minnesota and this particular immigrant community, but that it indicated the possibility that an albeit embryonic terrorist radicalization and recruitment infrastructure had been established in the United States. Shahzad is thus the latest person to jump out of this particular Pandora's box.

As disparate and diverse as the above list of individuals may appear, the one thing that the majority of them had in common was the role that the internet played in their respective plots and often their radicalization. For example:

- Zazi conducted several internet searches to identify and obtain commercially available materials for the bombs he intended to use in attacks on the New York City subway;⁷

⁶See Bruce Hoffman "American Jihad," *The National Interest*, no. 107, May/June 2010, pp. 17–27; and, idem, "Al-Qaeda's New Grand Strategy," *Washington Post* (Sunday Outlook section), 10 January 2010.

⁷United States District Court Eastern District of New York against Najibullah Zazi, Defendant, Memorandum Of Law In Support Of The Government's Motion For A Permanent Order Of Detention, 09–CR–663 (RJD), 24 September 2009, pp. 5, 7, and 11–12.

- Hasan exchanged at least 18 e-mails between December 2008 and June 2009 with Anwar al Awlaki, an operational officer with al-Qaeda in the Arabian Peninsula (AQAP);⁸
- Colleen LaRose used the online monikers “Fatima La Rose” and “JihadJane” allegedly to recruit others in the United States and abroad, supposedly to carry out a terrorist attack in Sweden.⁹ She boasted in e-mails how, given her appearance—e.g., a petite, blue-eyed, blonde—she could “blend in with many people.” She also sought to recruit other Western women who looked like her.¹⁰ David Kris, an assistant attorney general in the Department of Justice’s National Security Division, was quoted in the *Washington Post* as stating that the fact that a suburban American woman stands accused of conspiring to support terrorists and traveling overseas to implement an attack “underscores the evolving nature of the threat we face”;¹¹
- Hosam Smadi, the young Jordanian national implicated in the Dallas, Texas bomb plot, according to his indictment, allegedly belonged to “an online group of extremists . . . who espoused violence.” It further stated that Smadi “stood out based on his vehement intention to actually conduct terrorist attacks in the United States”;¹²
- Michael Finton, a U.S. citizen, implicated in a plot to bomb a Federal building in Springfield Illinois, claimed both to have been influenced by an al-Qaeda video and to have obtained “all that he could . . . use the internet to look up all he needed to know to conduct such an attack . . . ”.¹³
- David Headley, the U.S. citizen who allegedly carried out reconnaissance and surveillance operations on behalf of both Pakistani jihadi terrorist organizations and al-Qaeda was actively involved in on-line user groups and chat room forums¹⁴ as was one of his alleged co-conspirators, Tahawur Rana.¹⁵
- Tarek Mehanna, a U.S. citizen charged with conspiracy to provide material support to terrorists allegedly made extensive use of the internet, amassing, according to the criminal complaint filed against him in Federal court, “Video files, audio files, images, stored messages, word processed documents and cached web pages”;¹⁶
- Bryant Neal Vinas, a U.S. citizen from Long Island, New York who traveled to Pakistan to enlist in al-Qaeda and, in addition to providing information to facilitate an al-Qaeda plot to blow up a Long Island Rail Road train inside New York’s Pennsylvania Station, participated in an attack on U.S. military forces in Afghanistan, is believed to have been radicalized as a result of “visiting jihadist Web sites”;¹⁷
- Umar Farouk Abdulmuttalab, the AQAP operative who attempted to bomb a North West airlines flight on Christmas day, 2009 was in regular contact with the aforementioned Anwar al Awlaki;¹⁸ and,

⁸ Brian Ross and Rhonda Schwartz, “Major Hasan’s E-Mail: ‘I Can’t Wait to Join You’ in After-life,” ABC News, 19 November 2009 accessed at <http://abcnews.go.com/print?id=9130339>.

⁹ See United States District Court for the Eastern District of Pennsylvania, *United States Of America v. Colleen R. LaRose*, 10–Cr–123, 4 March 2010, pp. 3–8.

¹⁰ Quoted in *Ibid.*, p. 3.

¹¹ Quoted in Carrie Johnson, “JihadJane, an American woman, faces terrorism charges,” *Washington Post*, 10 March 2010.

¹² Quoted in United States District Court for the Northern District of Texas, *United States Of America v. Hosam Maher Husein Smadi*, 3:09–MJ–286, 24 September 2009, p. 1. See also, *Ibid.*, pp. 2 and 5; and, “Jordanian accused in Dallas bomb plot goes to court,” CNN.com, 25 September 2009 accessed at: <http://cnn.site.printthis.clickability.com/pt/cpt?action=cpt&title-Jordan>.

¹³ Quoted in United States District Court for the Central District of Illinois, *United States Of America v. Michael C. Finton*, 09–3048–M, 24 September 2009, pp. 11 and 15. See also, *Ibid.*, p. 17.

¹⁴ See United States District Court for the Northern District of Illinois, *United States Of America v. Ilyas Kashmiri, et al.*, 09 CR 830 October 2009, pp. 13 and 20.

¹⁵ *Idem.*, *United States Of America v. Tahawur Rana*, 18 October 2009, pp. 4, 8, 14, 24, and 42.

¹⁶ United States District Court of Massachusetts, *United States Of America v. Tarek Mehanna*, 09–10017–GAO CR 830, November 2009, pp. 2–3, 10–11, 14–30, 39–40, 43–49, & 56–73.

¹⁷ Quoted in William K. Rashbaum and Souad Mekennet, “L.I. Man Helped Qaeda, Then Informed,” *New York Times*, 23 July 2009.

¹⁸ Mark Hosenball, et al., “The Radicalization of Umar Farouk Abdulmuttalab,” *Newsweek*, 2 January 2010.

- Faisal Shahzad has been widely reported to have viewed radical jihadi material on the internet and apparently has admitted to having been inspired by al Awlaki as well.¹⁹

TERRORISM AS COMMUNICATION AND THE INTERNET AS A CRITICAL MEANS OF
RADICALIZATION AND RECRUITMENT

Terrorism has long been understood to be a violent means of communication. The terrorist act itself is of course designed to attract attention and then, through the publicity that it generates, to communicate a message. Indeed, nearly a quarter of a century ago, Alex Schmid and Janny de Graaf observed that, “Without communication there can be no terrorism.”²⁰ But communication is essential for a terrorist movement not just for the obvious purposes of summoning publicity and attention, but also to ensure its longevity and very survival. Indeed, without effective communications, a terrorist movement would be unable to recruit new members into its ranks, motivate and inspire existing members to carry on with the struggle despite formidable odds, as well as expand the pool of active supporters and passive sympathizers from which the movement draws its sustenance.

Given this constellation of requisite sustainable resources—motivated minions, energized recruits, along with generous sympathizers and supporters—it is not surprising that the weapons of terrorism are no longer simply the guns and bombs that they always have been, but now include the mini-cam and videotape, editing suite and attendant production facilities; professionally produced and mass-marketed CD-ROMs and DVDs; and, most critically, the lap-top and desk-top computers, CD burners and e-mail accounts, and internet and world wide web. Indeed, largely because of the internet—and the almost unlimited array of communications opportunities that it offers—the art of terrorist communication has now evolved to a point where terrorists can effortlessly and effectively control the communication of their ideology of hate, intolerance, and violence: determining the content, context, and medium over which their message is projected; and towards precisely the audience (or multiple audiences) they seek to reach.²¹

The implications of this development have been enormous. The internet, once seen as an engine of education and enlightenment, has instead become an immensely useful vehicle for terrorists with which to peddle their baseless propaganda and manifold conspiracy theories, lies, and clarion call to violence.²² These sites alarmingly present an increasingly compelling and indeed accepted alternative point of view to the terrorists’ variegated audiences.²³ This was of course precisely al-Qaeda’s purpose in creating its first website, *www.alneda.com*, and maintaining a variety of successor sites ever since: To provide an alternative source for news and information that the movement itself could exert total control over.

Because of its geographical reach, ubiquity, modest costs, and ability to communicate in real-time, the internet has thus become the terrorists’ favored means of propaganda dissemination and incitement to violence. As Professor Gabriel Weimann of Haifa University notes in his seminal study *Terror on the Internet*, when he began studying this phenomenon nearly a decade ago, there were only about 12 terrorist group websites. By the time he completed his research in 2005 the number had grown to over 4,300—a proliferation rate of about 4,500 percent per year.²⁴ And, by the time the book was published the following year, the number had jumped to over 5,000 websites.²⁵ Today, experts estimate that there are well over 7,000 such sites.

¹⁹ See Scott Shane and Souad Mekhennet, “Imam’s Path From Condemning Terror to Preaching Jihad,” *New York Times*, 8 May 2010.

²⁰ Alex Schmid and Janny de Graaf, *Violence As Communication: Insurgent Terrorism and the Western News Media* (Beverly Hills, CA: Sage, 1982), p. 9.

²¹ See, for example, the 2004 video clip, “Dirty Kuffar,” aimed at British youth at <http://video.google.com/videoplay?docid=9083681522527526242#docid=-4283987610134255997>, and, an al Shabaab video clip aimed at Americans and Westerners in general from 2009 “English Nasheed Rap by Shabab Al-Mujahideen (Blow by Blow)” at http://www.youtube.com/watch?v=ODGRd_DKchw.

²² See, for instance, the “Iraq” tab at *www.kavkazcenter.com* and the “Iraqi Resistance Report” tab at *www.jihadunspun.com* as well as such sites as *www.islammemo.cc/taqer/one_news.asp?Idnew=292*; *www.la7odood.com*; *www.balagh.com/thaqafa/0604ggpz.htm*; and *www.albasrah.net*: all accessed on 6 July 2005.

²³ See, also, Dina Temple-Raston, “Al-Qaeda media Blitz Has Some On Alert,” *Morning Edition*, National Public Radio, 8 April 2009 accessed at: <http://www.npr.org/templates/story/story.php?storyId=102735818>.

²⁴ Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), p. 105.

²⁵ Remarks by Professor Gabriel Weimann, book launch event held at the U.S. Institute of Peace, Washington, DC on 17 April 2006.

Thus, virtually every terrorist group in the world today has its own internet website and, in many instances, maintain multiple sites in different languages with different messages tailored to specific audiences. The ability to communicate in real time via the internet, using a variety of compelling electronic media—including dramatic video footage, digital photographs, and audio clips accompanied by visually arresting along with savvy and visually appealing web design—has enabled terrorists to reach a potentially vast audience faster, more pervasively, and more effectively than ever before. The changing face of terrorism in the 21st Century is perhaps best exemplified by the items recovered by Saudi security forces in a raid during on an al-Qaeda safe house in Riyadh in late spring 2004. In addition to the traditional terrorist arsenal of AK-47 assault rifles, explosives, rocket-propelled grenades, hand grenades, and thousands of rounds of ammunition that the authorities the police expected find, they also discovered an array of electronic consumer goods including: Video cameras, laptop computers, CD burners, and the requisite high-speed internet connection. According to “60 Minutes” investigative journalist Henry Schuster, the videos:

“had been part of an al-Qaeda media blitz on the web that also included two on-line magazines full of editorials and news digests, along with advice on how to handle a kidnapping or field-strip an AK-47 assault rifle. The videos mixed old appearances by bin Laden with slick graphics and suicide bombers’ on-camera last wills and testaments. They premiered on the internet, one after the other, and were aimed at recruiting Saudi youth.”²⁶

As Tina Brown, the doyenne of post-modern media, has pointed out: the “conjunction of 21st-century internet speed and 12th-century fanaticism has turned our world into a tinderbox.”²⁷

CONCLUSION

The recent Times Square plot involving a naturalized American citizen of Pakistani descent is a wake-up call. The wishful thinking that the American “melting pot” theory provided a “fire wall” against the radicalization and recruitment of American citizens—whether naturalized or born here—along with U.S. residents (green card holders), arguably lulled us into a sense of complacency that home-grown terrorism couldn’t happen here. The British similarly believed before the 7 July 2005 London suicide attacks that there was perhaps a problem with the Muslim communities in Europe but certainly not with British Muslims in the United Kingdom who were better integrated, better education, and wealthier than their counterparts on the continent.

By stubbornly wrapping ourselves in this false security blanket we lost 5 years to learn from the British experience. Indeed, the United States missed a rare chance 3 years ago to get in front of this issue and potentially fully understand how Americans are radicalized and recruited to terrorism. In 2007, the Chair of this same subcommittee introduced House Resolution 1955, the “Violent Radicalization and Homegrown Terrorism Prevention Act of 2007,” which would have established a National commission to study domestic terrorism. Although the bill passed the House of Representatives, it never came to a vote in the Senate. Given that the terrorist threat has changed so appreciably since the 9/11 Commission concluded its work 6 years ago, we require the same fresh look and new approaches that would have been this commission’s remit. Moreover, these days it seems bipartisan commissions are the only way our Government can accomplish anything terrorism-related. In this case, such a body would have provided a baseline assessment of terrorist radicalization and recruitment processes, and made policy recommendations about how to counter them by drawing on a comprehensive survey of the experiences and best practices of other countries—and by better understanding how terrorist groups might target and attract Americans and U.S. residents into their ranks.

Instead, 10 years into the war on terrorism, the big questions that the commission proposed in H.R. 1955 may have shed critical light on lamentably remain unanswered. What do we do when the terrorists are like us? When they conform to the archetypal American immigrant success story? When they are American citizens or American residents? When they are not perhaps from the Middle East or South Asia and in fact have familiar-sounding names? Or, when they are “petite, blue-eyed,

²⁶Henry Schuster, “Studios of Terror: Al Qaeda’s Media Strategy,” *CNN International.Com, Tracking Terror*, 16 February 2005, accessed at <http://207.25.71.245/2005/WORLD/meast/02/15/schuster.column/index.html>.

²⁷Tina Brown, “Death by Error,” *Washington Post*, 19 May 2005.

blonde” suburban housewives who, as the infamous Jihad Jane boasted, “can easily blend in”?

Who in fact is responsible in the U.S. Government to identify radicalization when it is occurring and then interdict attempts at recruitment? Is this best done by Federal law enforcement (e.g., the FBI) or State and local jurisdictions working closely with Federal authorities? Is it a core mission for a modernized, post-9/11 FBI? Or for the Department of Homeland Security (DHS)? Can it be done by the National Counterterrorism Center (NCTC), even though it has only a coordinating function and relies on other agencies for intelligence collection, analysis, and operations? What is the role of the Office of the Director of National Intelligence (ODNI) in home-grown terrorism and recruitment and radicalization? Will coming to grips with these challenges be the remit of the next FBI Director given the incumbent’s impending retirement?

And, finally and most critically, have terrorists discovered our Achilles Heel in that we currently have no strategy to counter this type of threat or to interdict radicalization and prevent terrorist recruitment?

Ms. HARMAN. Thank you, Dr. Hoffman.

Mr. Jenkins, you are recognized for 5 minutes.

**STATEMENT OF BRIAN MICHAEL JENKINS, SENIOR ADVISER,
THE RAND CORPORATION**

Mr. JENKINS. Madam Chair, Mr. Chairman, thank you very much for the opportunity to address this important topic.

I have submitted written testimony, but let me here just underscore some of the aspects of current terrorist recruiting.

Nearly 9 years after 9/11, the principal terrorist threat comes from a galaxy of jihadist groups that subscribe to al-Qaeda’s ideology of global arms struggle. Their terrorist campaign has become more decentralized, relying more on al-Qaeda’s affiliates and on on-line exhortation to individual followers to do whatever they can wherever they are. Such attacks may take the form of operations planned from abroad like the Christmas day airline bombing attempt or do-it-yourself attempts by homegrown terrorists.

These attempts are not evidence of our failure to protect the Nation. They reflect the fact that we are at war, and as in any war, the other side attacks.

According to a recent RAND paper, there were 46 reported cases of radicalization and recruitment to jihadist terrorism in the United States between 9/11 and the end of 2009. A few more cases have been added in 2010. In all, 125 persons were identified in these cases. The number of cases and the number of persons involved, as Dr. Hoffman has pointed out, both increased sharply in 2009, underscoring the fact that radicalization and the recruitment to jihadist terrorism do happen here.

Fortunately, al-Qaeda’s exhortations are not resonating among the vast majority of Muslim Americans. There are veins of extremism. There are handfulls of hotheads, but no apparent deep reservoirs from which al-Qaeda can easily recruit.

The U.S. criminal justice system seems to be working. With the exception of Jose Padilla, the individuals arrested in these cases were brought before U.S. courts and convicted or now await trial.

Most of these American jihadists appear to have radicalized themselves rather than having been recruited in the traditional sense.

The process of radicalization and recruitment to terrorist violence reflects a combination of individual circumstances and ideological motivation. Jihadists cite assaults on Islam to justify their violence,

as we saw in these videos, but the volunteers also view jihad as a chance to gain status in a subculture that exalts violence to be perceived as a warrior, as a hero in an epic struggle. Again we saw in the videos here use of the term “glorious past” or “restoring honor.” These are recurring themes.

Al-Qaeda’s ideology also has become a vehicle for revolving individual discontents, an opportunity to transcend personal problems, a path to glory. This individualistic quality of self-recruitment suggests a strategy that focuses on dissuading individuals from joining al-Qaeda’s version of jihad. The message to would-be terrorists should be that they will be detected, apprehended, and treated as ordinary criminals. There will be no applause. There will be no glory.

Reinforcing this message requires the active cooperation of the American Muslim community, which is the target of this jihadist recruiting. Community policing can facilitate that cooperation. Now that doesn’t involve the authorities in religious or ideological debates, which remain matters for the community. It simply requires building trust between local communities and local authorities.

But community cooperation will not prevent all terrorist attempts. The domestic intelligence collection is essential. Only three of the 25 homegrown plots to carry out attacks in the United States, including the failed Times Square bombing, got as far as implementation. Only two of those attempts resulted in casualties, both carried out by lone gunmen.

Now that is an undeniable intelligence success. But we have to do better than that. Our current emphasis on information sharing, which certainly has improved, shouldn’t distract us from the difficult and always delicate task of information and intelligence collection.

Many homegrown terrorists begin their journey to violent jihad on the internet. It is accessible to seekers, reinforcing and channeling their anger, it creates on-line communities of like-minded extremists, it facilitates clandestine communications. Yet, it is important that we keep this in perspective.

Despite the continuous, incessant on-line exhortations to Americans from these jihadist websites, while they have produced an army of on-line jihadists, that has resulted in only a tiny cohort of jihadists in the real world. Moreover, the internet has proved to be a source of valuable intelligence leading to arrests.

One last point. I have no doubt that jihadists will attempt further terrorist attacks in this country, and that some will succeed; That is war. But needless alarm, divisive finger-pointing, and unreasonable demands for absolute protection will only encourage terrorists’ ambitions to make America tremble in fear and bankrupt itself in a quest for security, which is precisely what our terrorist foes hope to achieve.

Thank you.

[The statement of Mr. Jenkins follows:]

PREPARED STATEMENT OF BRIAN MICHAEL JENKINS¹

MAY 26, 2010

NO PATH TO GLORY

DETECTING HOMEGROWN TERRORISM²

Madame Chair, Members of the subcommittee, thank you very much for the opportunity to address this important topic. It is an honor to again testify before Congress and, for the third time, before Members of this subcommittee. The views I express are my own. I do not speak on behalf of any department, agency, organization, or political agenda.

A Determined, Resilient, Opportunistic, and Adaptable Foe

Nearly 9 years after 9/11, the principal terrorist threat still comes from a galaxy of jihadist groups that subscribe to or have been influenced by al-Qaeda's ideology of a global armed struggle against the West. The complexity of the movement defies easy assessment. The ability of al-Qaeda's central leadership to directly project its power through centrally planned and managed terrorist attacks has been reduced. Terrorist organizations now confront a more hostile operating environment: Al-Qaeda has not been able to carry out a major terrorist attack in the West since the London bombings of 2005. For the time being, it has concentrated its resources and efforts on the conflicts in Afghanistan and Pakistan.

This should not imply that we are at a tipping point in the struggle against terrorism. Al-Qaeda, its affiliates, and its allies, remain determined to continue to attack, and they have proved to be resilient, opportunistic, and adaptable, capable of morphing to meet new circumstances. Complacency on our part would be dangerous.

A More Decentralized Terrorist Campaign

To carry on its international terrorist campaign, al-Qaeda now relies on its affiliates, principally in North Africa, Iraq, and the Arabian Peninsula, and on its continuous exhortation to followers to do whatever they can, wherever they are. Other terrorist groups, while concentrating on local contests, have adopted al-Qaeda's vision of a global struggle and may launch their own attacks or assist volunteers seeking support.

Emphasis on Do-It-Yourself Terrorism

The United States remains al-Qaeda's primary target. Some analysts believe that al-Qaeda is under growing pressure to prove that it can carry out another attack on U.S. soil in order to retain its credentials as the vanguard of the jihadist movement. Such an attack could take the form of an operation planned from abroad, like the Christmas day airline bombing attempt, or it could be do-it-yourself attempts by homegrown terrorists responding to al-Qaeda's call to action. Inevitably, one or more of these attacks may succeed.

Terrorist attempts are not evidence of our failure to protect the Nation from terrorism, nor should they be cause for feigned outrage and divisive finger-pointing. They provide opportunities to learn lessons and improve defenses. The attempts reflect that we are at war—although the term has been largely discarded—and as in any war, the other side attacks.

America's Homegrown Terrorists

According to a recent RAND paper, there were 46 reported cases of radicalization and recruitment to jihadist terrorism in the United States between 9/11 and the end of 2009.³ This number does not include attacks from abroad. In all, 125 persons were involved in the 46 cases. Two more cases and several more arrests in 2010 bring the total to 131 persons. Half of the cases involve single individuals; the re-

¹The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to Federal, State, or local legislative committees; Government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

²This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT348/>.

³Brian Michael Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001*, Santa Monica: The RAND Corporation OP-292-RC, 2010.

mainder are tiny conspiracies. The number of cases and the number of persons involved both increased sharply in 2009. Whether this presages a trend we cannot yet say. But these cases tell us that radicalization and recruitment to jihadist terrorism do happen here. They are clear indications of terrorist intent. The threat is real.

No Deep Reservoirs of Potential Recruits

Fortunately, the number of homegrown terrorists, most of whom are Muslims, is a tiny turnout in a Muslim American community of perhaps 3 million. (By contrast, several thousand Muslim Americans serve in the U.S. armed forces.) Al-Qaeda's exhortations to violence are not resonating among the vast majority of Muslim Americans. There are veins of extremism, handfuls of hotheads, but no deep reservoirs from which al-Qaeda can recruit. America's would-be jihadists are not Mao's fish swimming in a friendly sea.

The cases do not indicate an immigration or border-control problem. Almost all of those arrested for terrorist-related crimes are native-born or naturalized U.S. citizens or legal permanent residents. Most of them have lived in the United States for many years. There is no evidence that they were radicalized before coming to the United States. No armies of "sleepers" have infiltrated the country.

The Criminal Justice System Works

The cases also tell us that the U.S. criminal justice system works. With the exception of Jose Padilla, who was initially held as an enemy combatant, the individuals arrested in these cases (except for those who left to join jihad fronts abroad) were brought before U.S. courts and convicted or now await trial.

About a quarter of those identified have links with jihadist groups—al-Qaeda, Lashkar-e-Taiba, or the Taliban—but there is no underground network of foreign terrorist operatives, and there are no terrorist gangs in the United States like those active in the 1970s, when the level of terrorist violence was much higher than it is today.

Amateurs are Still Dangerous

Twenty-five of the 131 terrorists identified in the United States since 9/11 received some kind of terrorist indoctrination or training. Judging by the results, it was not very good. Al-Qaeda clearly has quality-control problems. The plots have been amateurish. Only two attempts succeeded in causing casualties—significantly, both were carried out by lone gunmen, a problem in the United States that transcends terrorism. But amateurs are still dangerous. There is no long mile between the terrorist wannabe and the lethal zealot.

America's jihadists may suffer from substandard zeal. Only one became a suicide bomber, although Major Nidal Hasan may not have expected to survive his murderous rampage at Fort Hood. The rest planned to escape.

Most American jihadists appear to have radicalized themselves rather than having been recruited in the traditional sense. However, itinerant proselytizing recruiters appear in some of the cases, and active recruiting does occur in prisons. Many homegrown terrorists begin their journey to violent jihad on the internet.

Diverse Personal Motives

The process of radicalization and recruitment to jihadist terrorist violence is complex and reflects a combination of individual circumstances and ideological motivations. Personal crisis and political cause are often paired in the process.

What does the jihadist acolyte seek in terrorism? Although recruitment may involve the rhetoric of religious belief, turning to violent jihad does not seem to result from profound religious discernment. Few jihadists appear to have more than a superficial knowledge of Islam. On the other hand, radicalization and recruitment do appear to be opportunities for an ostentatious display of piety, conviction, and commitment to their beliefs, ultimately expressed in violence.

Jihadists often use the need to avenge perceived assaults on Islam—insults to the religion, atrocities inflicted upon its believers, aggression by infidels against its people and territory, anger at specific U.S. policies—to justify their actions. These certainly are jihadist recruiting themes, but volunteer terrorists also view jihad as an opportunity for adventure, a chance to gain status in a subculture that exalts violence, to overcome perceived personal humiliation and prove manliness, to demonstrate prowess, to be perceived as a warrior in an epic struggle.

For lonely hearts, joining jihad offers a camaraderie that can sweep the more malleable along to schemes they would otherwise not have contemplated. For those who feel powerless, violent action offers the secret pleasures of clandestinity and power that come with the decision to kill.

Al-Qaeda's ideology also has become a vehicle for resolving personal discontents, an opportunity to start life over, to transcend personal travail and turmoil through

bloody violence, to soothe a restless soul with the spiritual comfort of an absolute ideology that dismisses the now as a brief passage between a glorious mythical past and eternal paradise. The jihadist may see terrorism as a path to glory in every sense of that word.

The Message to Would-Be Terrorists: No Path to Glory

Dealing with domestic radicalization does not mean countering jihadist propaganda. It means applying the law. What one believes is a matter of conscience. What one does to impose his or her beliefs on others concerns everyone. When a course of action involves the threat or use of violence, it becomes a matter of law. America's response to homegrown terrorism must, above all, be based upon the law.

The individualistic quality of radicalization and recruitment to jihadist terrorism in the United States suggests a counter-recruitment strategy that focuses on dissuading individuals from joining al-Qaeda's version of jihad. This can be accomplished not through ideological or theological debate with al-Qaeda's on-line communicators, but by deterrence through arrests, by treating terrorists and would-be terrorists as ordinary criminals, by stripping them of political pretensions.

The message to would-be terrorists should be that they can trust no one. They will fail. They will be detected and apprehended. They will be treated as ordinary criminals and will spend a long time in a prison cell. They will receive no applause. They will disgrace their families and their communities. They will be labeled fools. Their lives will be wasted. There will be no glory.

Authorities could go further and consider something like Italy's so-called "repentant program," in which convicted terrorists were offered reduced sentences in return for their cooperation. This kind of program differs from routine plea-bargaining and from efforts abroad to rehabilitate terrorists. A "repentant" program would reward those who not only provide authorities with operational intelligence, but also contribute to understanding the recruitment process itself, and who actively participate in efforts to discourage others from following the same destructive path. It would let the denunciations of al-Qaeda motivator al-Awlaki come from his own acolytes.

Local Authorities are Best Placed to Counter Recruiting

Preventing future terrorist attacks will require the active cooperation of the American Muslim community, which is the target of jihadist recruiting. It will require effective domestic intelligence collection. Both are best accomplished by local authorities.

The first line of defense against radicalization and recruitment to jihadist terrorism in the Muslim-American community is the Muslim-American community. America's invasion of Iraq, its support for Ethiopia's invasion of Somalia, and its current military efforts in Afghanistan and Pakistan have created some pockets of resentment, but polls indicate little support for al-Qaeda's jihadist fantasies among American Muslims. Cooperation against terrorism means more than the public denunciations of al-Qaeda that many non-Muslim Americans demand as proof of Muslims' patriotism, nor should tips to police be the sole metric.

Much of the defense against jihadist radicalization will be invisible—quiet discouragement, interventions by family members and friends, and when necessary, discreet assistance to the authorities. Reports indicate that this is already taking place.

Community policing can maintain the cooperation that is needed. This does not involve police in religious or political debates, which are matters for the community. It requires building and maintaining trust between the community and local authorities and understanding local communities and diasporas, their problems, and their concerns.

Community cooperation will not prevent all terrorist attempts. Respected community leaders may have limited influence over more radical elements or may have no clue about tiny conspiracies or individuals who are on an interior journey to terrorism.

Members of the community must realize that while they play an important role in discouraging terrorism, they cannot be intermediaries in criminal investigations or intelligence operations aimed at preventing terrorist attacks. American Muslims should not regard themselves or be perceived by others as targets because they are Muslims. But being Muslim brings no privileged or separate status.

Disruption of Terrorist Plots: An Undeniable Intelligence Success

Twenty-five of the reported cases of homegrown terrorism involved plots to carry out attacks in the United States. Only three—including the failed Times Square bombing attempt—got as far as implementation, an undeniable intelligence success. And no doubt, other terrorist plots have been disrupted without arrests, while the publicized success of authorities has had a deterrent effect on still other plotters.

Intelligence has improved since 9/11. Federal Government agencies share more information with each other and with local police departments and fusion centers, although there are still some problems. But connecting dots is not enough, and the emphasis on information-sharing should not distract us from the difficult and delicate task of domestic intelligence collection.

Domestic Intelligence Collection Remains Haphazard

The diffuse nature of today's terrorist threat and the emphasis on do-it-yourself terrorism challenge the presumption that knowledge of terrorist plots will come first to Federal authorities, who will then share this information with State and local authorities. It is just as likely—perhaps more likely—that local law enforcement could be the first to pick up the clues of future conspiracies.

Local police departments are best placed to collect domestic intelligence. Their ethnic composition reflects the local community. They know the territory. They don't rotate to a new city every 3 or 4 years. They report to local authorities. But they often lack an understanding of intelligence and require resources and training.

Despite the clear need for improved domestic intelligence, collection remains haphazard. The Joint Terrorism Task Forces are extremely effective, but they are case-oriented, and investigation differs from intelligence. The fusion centers are venues for sharing information and have diverse responsibilities, but few collect intelligence.

An Army of On-Line Jihadists but Few Terrorists

The internet plays an important role in contemporary terrorism, as jihadists have effectively demonstrated. It allows global communications, critical to a movement determined to build an army of believers. It facilitates recruiting. It is accessible to seekers, reinforcing and channeling their anger. It creates on-line communities of like-minded extremists, engaging them in constant activity. It is a source of instruction. It facilitates clandestine communication.

The internet, however, has not enabled al-Qaeda, despite its high volume of sophisticated communications, to provoke a global intifada. Its websites and chat rooms outnumber its Western recruits. Its on-line exhortations to Americans have produced a very meager return—an army of on-line jihadists, but only a tiny cohort of terrorists in the real world. And while the internet offers would-be terrorists a continuing tutorial on tactics and improvised weapons, again thus far, this has not yet significantly improved terrorist skills.

Moreover, the internet provides insights into jihadist thinking and strategy and has proved to be a source of intelligence leading to arrests. This must be kept in perspective when considering countermeasures. These might include ways to address the issue of anonymity and facilitate investigations—and here, terrorist use of the internet represents only one facet of a much larger problem of cyber-crime.

I have no doubt that jihadists will attempt further terrorist attacks. Some will succeed. That is war. But I also have no doubt that these attacks will not defeat this republic or destroy its values without our active complicity, as long as we do not yield to terror.

Ms. HARMAN. Thank you very much. Mr. Romero.

**STATEMENT OF ANTHONY D. ROMERO, EXECUTIVE DIRECTOR,
AMERICAN CIVIL LIBERTIES UNION**

Mr. ROMERO. Good morning, Chairman Harman, Ranking Member McCaul and other Members of the subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union about the need to preserve our rights to privacy and free speech even in times of threat to our Nation. We commend you, Chair, for recognizing that our founding principles must not be sacrificed in the name of National security.

However, by billing this hearing as an examination of recruitment of new terrorists using internet facilities, the subcommittee suggests an inherent evil in allowing the internet to continue without some change to its current open forum. We are here to implore this committee to resist leveling its legislative guns at the most democratic form of modern communication.

The internet is our most important communications medium. It has been and must remain the most open marketplace of ideas. Any suggestion to limit this marketplace will not only be a direct and immediate harm to the speech and privacy rights of law-abiding Americans, but it would also erode the very principles that make our country the beacon of freedom to people around the globe.

To be clear, the internet is not our enemy. Terrorists are our enemies.

Now some suggest taking down websites containing terrorist-laden material is necessary like the ones we saw today. But such discretion is exactly the kind of censorship that the Supreme Court has repeatedly cast aside in more than 20 years. In 1984, Justice Blackmun cautioned "By placing discretion in the hands of an official to grant or deny a license, such a statute creates a threat of censorship that by its very existence chills free speech." In the landmark case of *Reno v. ACLU* the Court again clearly extended protection to internet speech saying "Our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to internet speech."

Our history, our Nation's history is replete with regrettable Government actions restricting free speech and privacy rights in the name of National security. Consider the Alien and Sedition Act of 1798 during a time of conflict with France. One measure made it a crime to publish false, scandalous, and malicious writing against the Government or its officials.

The Sedition Act of 1918 in which Congress prohibited the use of "disloyal, profane, scurrilous, or abusive language about the government, the flag, or the Armed Forces." It also outlawed anything that caused others to view the Government or its institutions with contempt.

The Cold War brought about a red scare characterized by Congressional witch hunts orchestrated by Senator Joseph McCarthy and the House Un-American Activities Committee, which ruined the careers of thousands of loyal Americans based purely on their associations or their beliefs.

The COINTELPRO spying program, in which the FBI opened over 500 domestic intelligence files between 1960 and 1974 targeting people solely on their political affiliations and beliefs and created a list of 26,000 individuals who would be rounded up in an event of National emergency.

Now if our history is any indication, some of the policies adopted in the wake of 9/11, such as lowering the threshold for electronic surveillance or efforts that might try to rein in certain kinds of on-line communications, that these two will be ultimately seen as a stain on our Nation's reputation as the leading protector of individual rights.

The best antidote to harmful speech is not censorship, but more speech. Not only will we stand by the principles we hold dear, but we will show the world and ourselves that we are not afraid of dissent. We will show that we are not afraid of the cacophony that must be our democracy.

On a practical level, by keeping the internet free from censorship, we will provide new clues to our law enforcement and intel-

ligence personnel tasked with the difficult and necessary job of seeking out those who would do us real harm.

We must also not forgo our traditional notions of privacy in the mad scramble to provide false notions of security. Our system, based on the existence of probable cause and judicial oversight, provides an appropriate balance that preserves personal privacy while providing law enforcement and intelligence officials with the tools they need.

Fear, or fear mongering, must not drive Government policies any longer. Protecting the First and Fourth Amendments, honoring our values, and making sure that we keep this country both safe and free is the only way to approach the crisis that does, in fact, confront us.

Thank you very much.

[The statement of Mr. Romero follows:]

PREPARED STATEMENT OF ANTHONY D. ROMERO

MAY 26, 2010

Good morning Chair Harman, Ranking Member McCaul, and Members of the subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU), its more than half a million members, countless additional supporters and activists, and 53 affiliates Nation-wide. The ACLU is one of the Nation's oldest and largest organizations committed to defending the Constitution and Bill of Rights in the courts and before the Executive and Legislative branches of Government. The ACLU is concerned about the need to steadfastly preserve our rights to privacy and free speech even in times of threat to our Nation. We all acknowledge the Government's legitimate interest in protecting the Nation from terrorism and in stemming actions that further the unlawful, violent acts of terrorist groups. But just because a threat exists does not justify the erosion of principles that are at the core of our Constitutional identity. The Constitution requires precision in pursuing legitimate Government goals to ensure the Government properly distinguishes between confederates of terrorist groups who seek to facilitate their unlawful aims, and others whose legitimate First Amendment-protected activity brings them into association with such groups. Sacrificing our civil liberties in the pursuit of security is unwise, unnecessary, and counterproductive to preventing extremist violence.

We commend this subcommittee for recognizing that our founding principles must not be sacrificed in the name of homeland security. Merely by billing this hearing as an examination of recruitment of new terrorists using internet facilities, however, the subcommittee suggests an inherent evil in allowing the internet to continue to exist in its current open form. Since terrorists use the internet to recruit new terrorists, as the narrative goes, Congress must do something to stop such on-line activity. We leave it to others to debate whether evidence shows that terrorists' use of the internet makes them more effective or simply more vulnerable to interception of their communications. Instead we are here to implore this subcommittee not to level its legislative guns at this most democratic of communications tools. The internet is merely a communications medium. It should remain the most open marketplace of ideas, where those who believe in the American system of individual rights should out-argue those who would advocate harm to our homeland. Any suggestion to limit this marketplace would not only be a direct and immediate harm to the speech and privacy rights of law-abiding Americans, it would also erode those very principles that make our country the beacon of freedom to people around the globe.¹

¹ Our statement before this subcommittee in December 2009 addressed our concern that some envisioned an overly rigid "path to extremism", whereas the best evidence suggests there is no fixed path and that there are many ways that individuals come to take violent action—whether based on extremist beliefs or not. In that hearing, we argued for a focus on how individuals become predisposed to violence and not on the nature of any ideology, since ideology—even extremist ideology—need not be inherently violent. Statement of Michael W. Macleod-Ball, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Violent Extremism: How Are People Moved from Constitutionally-Protected Thought to Acts of Terrorism?* (Dec. 15, 2009).

Without doubt, the rise of communications technologies presents challenges to those interested in preserving traditional civil liberties standards. Nearly 50 years ago, in a case involving the wearing of an undercover “wire”, Chief Justice Earl Warren anticipated many legal disputes of the more recent past. “The fantastic advances in the field of electronic communication,” he wrote in 1963, “constitute a greater danger to the privacy of the individual.”² Four years later, the Chief Justice also foresaw that measures adopted in the name of National security often posed special dangers to individual rights—an argument that bears directly on any proposal to limit the internet in the name of fighting terrorism. In *U.S. v. Robel*, he wrote:

“This concept of ‘National defense’ cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal. Implicit in the term ‘National defense’ is the notion of defending those values and ideals which set this Nation apart . . . [O]ur country has taken singular pride in the democratic ideals enshrined in its Constitution, and the most cherished of those ideals have found expression in the First Amendment. It would indeed be ironic if, in the name of National defense, we would sanction the subversion . . . of those liberties . . . which make the defense of our Nation worthwhile.”³

Today, we urge this subcommittee to stand strong for freedom as you work to protect our Nation from harm. If you find that our enemies are using the internet to recruit, we encourage use of the internet to dissuade. At the same time, we can and should be using their on-line communications to learn as much as is lawfully possible about those who would do us harm and their activities and motives, following proper law enforcement and intelligence procedures and with appropriate judicial oversight. We urge you to leave the internet alone as an unfettered place of freedom and anonymity—and preserve the rights to speech and privacy for all those law abiding Americans who use these “fantastic” forms of electronic communications.

I. FIRST AMENDMENT FREEDOMS

The First Amendment to the United States Constitution guarantees freedom of religion, speech, press, petition, and assembly.⁴ These protections are based on the premise that open and unrestrained public debate empowers democracy by enriching the marketplace with new ideas and enabling political and social change through lawful means.⁵ These freedoms also enhance our security. Though “vehement, caustic and sometimes unpleasantly sharp attacks on Government and public officials” have to be endured under our Constitutional system of Government, the uninhibited debate these freedoms guarantee is recognized as “essential to the security of the Republic” because it ensures a Government responsive to the will of the people.⁶ Moreover, as Justice Louis Brandeis explained, our Nation’s Founders realized that the greater threat to security lay not in protecting speech, but in attempting to suppress it:

“Those who won our independence . . . knew that order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope, and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable Government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies, and that the fitting remedy for evil counsels is good ones. Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law—the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.”⁷

Some who seek to curtail the use of email and websites by purported terrorists would do so by taking down websites. In order to do so, though, someone in Government would have to be assigned the job of deciding what sites to censor and what

²*Lopez v. U.S.*, 373 U.S. 427, 441 (1963) (Warren, J., concurring).

³*U.S. v. Robel*, 389 U.S. 258, 264 (1967).

⁴U.S. Const., amend. 1: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”

⁵See *U.S. v. Associated Press*, 52 F. Supp. 362, 372 (S.D.N.Y. 1943); *Roth v. U.S.*, 354 U.S. 476, 484 (1957).

⁶See *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964), quoting *Stromberg v. California*, 283 U.S. 359, 369 (1931).

⁷*Whitney v. California*, 274 U.S. 357, 375–376, (1927), (Brandeis, J., concurring).

sites to leave in place. Such discretion is exactly the kind of censorship that the Court has repeatedly cast aside. Justice Harry Blackmun addressed the notion of such discretionary censorship. “By placing discretion in the hands of an official to grant or deny a license, such a statute creates a threat of censorship that by its very existence chills free speech.”⁸ More specifically, the Supreme Court has held that internet speech is protected to the full extent of the First Amendment.⁹ “[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.”¹⁰ There is simply no fair and just way to draw a line that protects the rights of those who are merely controversial from those who are pursuing a more sinister objective.¹¹ Accordingly, such recommendations must yield to the enduring power of our First Amendment.

II. THE RIGHT TO PRIVACY

The Fourth Amendment to the U. S. Constitution establishes the core of our understanding of our right to privacy.¹² In short, government may not invade an individual’s privacy without justifying the need for doing so to a court. Courts have applied this basic principle to different forms of communications, including letters, telephone conversations, and other more advanced forms.¹³ Anticipating the oncoming development of privacy law, Justice William Douglas asserted that the right to be let alone is “indeed the beginning of all freedoms”.¹⁴

Some have argued that the on-line presence of websites advocating terrorist causes justifies casting aside the Fourth Amendment standard to chase down anyone who might have visited any such site. Just as the mere use of the internet as a tool does not justify setting aside our speech rights, so too should the privacy right remain untouched. No court will stand in the way of a legitimate and well-founded Government application for a search of electronic communications when probable cause exists to believe that wrongdoing has occurred or is about to occur. To now further blur the line that defines when law enforcement may secretly invade one’s personal communications will inevitably lead to abuse—as it has already done.¹⁵

III. GOVERNMENT INFRINGEMENT ON CIVIL LIBERTIES IN TIMES OF CRISIS

As Congress grapples with determining what it can do to help reduce the threat of terrorism within our borders, it is important to keep in mind that our Nation’s history is replete with regrettable Governmental actions restricting speech and privacy rights in the name of protecting the country. Indeed the ACLU was founded in 1920 to come to the defense of immigrants, trade unionists, and political activists who were illegally rounded up by the thousands in the infamous Palmer raids during America’s first “red scare,” a period of significant anarchist violence. Rather than focusing on finding the perpetrators of the violence, the Government sought anyone who supported similar political views, associated with disfavored organizations or wrote or spoke in opposition to Government policies. Lawyers who complained of the abuse, which included torture, coerced confessions, illegal searches and arrests, were subject to investigation themselves.¹⁶

⁸ *Secretary of State of Md. v. Munson Co.*, 467 U.S. 947, 964 n. 12 (1984).

⁹ *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

¹⁰ *Id.*

¹¹ “[T]he mere abstract teaching . . . of the moral propriety or even moral necessity for a resort to force and violence, is not the same as preparing a group for violent action and steeling it to such action.” *Brandenburg v. Ohio*, 395 U.S. 444, 448 (1969) (per curiam) (quoting *Noto v. U.S.*, 367 U.S. 290, 297–98). The *Brandenburg* opinion set aside a state statute that barred advocacy of the propriety of violence or voluntary assembly for such criminal purposes. *Id.*

¹² U.S. Const., amend. 4: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

¹³ See *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (letters and sealed packages); *Katz v. U.S.*, 389 U.S. 347, 352 (1967) (telephone communications); *Kyllo v. U.S.*, 533 U.S. 27, 34 (2001) (changing technology should not erode society’s expectation of privacy).

¹⁴ *Public Util. Comm’n v. Pollak*, 343 U.S. 451, 467 (1952) (Douglas, J., dissenting).

¹⁵ Substantial exceptions to the norm of requiring judicial approval for such searches have already been adopted. The USA PATRIOT Act and amendments to the Foreign Intelligence Surveillance Act provide major loopholes to traditional standards. We oppose those exceptions and have challenged some of them in court. Numerous reports, including those of the DOJ Inspector General, document abuses of these special authorities. Their existence serves as even further basis to argue against any form of additional extrajudicial surveillance authority for the purpose of seeking out those who visit websites relating in some way to terrorism or terrorist activities.

¹⁶ SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, 94TH CONG., FINAL REPORT ON SUPPLE-

We are able to see such actions for what they are when they occur in foreign lands. When Google was the subject of a sophisticated cyberattack and subsequently revealed that the Chinese government wanted its cooperation in blocking access to sites based on political content, the world was naturally aghast.¹⁷ But in contemporaneous public discourse we tend not to apply the same standards when our own Government attempts to take similar actions to restrict civil liberties in the name of National security. It is only well after the precipitating crisis has passed that we tend to see our own Government's actions in a clearer light.

The pattern of abusive Government action in the United States in times of crisis goes much further back than the Palmer raids of the 1920s and continues to today.

- *Alien and Sedition Acts.*—Congress enacted four bills in 1798 during a time of conflict with France. The Federalists in the John Adams administration strongly objected to the dissenting voices of those led by Thomas Jefferson and other Democratic-Republicans, who were generally sympathetic to the French cause. Of the four laws, the Sedition Act made it a crime to publish “false, scandalous, and malicious writing” against the Government or its officials. Negative reaction led to Jefferson’s election in 1800 and the laws ultimately expired or were repealed.¹⁸
- *Anarchist Exclusion Act.*—Congress passed this law to authorize the deportation of immigrants who subscribed to anarchist ideas. Adopted at a time of unrest concerning immigration into the United States, the Anarchist Exclusion Act was re-adopted following the assassination of President McKinley by the American son of Polish immigrants. The law’s authorities were expanded to allow wider discretion for deportations in the Immigration Act of 1918.¹⁹
- *Sedition Act of 1918.*—Congress prohibited the use of “disloyal, profane, scurrilous, or abusive language” about the Federal Government, the flag, or the armed forces. It also outlawed anything that caused others to view the Government or its institutions with contempt. It was repealed in 1920 after the war ended, but those convicted under its terms generally received sentences of 10 to 20 years.²⁰
- *Justice Department GID.*—Following World War I, the Department of Justice General Intelligence Division (GID), the precursor agency to the Federal Bureau of Investigation (FBI), collected 150,000 secret files “giving detailed data not only upon individual agitators connected with the radical movement, but also upon organizations, associations, societies, publications and social conditions existing in certain localities.”²¹ By the GID’s own account the warrantless searches, arrests, and deportations were not useful in identifying suspected terrorists or other criminal activity. Rather, its claimed success was in “wrecking the communist parties in this country” and shutting down “the radical press.”²²
- *State investigations.*—The New York State Legislature initiated a 2-year investigation from 1919 to 1920 into the spread of radical ideas. The Joint Legislative Committee to Investigate Seditious Activities (commonly referred to as the Lusk Committee) ultimately produced a report, *Revolutionary Radicalism: Its History, Purpose and Tactics*, which “smeared liberals, pacifists, and civil libertarians as agents of international Communism.”²³ Though thousands were ar-

MENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94–755, at 385 (1976), available at: http://www.aarclibrary.org/publib/church/reports/book3/html/ChurchB3_0196b.htm.

¹⁷“Google Said to Have Made No Progress in China Dispute,” Bloomberg Businessweek (Mar. 23, 2010) (available at <http://www.businessweek.com/news/2010-03-23/google-said-to-have-made-no-progress-in-two-month-china-dispute.html>).

¹⁸An Act for the Punishment of Certain Crimes against the United States, ch. 74, 1 Stat. 596 (available at http://avalon.law.yale.edu/18th_century/sedact.asp).

¹⁹An Act to Regulate the Immigration of Aliens into the United States, ch. 1012, 32 Stat. 1222.

²⁰Stone, Geoffrey R., *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism* (2004) (hereinafter Stone, *Perilous Times*).

²¹SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, 94TH CONG., FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94–755, at 386 (1976), [hereinafter, CHURCH REPORT] available at: http://www.aarclibrary.org/publib/church/reports/book3/html/ChurchB3_0196b.htm.

²²Id. at 387.

²³Samuel Walker, *In Defense of American Liberties: A History of the ACLU* (1990) at 16.

rested, few were prosecuted or deported and little incriminating information was obtained during the committee's investigation.²⁴

- *Smith Act*.—Congress outlawed the publication of any printed matter advocating the overthrow of the Government and required the registration of all non-citizen adult residents in 1940. The law was used for a number of high profile political prosecutions against isolationists, pro-fascists, and communists in the 1940s and 1950s, including one of the early leaders of the ACLU. The law fell into disuse after several convictions were set aside by the Supreme Court in the late 1950s.²⁵
- *McCarthy hearings and House Un-American Activities Committee*.—The Cold War brought about a new red scare characterized by Congressional witch hunts orchestrated by Senator Joseph McCarthy's Permanent Subcommittee on Investigations and the House Un-American Activities Committee, which ruined the careers of many loyal Americans based purely on their associations. In particular, their work helped to blacklist people from certain industries and in particular the entertainment industry in the late 1940s and 1950s based solely on political views of those who were targeted.²⁶
- *COINTELPRO*.—The FBI ran a domestic counter-intelligence program that quickly evolved from a legitimate effort to protect the National security from hostile foreign threats into an effort to suppress domestic political dissent through an array of illegal activities. The Senate Select Committee that investigated COINTELPRO (the "Church Committee") said the "unexpressed major premise of . . . COINTELPRO is that the Bureau has a role in maintaining the existing social order, and that its efforts should be aimed toward combating those who threaten that order."²⁷ Instead of focusing on violations of law, these investigations targeted people based on their beliefs, political activities and associations. FBI opened over 500,000 domestic intelligence files between 1960 and 1974, and created a list of 26,000 individuals who would be "rounded up" in the event of a National emergency.²⁸ The FBI used the information it gleaned from these improper investigations not for law enforcement purposes, but to "break up marriages, disrupt meetings, ostracize persons from their professions and provoke target groups into rivalries that might result in deaths."²⁹
- *Warrantless surveillance after 9/11*.—The Bush administration authorized a sweeping program of surveillance of electronic communications without Congressional approval. While some in Congress spoke out against the program, Congress ultimately not only authorized much of the surveillance after-the-fact, but also granted immunity to the large telecommunications companies that gave the Government access to the communications records in question.³⁰ In 2008, Congress legislated an even broader warrantless spying program when it passed the Foreign Intelligence Surveillance Act (FISA) Amendments Act, which permits the Government to intercept all international internet activity without an individualized warrant based on probable cause to believe that a crime or act of terrorism has been or will be committed, even if one party to the communication is a U.S. person within the boundaries of the United States.³¹
- *National security letter abuses*.—The month after 9/11, Congress enacted the USA PATRIOT Act which greatly expanded the FBI's ability to access private records without judicial oversight. The FBI actually went further and abused

²⁴The Lusk Committee: A Guide to the Records of the Joint Committee to Investigate Seditious Activities: A Guide to the Records Held in the New York State Archives, available at: http://www.archives.nysed.gov/a/research/res_topics_bus_lusk.shtml.

²⁵18 USC § 2385. See also Stone, *Perilous Times*.

²⁶Goodman, Walter, *The Committee* (1968); Whitfield, Stephen J., *The Culture of the Cold War* (1996).

²⁷CHURCH REPORT, at 7.

²⁸*Id.*, at 6–7.

²⁹*Id.*, at 5.

³⁰ACLU letter to U. S. Senate, "Vote NO on H.R. 6304, the FISA Amendments Act—Oppose Warrantless Surveillance and Immunity for Telecommunications Companies" (Jun. 25, 2008) (available at http://www.aclu.org/files/images/general/asset_upload_file902_35782.pdf).

³¹50 U.S.C. §§ 1881–1881g. Allegations of abuse go well beyond the electronic surveillance issues referenced here. Many American Muslim community leaders and members have pointed to the selective and disproportionate enforcement of counterterrorism laws against American Muslim individuals and charities as evidence of discriminatory, religion-based targeting of Muslims and their charitable organizations. See *Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the War on Terrorism Financing*, ACLU (Jun. 2009) (available at www.aclu.org/human-rights/report-blocking-faith-freezing-charity). Congress must avoid conflating the real issue of terrorism recruiting with the right to dissent or the right to practice one's religious beliefs.

the vastly expanded authorities it received under the new law. It used the authority to acquire records having no relation to National security and it used NSLs to circumvent other authorities requiring judicial oversight.³² The USA PATRIOT Act unconstitutionally amended other provisions of surveillance laws so that the Government could obtain communications and records of individuals who are not suspected of engaging in or preparing for an act of terrorism.³³

Unfortunately, we have not yet seen the outrage and curative legislation to the Executive branch's unilateral initiation of systematic surveillance of email and telephone records without Congressional authorization in the years following 2001. It did not exist in sufficient force to cure those unlawful executive actions, just as it did not exist in sufficient force to immediately overturn the Sedition Act or the Anarchist Exclusion Act or the Smith Act. Perhaps we are still too close the shocking events of September 11 and we remain blind to the harm that arises out of such restrictions on our freedoms. If history is any indication, however, in time these laws will be seen as a stain on our Nation's reputation as the leading protector of individual rights—and any attempt to limit speech on the internet, even for the purpose of protecting the homeland, will surely be viewed by later generations in the same harsh light as we now view the Alien and Sedition Acts and the hearings of the House Un-American Activities Committee and the actions of the FBI under COINTELPRO.

IV. PROTECT SPEECH AND PRIVACY ON THE INTERNET

A report by the Senate Homeland Security and Governmental Affairs Committee (HSGAC) entitled *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat* placed inordinate and inappropriate significance on the role of the internet in the radicalization process.³⁴ The internet is simply a tool for communication and the expression of ideas—some beneficial, some benign, some harmful. In that sense, the internet is like the printing press or the postal service or the telephone. Focusing on the tools used to transmit despised ideas as the key to solving our security problem only increases the likelihood that censorship on the internet will be part of a proposed solution. Indeed, shortly after the publication of the HSGAC report Senator Joseph Lieberman sent a letter to Google calling on them to take down “terrorist content.”³⁵ We are concerned that this subcommittee, seeking to reduce on-line recruits to terrorist causes, will make the same mistakes made by countless lawmakers throughout our history.

Government censorship violates the First Amendment and undermines democracy. Moreover, any attempt to censor the internet would be futile and counter-productive. Electronic content is ubiquitous and easily transferable. Media removed from one source is often duplicated elsewhere, and a closed website can soon reopen in another guise and at another location. Lt. Col. Joseph Felter, Ph.D., Director of the Combating Terrorism Center at West Point, told the HSGAC that “[a]ttempts to shut down websites have proven as fruitless as a game of whack-a-mole.”³⁶ Such attempts at censorship would only bring greater attention to the objectionable content.

It is vital to the freedom of all Americans that free speech on the internet be protected. It is possible that the unique nature of the cyber-revolution has posed some challenges in protecting the internet.³⁷ But such a conclusion would not be unique to the internet. “Each medium of expression . . . may present its own problems.”³⁸

³²A *Review of the FBI's Use of National Security Letters*, DOJ Office of Inspector General (Mar. 2007) (available at <http://www.justice.gov/oig/special/s0703b/final.pdf>).

³³See 50 U.S.C. § 1861, as amended by Section 215 of the USA PATRIOT Act. This statute permits Government to obtain a secret court order for “any tangible thing” upon showing “relevance” to a foreign intelligence investigation, such as a list of every person who visits a certain website, a list of every person who entered a certain search term into a search engine, or the identity of an anonymous poster on a website.

³⁴United States Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff Report, “Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat,” (May 8, 2008). The report noted, for instance, that “For those who want to know more about violent Islamist ideology, immense caches of information and propaganda are available on-line,” and “the internet can play a critical role throughout the radicalization process, the potential end point of which is planning and executing a terrorist act.” *Id.* at 5, 10.

³⁵Letter from Senator Joseph Lieberman to Dr. Eric Schmidt, Chairman of the Board and Chief Executive Officer, Google, Inc., (May 19, 2008) at: <http://lieberman.senate.gov/newsroom/release.cfm?id=298006>.

³⁶Statement of Lt. Col. Joseph Felter, Hearing before the Senate Committee on Homeland Security and Governmental Affairs, “The Internet: A Portal to Violent Islamist Extremism,” (May 3, 2007), at: <http://www.investigativeproject.org/documents/testimony/224.pdf>.

³⁷*Universal City Studios, Inc. v. Corley*, 273 F. 3d 429, 433 (2d Cir. 2001).

³⁸*Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 557 (1975).

Nevertheless, our “profound national commitment to the free exchange of ideas” requires that we meet those challenges to preserve fundamental freedoms, on the internet just as rigorously as in other forms of communication.³⁹

Courts acknowledge the importance of keeping the web’s channels of communication open and free from discrimination. The United States Supreme Court has concluded that speech on the internet is entitled to the highest level of protection under the First Amendment. Any attempts to censor its content or silence its speakers are viewed with extreme disfavor.⁴⁰

In addition, courts recognize that the public has a First Amendment interest in receiving the speech and expression of others. “[T]he right of the public to receive suitable access to social, political, aesthetic, moral and other ideas and experiences” is one of the purposes served by the First Amendment.⁴¹ Indeed, the “widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public.”⁴² The internet has become the principal source for the public to access this diversity of ideas—good ideas, bad ideas, and all those in between.⁴³

Courts also understand that “the internet represents a brave new world of free speech.”⁴⁴ Specifically, the internet provides unique opportunities for speech and discourse. Unlike other communication media, “the internet has no ‘gatekeepers’—no publishers or editors controlling the distribution of information.”⁴⁵ As a result, the internet does not suffer from many of the limitations of alternative markets for the free exchange of ideas. Therefore, courts have vigorously protected the public’s right to uncensored internet access on First Amendment grounds.

In a similar vein, Congress has enacted legislation to protect and promote free speech on the internet. In the 1996 Telecommunications Act, Congress found that “[t]he rapidly developing array of internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.”⁴⁶ Congress further declared that it is the policy of the United States “to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the internet.”⁴⁷ Congress therefore immunized internet providers and users from any liability for publishing “any information provided by another information content provider.”⁴⁸

V. CONCLUSION

The best antidote to harmful speech is more speech expressing countervailing messages. It is far better in this context, then, to do the best possible job to oppose the messages with which we disagree than to stifle them and drive them underground. Not only will we stand by the principles we hold dear, we will show that we are not afraid of dissent and that we will stand toe-to-toe with all comers and stand proud of our faith in our institutions and principles. Moreover, by refusing to yield to those who would censor the internet, we provide new clues to our law enforcement and intelligence personnel tasked with the difficult job of seeking out those specific individuals who would do us harm. Active censorship would minimize the availability and utility of such information.

Similarly, we must not forego our traditional notions of privacy in the race to provide security. Our well-tested system, based on the existence of probable cause to believe wrongdoing has occurred or is about to occur and appropriate judicial oversight, has served our country well. That system provides an appropriate balance that preserves the personal privacy of our fellow Americans, while providing law enforcement and intelligence officials the tools they need. Disrupting that balance

³⁹ *Harte-Hanks Comm., Inc. v. Connaughton*, 491 U.S. 657, 686 (1989).

⁴⁰ See, e.g., *Ashcroft v. ACLU*, 542 U.S. 656 (2004) (upholding a preliminary injunction of the Child Online Protection Act); *Reno v. ACLU*, 521 U.S. at 844 (striking down certain provisions of the Communications Decency Act).

⁴¹ *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 390 (1969).

⁴² *Metro Broad., Inc. v. FCC*, 497 U.S. 547, 566–67 (1990) (quoting *Associated Press v. U.S.*, 326 U.S. 1, 20 (1945)).

⁴³ Over one billion people have used the internet, including nearly 70 percent of all people in North America. See <http://www.internetworldstats.com/stats.htm> (visited on Oct. 4, 2006).

⁴⁴ *Blumenthal v. Drudge*, 992 F. Supp. 44, 48 n. 7 (D.D.C. 1998) (quoting Sanford & Lorenger, *Teaching an Old Dog New Tricks; The First Amendment in an Online World*, 28 Conn. L. Rev. 1137 (1996)).

⁴⁵ *Id.*

⁴⁶ 47 U.S.C. § 230(a)(1).

⁴⁷ 47 U.S.C. § 230(b)(3).

⁴⁸ 47 U.S.C. § 230(c)(1).

would put later prosecutions at risk while necessarily heightening Government intrusion into the private affairs of wholly innocent individuals.

Fear should not drive our Government policies. As Justice Louis Brandeis reminds us:

“To courageous, self-reliant men, with confidence in the power of free and fearless reasoning applied through the processes of popular government, no danger flowing from speech can be deemed clear and present unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion . . . Such must be the rule if authority is to be reconciled with freedom.”⁴⁹

The statement is just as true applied to standards of personal privacy. Protecting our First and Fourth Amendment freedoms will both honor our values and keep us safe.

Ms. HARMAN. Thank you, Mr. Romero.

I just would underscore the title of this hearing in light of what you have just said, which is: “Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?”

Now I yield 5 minutes to Mr. Morris to summarize his testimony.

**STATEMENT OF JOHN B. MORRIS, JR., GENERAL COUNSEL,
CENTER FOR DEMOCRACY AND TECHNOLOGY**

Mr. MORRIS. Madam Chair, Mr. Chairman, Ranking Member McCaul, and Members of the committee, on behalf of the Center for Democracy and Technology I would like to thank you for the opportunity to testify, and I would like to applaud the committee for, as Chair Harman just pointed out, for focusing a hearing on the need to balance free speech versus the need to protect this country, both of which are very important needs.

On the key Constitutional question let me just start by simply agreeing with the analysis presented by Mr. Romero.

The First Amendment places important limitations on Governmental actions to restrict speech, even speech by those who would do harm to the United States, and these Constitutional principles must underlie any analysis of Governmental responses to terror recruiting. In the context of the internet, these concerns are even more challenging.

But beyond the Constitutional issues, I would like to spend a few minutes looking at the broader statutory context in which speech on the internet arises. A key question that is implicit in this hearing is what, if anything, can the Government do to stop the recruiting of terrorists on-line? That leads to the question of should we require service providers who facilitate internet communications to act to somehow stop the terror recruiting?

So in the language of the internet, the service providers are often called, at least legally called, intermediaries. The ISPs that allow you access to the internet, the on-line websites, and services like YouTube and Facebook are all intermediaries whose services enable users, including both speakers and listeners, to exchange ideas and communicate on-line.

These intermediaries are really what sets the internet apart from other forms of mass communications. With newspapers and TV, the owner of the newspaper or the owner of the TV station is the one who picks and chooses what gets put up and communicated to the

⁴⁹ *Whitney v. California*, 274 U.S. 357, 376, (1927), (Brandeis, J., concurring).

masses. But on the internet, in contrast, anyone can publish to the entire world often for little or no money. This openness has transformed our society, allows all of us, including terrorists, to become content creators, creating a vast audience, reaching a vast audience without having to own a newspaper or a TV station. As Mr. Romero says, that really has transformed our society for the better.

But this new structure has led to new questions such as should intermediaries, should the ISPs and the web hosting companies be responsible or legally liable for the content that their users put up?

In 1996, Congress took a very strong action to answer this question and to protect on-line intermediaries from responsibility for the content that their users post. As part of the Telecommunications Act of 1996, Congress passed what is now known as simply Section 230 of the Communications Act. Section 230 says in its simple terms that on-line service providers cannot be held to be responsible for the content posted by their users.

This intermediary protection has been extraordinarily successful and is directly responsible for the explosive growth of innovative and dynamic new services. But by protecting on-line providers, Congress enabled the huge range of social networking and video sharing sites and other Web 2.0 services that enable individual citizens and constituents to speak on-line.

So as this committee considers the problem of on-line terror recruiting, we would urge it to keep in mind how vital intermediary protection has been to the growth of the internet. If Congress were to somehow make on-line services responsible to keep terror recruiting off of the internet, that could have a significant harmful effect on the growth of the internet.

Let me look at one example, just to look at YouTube, the YouTube video sharing service. On that site, users post 24 hours of video every single minute of every day. If Congress compelled YouTube to examine each one of these videos before allowing it to be posted on-line to be sure that it didn't have objectionable content, YouTube simply couldn't continue to operate as an open forum for user expression. The same is true of countless other forums and blogs where users post hundreds of thousands of comments every hour.

The protection for intermediaries has been a key foundation for the success of the internet, and a decision to undo that would raise some grave concerns about the future of the internet.

It doesn't mean that there is nothing that can be done. To speak to what Congressman McCaul asked about self-monitoring, YouTube is another good example. They have terms of service that specifically allow them to take down incitements to violence. I don't know if these videos were on YouTube, I don't know what YouTube would say about these particular videos. But videos that really do incite violence, YouTube will certainly look at. They have a 24/7 staff to review complaints about videos, and I think they would take prompt action.

Thanks very much.

[The statement of Mr. Morris follows:]

PREPARED STATEMENT OF JOHN B. MORRIS, JR.

MAY 26, 2010

FREE SPEECH AND ONLINE INTERMEDIARIES IN AN AGE OF TERROR RECRUITMENT

Chair Harman, Ranking Member McCaul, and Members of the subcommittee: On behalf of the Center for Democracy & Technology (CDT),¹ I thank you for the opportunity to testify today. The issues raised by on-line terror recruiting are difficult ones, made challenging by the Constitutional and statutory implications of any Governmental attempts to regulate on-line speech. We applaud the subcommittee for holding this hearing, which directly looks at the free speech questions raised, and we appreciate the opportunity to address the implications that regulation of terror recruiting could have for on-line free speech, as well as for innovation and competition on the internet.

INTRODUCTION AND OVERVIEW

Terrorism is a defining threat in our society today, and the use of any medium of communications—including the internet—to recruit foot soldiers for terror attacks on the United States is a serious concern. It is understandable and appropriate that this subcommittee should consider possible Governmental responses to this concern, and the legal and Constitutional implications of such responses.

There are a number of possible Governmental responses to on-line terror recruitment, including (among others) seeking to directly prohibit speakers from posting such content and seeking to require on-line service providers to prevent such speech from being posted in the first place, or otherwise holding service providers responsible for the speech. This testimony first looks at the First Amendment issues raised by any Governmental attempt to restrict on-line speech. The testimony then focuses on one possible response—seeking to make on-line websites and services responsible for policing user content for on-line terror recruitment activities, or otherwise being held liable for such content.

This possible response is one part of a larger question of whether on-line “intermediaries” should be liable or responsible for content posted by their users. The term “on-line intermediary” encompasses conduits (such as ISPs) and platforms (such as social networks and video sharing sites) that allow users to access on-line content and communicate with one another. In 1996, Congress enacted broad and strong protection for intermediaries from attempts to impose liability on them for content posted by others, or otherwise force them to police the content posted on-line. This intermediary liability protection has been extraordinarily successful and is directly responsible for the explosive and innovative growth of on-line services that we have experienced over the past decades. By protecting on-line providers from intermediary liability, Congress enabled a huge range of innovative new websites to offer social networking, video sharing, and other “Web 2.0” services that have transformed how we do business and socialize on-line.

A decision by Congress to step back from such protections and to impose obligations on service providers to police on-line content—even in the effort to fight terrorism—would have serious and harmful implications both for free speech on-line and for innovation and competition in on-line services. We urge this subcommittee to exercise great caution as it considers what steps would be appropriate to respond to on-line terror recruiting.

INTELLIGENCE AND LAW ENFORCEMENT CONSIDERATIONS

Before addressing the range of issues raised by terror recruiting, we would like to raise a threshold question for the subcommittee to consider. A mandate requiring the removal of terror recruiting content on-line could be counterproductive to the fight against terrorism. On-line content gives insight into terrorist groups’ intentions and methods. In a range of contexts, on-line content provides law enforcement and intelligence agencies with a wealth of information about the messages of terrorists groups, as well as the sources of the communications. Using appropriate legal process, Government agencies may be able gain invaluable information about terrorist operations by monitoring on-line sites and services. It is thus not clear that a broad mandate to block or remove this type of content would be the most effective response to it.

¹The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the internet open, innovative, and free. Among our priorities is preserving the balance between security and freedom in an age of terrorism. CDT has offices in Washington, DC, and San Francisco.

TERROR RECRUITING AND THE FIRST AMENDMENT

As Congress considers possible responses to terror recruiting, it must confront an unavoidable fact: that most of the “anti-American” speech of terrorists and other enemies of the United States is protected speech under our First Amendment. The modern First Amendment shields from Government regulation even speech that calls for the demise of the United States, so long as the speech does not cross the line into an incitement to violence or a “true threat.”

As the Constitutional context for the subcommittee’s consideration of terror recruiting, it should consider at least two important strands of First Amendment doctrine: First, the limits on restrictions on violent content and content that might incite violence, and second, the limits on the Government’s ability to impose a “prior restraint” on unlawful speech.

Violence, Incitement to Violence, and True Threats

On-line content that seeks to recruit for a terrorist cause may contain three different types of content that have been addressed in First Amendment cases: Depictions of violence, incitement to violence, and “true threats” of violence.

While the U.S. Supreme Court has deemed certain sexual content to be obscene—and thus outside of the protection of the First Amendment—the Court has never declared that violent expressive content should be excluded from First Amendment protection. In a 1948 case focused on crime story magazines, the Supreme Court concluded that depictions of violence in the magazines are “as much entitled to the protection of free speech as the best of literature.”² Consistent with that conclusion, courts have rejected attempts to characterize violent content as “obscene”: “Material that contains violence but not depictions or descriptions of sexual conduct cannot be obscene.”³ And last month, in a case involving depictions of animal cruelty, the Supreme Court again declined to expand the realm of Constitutionally permissible speech restrictions past the few categories of speech it has historically included.⁴ As Chief Justice Roberts wrote in that case:

“The First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs. Our Constitution forecloses any attempt to revise that judgment simply on the basis that some speech is not worth it. The Constitution is not a document ‘prescribing limits, and declaring that those limits may be passed at pleasure.’”⁵

In light of these decisions, terrorist communications that simply depict violent or terrorist acts would likely be beyond the reach of Government regulation.⁶

Speech that incites violence, however, can in some context be regulated, but the First Amendment nevertheless protects speech that merely advocates for violence. In its 1969 decision in *Brandenburg v. Ohio*, the Supreme Court held that:

“[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or regulate advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.”⁷

A few years later, the Court made clear that to be advocacy of violence could be prohibited only where there was evidence that challenged speech was “intended to produce, and likely to produce, imminent disorder.”⁸

In evaluating terror recruitment, a court applying the *Brandenburg* test would consider whether the speech would likely yield “imminent” violence. A related but murkier area of the law is the First Amendment jurisprudence allowing the prohibition of a “true threat.” Generally, the First Amendment will not protect statements that convey a direct threat of violence against particular individuals, but the courts

² *Winters v. New York*, 333 U.S. 507, 510 (1948).

³ *Video Software Dealers Ass’n v. Webster*, 968 F.2d 684, 688 (8th Cir. 1992). See also *Eclipse Enters., Inc. v. Gulotta*, 134 F. 3d 63, 66 (2d Cir. 1997) (“We decline any invitation to expand these narrow categories of [unprotected] speech to include depictions of violence.”).

⁴ *United States v. Stevens*, 559 U.S. _____ (2010) (available at <http://www.supremecourt.gov/opinions/09pdf/08-769.pdf>).

⁵ *Id.* at _____ (quoting *Marbury v. Madison*, 1 Cranch 137, 178 (1803)).

⁶ The Supreme Court recently agreed to review a case concerning violent content and minors, see *Video Software Dealers Ass’n v. Schwarzenegger*, 556 F. 3d 950 (9th Cir. 2009), cert. granted, 559 U.S. _____ (2010), but that appeal is unlikely to affect the Constitutional analysis of a broader restriction on violent content.

⁷ *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969). See also *Hess v. Indiana*, 414 U.S. 105 (1973) (speech of antiwar protestor not intended to incite violence).

⁸ *Hess*, 414 U.S. at 109 (1973) (finding that speech of antiwar protestor was not intended to incite violence).

have struggled to provide a clear test by which to gauge a “true threat.” In its 1969 decision in *Watts v. United States*, the Supreme Court concluded that an anti-war protester who threatened the President was not making a “true threat.”⁹ In 2003, although not speaking for a majority of the Court, Justice O’Connor explained that a “true threat” was “where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death.”¹⁰ But the Supreme Court has made clear in the “true threat” context that “mere advocacy of the use of force or violence does not remove speech from the protection of the First Amendment.”¹¹

Only a few reported cases have addressed the use of the internet in the incitement of or threat of violence. In *United States v. Harrell*, the defendant was convicted of posting a terrorist threat to an internet chat site on the day following the September 11, 2001, terrorist attacks on the United States; the defendant apparently did not raise, and the court did not address, any First Amendment issues concerning the incident.¹²

In *Zieper v. Reno*, the courts addressed a case in which a U.S. Attorney’s office attempted (with some brief success in November 1999) to suppress the display on a website of a video film “which depicted a planned military takeover of New York City’s Times Square during the millennial New Year’s Eve.”¹³ According to allegations made in a later action for damages and injunctive relief, Federal officials sought to block public access to the film; the website owner removed the film from the internet, but later restored it and the Federal officials took no further action. In the damages action, the district court concluded that the plaintiffs had adequately pleaded a First Amendment violation.¹⁴

The most significant case concerning violence or threats of violence over the internet involved an anti-abortion website. In *Planned Parenthood of Columbia/Willamette, Inc. v. American Coalition of Life Activists*, plaintiff doctors (who provided medical services including abortions to women) challenged a website that contained “Wanted” style posters targeting doctors (and some of the doctors targeted were in fact murdered). The Ninth Circuit Court of Appeals concluded that the “Wanted” posters did constitute a “true threat” and thus were not protected under the First Amendment.¹⁵

Under the prevailing First Amendment jurisprudence, any attempt to regulate terror recruiting on the internet would likely face strong First Amendment challenges, but depending on the precise language of the recruiting message and whether it contained a “true threat” or an incitement to imminent violence, it is possible that such speech could Constitutionally be subject to criminal penalties.

Prior Restraints

Beyond the question of whether terror recruiting can Constitutionally be penalized is the question of whether such speech could be the subject of a prior restraint—that is, whether it could be restricted on a blanket basis, in advance, and without a full panoply of procedural safeguards.

The concern over prior restraints on speech is central to our First Amendment jurisprudence. The First Amendment was first conceived as a prohibition on prior restraints, in response to the seventeenth century English system that licensed all printing presses and prevented anything from being printed without prior permission from the governing authorities.¹⁶ As the Supreme Court made clear in the leading modern prior restraint case, *Bantam Books, Inc. v. Sullivan*, “[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its Constitutional validity.”¹⁷ The Government bears “a heavy burden of showing justification for the imposition of such a restraint.”¹⁸ As evidenced by the

⁹ *Watts v. United States*, 394 U.S. 705 (1969).

¹⁰ *Virginia v. Black*, 538 U.S. 343, 360 (2003).

¹¹ *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 927 (1982).

¹² *United States v. Harrell*, 207 F. Supp. 2d 158 (S.D.N.Y. 2002).

¹³ *Zieper v. Reno*, 30 Media L. Rep. 2164, 2164 (S.D.N.Y. 2002). See also *Zieper v. Reno*, 111 F. Supp. 2d 484 (D.N.J. 2000).

¹⁴ *Zieper v. Metzinger*, 62 Fed. Appx. 383 (2nd Cir. 2003). In another case, a Federal court concluded that a website operator who listed names, addresses, and telephone numbers of law enforcement personnel was protected by the First Amendment, since that information, even if made available with the intent to harm, could not be a threat. See *Sheehan v. Gregoire*, 272 F. Supp. 2d 1135 (W.D. Wash. 2003).

¹⁵ *Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058, 1087–88 (9th Cir. 2002).

¹⁶ See *Near v. State of Minn. ex rel. Olson*, 283 U.S. 697, 713–14 (1931) (discussing original focus of First Amendment).

¹⁷ *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963).

¹⁸ *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971).

case involving the “Pentagon Papers,” even a strongly asserted claim of National security may not overcome the presumption against prior restraints.¹⁹

The courts have allowed prior restraints to stand only in the narrowest of contexts. For example, because obscene material has been declared to be unprotected under the First Amendment, the courts have allowed prior restraint of specific obscene items. But, even with content that is not protected by the First Amendment, the First Amendment requires that strict procedural safeguards be implemented and followed before a prior restraint would be upheld.²⁰ In a long line of cases, the Supreme Court has articulated clear procedures that must be followed, including (a) an adversarial hearing, (b) with the burden on the Government, and (c) with clear opportunity for prompt judicial review and appeal.²¹ The Supreme Court has made clear that any prior restraint of speech can only “take[] place under procedural safeguards designed to obviate the dangers of a censorship system.”²²

Moreover, the problems raised by prior restraints are even greater on the internet, where on-line content can change frequently and quickly, and where the primary means of identifying content (“IP addresses” such as “124.45.23.98,” and world wide web “URLs” such as “http://www.cdt.org”) are only pointers to potentially changing content. Thus, even if content on a particular day at a particular website is determined by a court to be a “true threat” or an incitement to violence, the content could change the next day and the prior determination of illegality would not apply to the new content. The Supreme Court has made clear that a finding that a particular publication or venue was found to contain or display illegal content was not enough to justify imposing a prior restraint on future content in the publication or at the venue.²³ Consistent with the Court’s holdings, in 2004 a district court in Pennsylvania struck down as unconstitutional a State prior restraint law that applied to websites.²⁴

The Supreme Court sets a very high bar against prior restraints. The Court has noted:

“The presumption against prior restraints is heavier—and the degree of protection broader—than that against limits on expression imposed by criminal penalties. Behind the distinction is a theory deeply etched in our law: A free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand.”²⁵

BEYOND THE CONSTITUTION: PROTECTION FOR ONLINE INTERMEDIARIES

In considering possible approaches to terror recruiting, a threshold question is whether the Government can Constitutionally regulate or prohibit the speech at issue. If the speech falls into a category that can be restricted, then the Government can consider using the criminal law to penalize the speech.

The question of whether the Government can do more—such as to try to prevent the speech from occurring in the first place—raises the prior restraint issues discussed above. In the internet context, this question also raises another vital issue: What responsibilities, if any, should be placed on the service providers and other intermediaries to control the targeted content?

To assess this question, it is critical that the subcommittee understand the broader context of the strong intermediary liability protection that has marked the United States’ approach to on-line content since the early days of the commercial internet. This protection has played an essential part in supporting the innovation and growth that we have experienced in on-line services. As important as the fight against terrorism unquestionably is, we urge the subcommittee not to go down the path of seeking to impose liability or responsibility for content on intermediaries.

The Need for Strong Protections for Intermediaries

The global internet has become a vibrant and essential platform for economic activity, human development, and civic engagement. Every day, millions of journalists, educators, students, business people, politicians, and ordinary citizens go on-line to

¹⁹ *New York Times Co. v. United States*, 403 U.S. 713 (1971).

²⁰ See, e.g., *Freedman v. State of Md.*, 380 U.S. 51 (1965).

²¹ See, e.g., *Freedman*, 380 U.S. at 58–59; *Southeastern Promotions Ltd. v. Conrad*, 420 U.S. 546, 560 (1975); *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 227 (1990).

²² *Southeastern Promotions*, 420 U.S. at 560 (quoting *Freedman*, 380 U.S. at 58).

²³ See *Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931) (holding where publication was a magazine); *Vance v. Universal Amusement Co., Inc.*, 445 U.S. 308 (1980) (holding where venue was a movie theatre).

²⁴ See *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 656 (E.D. Pa. 2004).

²⁵ *Vance*, 445 U.S. at 316 n. 13.

speak, access information, and participate in nearly all aspects of public and private life.

Internet service providers (ISPs), websites, on-line services, and a range of other technology companies act as conduits and platforms for speech. These “intermediaries” play critical roles in getting information and ideas from one corner of the on-line world to another, and they provide valuable forums for speech, from the political to the mundane—forums that are open, up-to-the-minute, and often free of charge.

The openness of these forums means, of course, that some users will post content or engage in activity that is unlawful or otherwise offensive. Liability for on-line content can arise in a number of situations, including for defamation, obscenity, invasion of privacy, or intellectual property infringement. This reality raises important policy questions that have an impact on the growth of the on-line environment: Specifically, should technological intermediaries such as ISPs and on-line services be held liable for or be responsible to police content posted by their users and other third parties?

The answer in the United States has been to protect intermediaries from responsibility to police content posted by users.²⁶ While users themselves should remain responsible for their unlawful on-line activities, policies protecting intermediaries from liability for content posted by third parties expand the space for expression and innovation and promote the internet as a platform for a wide range of beneficial activities. The history of the internet to date shows that providing broad protections for intermediaries against liability is vital to the continued robust development of the internet.

The internet developed and flourished because of an early U.S. policy framework based on competition, openness, innovation, and trust. This framework places power in the hands not of centralized gatekeepers, but rather of the users and innovators at the edges of the network. Importantly, this approach provides broad protections from liability for ISPs, web hosts, and other technological intermediaries for unlawful content transmitted over or hosted on their services by third parties (such as users).

It is vital to understand the reasons why intermediary liability protection is so important for free speech on the internet. When intermediaries are liable or responsible for the content created by others, they will strive to reduce their liability risk. In doing so, they are likely to overcompensate, blocking even lawful content. In this way, intermediary liability chills expression on-line and transforms technological intermediaries into content gatekeepers.

Indeed, holding intermediaries broadly liable for user content greatly chills their willingness or ability to host any content created by others. Liability creates strong incentives to screen user content before it is posted on-line, creating an indirect prior restraint on speech and inevitably leading to less user-generated content overall. In some instances, entire platforms for expression simply could not exist because the sheer volume of content would make it impossible or economically unviable for the company to screen all user-generated content. As one example, users post over 24 hours of video to YouTube every minute.²⁷ If liability concerns or an obligation to keep certain videos off of the service compelled YouTube to examine each video before allowing it to be posted on-line, YouTube could not continue to operate as an open forum for user expression. The same is true of the countless forums and blogs where users post hundreds or thousands of comments every hour.

Intermediary liability also creates another problematic incentive: Intermediaries will tend to over-block content and self-censor, especially where definitions of illegal content are vague and overbroad. In the face of threatened liability or policing responsibility, intermediaries will err on the side of caution in deciding what may be allowed. This incentive is especially strong (and can cause particular damage) when intermediaries are not able to easily determine if the content is unlawful on its face.²⁸

²⁶In appropriate cases and pursuant to lawful process, intermediaries do continue to be required to respond to law enforcement subpoenas concerning on-line speakers who post illegal content.

²⁷Ryan June, “Zoinks! 20 Hours of Video Uploaded Every Minute!”, Broadcasting Ourselves ;), May 20, 2009, <http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every-20.html>. Representatives of Google have recently stated that the current figure is 24 hours of video posted every minute.

²⁸For example, while a private party may allege that certain content is defamatory or infringes copyright, such determinations are usually made by judges and can involve factual inquiry and careful balancing of competing interests and factors. ISPs and on-line service providers are not well-positioned to make these types of determinations.

In 1996, to address these concerns, Congress took strong action to insulate on-line intermediaries from liability. As part of the Telecommunications Act of 1996, Congress enacted Section 230 of the Communications Act.²⁹ Now known simply as “Section 230,” the statute advances three policy goals: (1) To promote the continued rapid and innovative development of the internet and other interactive media; (2) to remove disincentives to voluntary self-screening of content by service providers; and (3) to promote the development of tools (like filters) that maximize user control over what information the user receives online.

To advance its first goal, Section 230 gives intermediaries³⁰ strong protection against liability for content created by third-party users.³¹ Section 230 has been used by interactive on-line services as a screen against a variety of claims, including negligence, fraud, defamation, violations of Federal civil rights laws, and violations of State criminal laws.³²

It is precisely these protections that led to the dramatic growth of social networking and other interactive, user-generated content sites that have become vibrant platforms for expression in the United States and all over the world. It is no surprise that almost all “Web 2.0” innovation on-line has taken place in the United States, which has the strongest protections for intermediaries. Without Section 230, entry barriers for new internet services and applications that allow user-generated content would be much higher, dampening the innovation we have seen in interactive media. The threat of liability would also tend to close the market to start-ups, which are often unable to afford expensive compliance staffs (thereby entrenching existing market players).

Protection for intermediaries has been a key foundation for the success of the internet. A decision to undo that foundation, and to seek to impose responsibility on online intermediaries for problematic content—including terror recruiting—would threaten the continued growth and innovation that has been the hallmark of the internet.

Terms of Service

The first operative part of Section 230—§ 230(c)(1)—provides strong and important protection to intermediaries, but the second part provides a different type of protection: protection from liability for a provider’s voluntary decision to remove content. Under § 230(c)(2)(a), intermediaries can block or take down content they believe is inappropriate, without fear of liability to the poster of the content.

This protection has encouraged all of the leading Web 2.0 sites and services to promulgate robust “terms of service” that specify types of content that are not permitted on the sites. Thus, for example, most leading social networks and video sharing sites have rules against sexually explicit material, and they routinely remove even legal content if it violates their terms of service. These self-regulatory efforts illustrate how a policy of protecting intermediaries from liability is compatible with—and can even help serve—other societal interests.

These terms of service will often prohibit terror recruiting content of the types discussed above. As one illustration, the terms of service from one leading video sharing site—YouTube.com—contain a number of prohibitions that could bar a video promoting terrorism:

- Graphic or gratuitous violence is not allowed. If your video shows someone being physically hurt, attacked, or humiliated, don’t post it.
- YouTube is not a shock site. Don’t post gross-out videos of accidents, dead bodies, or similar things intended to shock or disgust . . .
- We encourage free speech and defend everyone’s right to express unpopular points of view. But we don’t permit hate speech (speech which attacks or de-mans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity).

²⁹ 47 U.S.C. § 230. In addition to Section 230, Congress has also protected intermediaries through Section 512 of the Digital Millennium Copyright Act, 17 U.S.C. § 512, which protects intermediaries from liability so long as they afford copyright holders a means to have copyright violations taken down. Beyond the statutory bases for liability protection, there are strong arguments that the First Amendment would require such protection in at least some contexts.

³⁰ Section 230 calls these intermediaries “interactive computer services.” 47 U.S.C. § 230(c)(1).

³¹ The statute provides: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1).

³² See, for example, Center for Democracy & Technology, “CDT Joins Briefs Urging Courts to Properly Apply § 230 of the CDA,” Policy Post 14.4, March 31, 2008, <http://www.cdt.org/policy/cdt-joins-briefs-urging-courts-properly-apply-section-230-cda>. See also Electronic Frontier Foundation, “Section 230 Protections,” Bloggers’ Legal Guide, <http://www.eff.org/issues/bloggers/legal/liability/230>.

- Things like predatory behavior, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information, and inciting others to commit violent acts or to violate the Terms of Use are taken very seriously. Anyone caught doing these things may be permanently banned from YouTube.³³

YouTube has in the past taken down terrorist videos that violate its terms of service, and there is nothing to suggest that it and other leading on-line services will not do so in the future.³⁴

Although relying on voluntary enforcement of terms of service will not lead to the complete removal of terror recruiting content from the internet, it will make such content less available, and will do so in a manner that is consistent with both the First Amendment and the statutory regime of intermediary protection.

CONCLUSION

CDT would like to thank the subcommittee for holding this important hearing to consider both the problem of terror recruiting as well as the free speech implications of efforts to address the problem. We appreciate the opportunity to testify today and we look forward to working with the subcommittee on these issues.

Ms. HARMAN. Thank you very much.

Mr. Mudd.

STATEMENT OF JOHN PHILIP MUDD, SENIOR RESEARCH FELLOW, COUNTERTERRORISM STRATEGY INITIATIVE, NEW AMERICA FOUNDATION

Mr. MUDD. Madam Chair, Mr. Chairman, Ranking Member and others, I have to say at the outset I don't have any formal remarks. I would like to make a few comments. It is a real honor to be here. It is my first time to be here as a private citizen outside of 24 years in Government. There aren't a lot of rewards from the Government but to get a letter from the committee saying please come talk to us, you guys made my day. So thank you.

Ms. HARMAN. Not everyone would feel that way.

Mr. MUDD. I guess it ain't over yet. Right?

A couple of thoughts I guess from the outset.

First, we are not going to stop internet recruitment and radicalization. It ain't going to happen in the world of internet and the information age. So we can work on it, we can chip away at it, but it is not going to stop.

Second, we mistake this group in this country often as a terrorist group. I'm talking about al-Qaeda. It is not. It is a revolutionary organization. Revolutionary organizations can't win without an ideology that wins. In the 21st Century, that ideology is spread by the internet. So this is an important meeting because this is not a group whose end is to kill civilians by taking out airplanes and buildings. Its end is to recruit people who think and act as the organization wants them to think and act, even if these people never met an al-Qaeda member. So ideology is important. I wouldn't call them a terrorist group. I would call them a revolutionary organization.

Third, and the reason I think they are going to lose, they are not jihadists, they are not terrorists, and we are not talking about hate speech. They are murdering criminals. They hate to be called that.

³³ Excerpts from YouTube Community Guidelines, available at http://www.youtube.com/t/community_guidelines (last viewed May 24, 2010).

³⁴ Thomas Claburn, "Senator Lieberman Wants Terrorist Videos Removed From YouTube," *InformationWeek*, May 20, 2008, available at <http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=207801148> (last viewed May 24, 2010).

They should be called that. Khalid Sheikh Mohammed is not a terrorist. He murdered 3,000 people. So when I think about this issue, what I think about is showing the murder of an innocent, Nick Berg, on the internet. I don't think about a terrorist act. I don't care if jihadists and Yemen want to talk about jihad, that is fine. If you want to talk about murdering innocents, that is what I worry about. It is not about jihad, and it is not about terrorism. They are not terrorists. They are revolutionaries. Their revolution is about killing innocents.

So let me transition to a few thoughts.

As we deal with this, I think we have to watch the transition into terrorism, and in the paper Brian Jenkins wrote is really instructive. Now I remember sitting around the table with George Tenet in 2002 and watching the paramilitary campaign unfold at the nightly 5 o'clock meetings. I use the word "paramilitary" advisedly. It is a campaign on the ground in Afghanistan. Then we transition into one of the worst periods as I remember as a professional, 2003, watching the series of attacks in places like Saudi Arabia and Southeast Asia and saying, boy, we are in deep trouble. Attacks by people who are al-Qaeda affiliates or al-Qaeda members in places like, again, the heartland, Saudi Arabia and Indonesia. Fast forward to the last year 2009, 2010. The revolutionary movement has led to people in Dallas, Chicago, New York, Atlanta, Miami, and California. Most of the people involved in this activity are native-born Americans, are people who are American citizens born of foreign immigrants. They are not people—Zazi would be an exception, the Denver kid. They are people who took the message, may have some affiliation or connection with al-Qaeda, often they don't, but the revolution is spreading, and one of the ways it spreads is the internet. There is no question about that.

Let me close with a few thoughts on the practicalities of this and things I would think about if I were you. Three or four questions come up when you sit around the table and watch this stuff for 9 years.

First, what do you do with the service provider? Can you force him to say, you can't put that Nick Berg video up? I say Nick Berg because that is about as far as you can get down the road of a brutal showing of the murder of an innocent. I'm not talking about whether we're looking at websites where someone again talks about jihad, I'm talking about showing and glorifying the murder of a human being who has a soul.

So what do you do with service providers? Can you force them to take it out?

The second is what about people who upload that stuff? What do you do with them practically, not only in terms of legislation, but can we follow them and should we? I want to get back to that in just a second. I promise not to take too much time.

The third, obviously, is what to do with the websites. Can we just shut them off? I know there is a question about balance between operations and whether we learn from those websites and ideology. I can tell where I side, and hope you figure out where I am going. This is an ideological group and you might have short-term gains operationally, but in general I would say make sure they can't spread the ideology, because that is spreading the revolution.

One final thought, and then I will close. When you are talking about looking at people, one of the things you want to think about, I believe, is what I would call sort of the algorithm of intelligence. We are not just talking about a person in Texas or New Jersey who is looking at someone like al-Awlaki. The question I would have as a career analyst and someone who managed intelligence operations would be if you have someone who travels repeatedly to Pakistan, it is doing modeling, who travels repeatedly to Pakistan, who is under the age of 35, who traveled alone, who paid for his ticket with cash, and who is looking at al-Awlaki's website, I am asking how do you deal with the situation where you put that in the mix and you have seen that kind of activity not only in the United States but in Western Europe, do you think that is okay to look at someone? Because note in everything I said there is no predicate that says that individual did anything wrong. There is just modeling, as I learned in the past, that shows me there ain't no learn in the second kick of the mule. I have seen this happen before. People who look like that.

Okay, cautionary note as I close. If we are going to go down this road, and I'm not suggesting we do, I just want to be sort of, I have done this a long time, sort of offer you some suggestions. You are going to hit a lot of dry holes. So someone who says you should have, you could have found Hasan, I am going to say, okay, make sure you understand that 200 people who fit that same model are going to be pretty ticked off. So think about that. Think about when that story breaks, that we found Hasan, but 200 people who we also looked at because they had the same sort of modeling characteristics popped up.

The second thing I would say is think about the resources to do this. I'm sure Brian and Bruce can talk about this better than I can. You are not talking about a couple of people engaged in looking at these websites. Tens of thousands. So I don't represent the Bureau any more, but I want a free lunch from Director Mueller. If you want to do this, you are talking about asking analysts and agents to look at a funnel of tens of thousands of people, not only here, but partnering in visa waiver countries and then necking down that number and not only doing the analysis to do that but cutting hundreds of leads to the field to say divert yourself from white collar crime or public corruption or other terrorism investigations and go look at someone because we kind of sort of think he fits the model for activity.

So thanks for having me. It really is a pleasure to be here.
[The statement of Mr. Mudd follows:]

PREPARED STATEMENT OF JOHN PHILIP MUDD

MAY 26, 2010

We often consider al-Qaeda and its affiliates and followers as terrorists: Individuals who conduct attacks that down aircraft, destroy buildings, and murder innocents. Terrorism is a tactic, however, not an end. Al-Qaeda's end is ideological, an effort to spark a global revolution among like-minded who see as their first goal the ouster of the United States and its allies from Muslim lands and the overthrow of regimes viewed by al-Qaeda as corrupt. Messaging is central to this end, an end that entails reaching individuals who may never meet a formal al-Qaeda member. This is a campaign of ideas.

The internet is a brilliant tool for spreading ideology, and al-Qaeda uses the tool effectively. The conversation we have today will be far more about how to stop the spread of the ideology behind al-Qaeda—a long-term goal—than about how curbing internet-inspired violence can stop attacks in the near term. We are engaged in a long campaign against an idea, not a short war against a group. If we assume that this is an ideological battle, digital strikes may be as important as kinetic strikes. As one U.S. general has said, this battlefield is the battlefield of the mind. And the internet is proving, time and again, as a powerful tool to poison minds of those who then enter the battlefield.

There are balancing issues to deal with here. Is it worth attacking internet sites that can quickly morph? Can we use internet tracking to look for individuals who might commit acts of violence? How does the ideological benefit of blocking internet activity balance against operational interests in watching internet activity? And, of course, how much of what we see is legitimate free-speech activity?

We are concluding 9 years of post-9/11 operations. Noteworthy are two facts that should affect our conversation:

- First, most attacks post-9/11 have been conducted by al-Qaeda affiliates and like-minded individuals, not al-Qaeda members themselves. This is in stark contrast to the major attacks in East Africa in 1998; in Yemen in 2000; and in the United States in 2001. The message of venom has spread.
- Second, most individuals connected to al-Qaeda-inspired activity in this country are converts or native-born Muslims. We see very few plots linked to al-Qaeda recruits that fit the mold we might have expected when we accelerated this campaign 9 years ago. The message of venom has spread.

We can make great progress in the ideological campaign. Our adversary has clearly telegraphed their weaknesses: They fear that they are on ideological thin ice when they kill innocents, and we should talk about this. This is a long campaign, and we have many chapters to go. Historians may well write the next chapters, in years to come, with less focus on how many innocents died than on how many lives were saved as al-Qaeda's ideology crumbled under its own weight.

Ms. HARMAN. Thank you, Mr. Mudd. I think we will all agree that we all had a full spectrum of views on this panel.

It is now time for questions.

Again, thanks to the witnesses for very careful testimony, very thoughtful, very provocative, very informative testimony, I think probably the best we have seen in a series of hearings on this very difficult topic.

I want to put a proposition before you and just ask if you agree with me. I am yielding to myself for 5 minutes for questions, and then we will go to others.

I keep saying that security and liberty are not a zero sum game. You either get more of both or less of both. I also keep saying that the expression of radical views, even if we dislike them, are protected by our First Amendment in our Constitution, no matter how much we dislike them, and some of them are odious, I think we would all agree, and I could list some but we don't need to go there. But violent behavior is not protected by our Constitution. The hard piece is finding that line, that transition, between the expression of radical views and someone with radical beliefs, which are protected, who then becomes someone willing to engage in violent behavior.

So let me ask all of you just going down the road, and we will start with Dr. Hoffman, do you agree that there is no zero sum game if we are trying to live our values in this country? Do you agree that it is appropriate to try to find a way to intervene at that magic point where radical views become violent behavior?

Mr. HOFFMAN. Absolutely, Madam Chair. This is why I am such an outspoken supporter of your legislation that never passed, because I think we need an empirical foundation before we can attempt to do that.

I think, very clearly, our adversaries have communication strategy. As I said in my testimony, I think, lamentably, we don't; and that is what we need. Only based, I think, on a thorough understanding of the process, can we develop one. But I think the opposite reaction, which is to stick our head in the sands, in essence to say that we don't have a problem here, means that we are on a path to seeing, unfortunately, a successful event like Times Square or like the Northwest Airlines flight on Christmas day.

Ms. HARMAN. Thank you.

Mr. Jenkins.

Mr. JENKINS. I certainly don't see liberty and security as a zero sum game. I agree with you on that.

On the issue of radicalization versus action, that is the important distinction here. I think all of us have spoken about radicalization and recruitment to terrorism violence. That point is the real challenge. After 9/11, as a consequence of concern about terrorism, we have been pushing the authorities to move further upstream; that is, to intervene in a preventive fashion rather than to simply react in the traditional law enforcement mode. But, in that process, that is delicate, how far upstream we can push that. At what point does thought become action?

Ms. HARMAN. You nailed it, Mr. Jenkins.

Mr. Romero.

Mr. ROMERO. Well, of course, I very much agree with you, Chair, about the fact that safety and freedom do not have to be a zero sum game. But yet when we often talk about balancing safety and freedom, we are often taking about a Faustian bargain. It is an effort to give up some of the freedoms in the name of National security, and that is where I think we go wrong.

I think the question you posed to us about where you draw that line is actually quite easy to answer and rather well established. Go back to the Supreme Court, *Brandenburg v. Ohio*; very clear. The line between speech and ideas and conduct is very clear in that case. It applies. There it says, you can bar speech that is causing imminent lawless conduct. Imminent lawless conduct. If it is not imminent, it is protected. If it is not lawless, it is protected. If it is not conduct, it is protected. So mere advocacy of violence, as we saw on these videos, while loathsome and disgusting, are certainly protected by the First Amendment and certainly must remain a part of our body politic.

Ms. HARMAN. Thank you.

Let me just follow up with you for one second. So if someone goes on a bomb-making site on the internet—how to make a dirty bomb, how to make a nuclear bomb; pick one—should that person have an expectation of privacy because that person is exercising his free speech rights to surf the web, or should we perhaps decide that that person could be about to engage in imminent conduct and monitor him or her?

Mr. ROMERO. First, let's deal with the practicality of the reality. I think in the aftermath of September 11 we have given law enforcement intelligence officials enormous tools to use the internet and to surveil individuals. The PATRIOT Act, for instance, grants enormous latitude under National Security Letters to be able to intercept communications on the web. The amendments to the For-

eign Intelligence Surveillance Act have given enormous powers to our law enforcement officials—we often think too many powers—with insufficient judicial oversight.

The fact that one goes on a website to see how a bomb might be created, that alone should not be a reason to put a person under surveillance. What if I am a journalist writing a book on the Times Square bomber? I want to understand how he put it together. I want to give the most thorough analysis of what was going on, how he did it. I want to show the diagram of the car in my book. I want to be able to explain to the American public how easy it is to build a bomb. Should then I, as a journalist or an author, find myself on an FBI list? That is where we have to continue to look at the line between speech and conduct.

Ms. HARMAN. Thank you.

Mr. MORRIS.

Mr. MORRIS. Frankly, I am not sure I can add much beyond what Mr. Romero said. I certainly agree there is not a zero sum game for security and freedom, and I think we can achieve both. It is important that we work to achieve both.

As my testimony detailed—written testimony—and I think probably Mr. Romero's, I assume, and the Brandenburg case, there is another line of Supreme Court cases about true threats, whether a particular piece of speech is an actual direct threat of harm to someone. Those can be Constitutionally restricted. But the Supreme Court has made very clear that merely advocating the use of force is not by itself Constitutionally prohibitable.

Ms. HARMAN. Thank you.

Mr. MUDD.

Mr. MUDD. I think that is right. If someone wants to get on the web and talk about jihad, I think that is their right. If they want to talk about recruiting somebody to go to Afghanistan to fight, that is against the law and that is going to murder American soldiers. So, to me, I view it again as sort of a criminal issue, not as an ideological issue. Ideology is whatever you want to believe.

Second, I would again go back to the practical and talk about resources. Even if someone were to tell me—and I would be uncomfortable participating in this—if someone were to tell me, you need to go look at all jihadists, it is not practical in resource terms.

Last two thoughts, one technical. I think there is a big distinction between looking at people who are searching the web and looking at people who are engaged in chat rooms and talking in chat rooms that are publicly accessible, a big difference there. I am not a technical expert or legal expert, but, to my mind, those are fundamentally different activities.

Finally, I sort of want to throw you a curve ball, maybe. I think we in this country beat ourselves up a lot on ideology. The adversary, I believe—and I spent 9 years watching them—thinks we are doing better than they are, and they believe they are losing the war of ideology. I would argue if you look at Pew Research studies, they are, because they murder too many people.

Ms. HARMAN. Thank you very much.

The Chair now yields 5 minutes to the Ranking Member for questions.

Mr. MCCAUL. Thank you, Madam Chair. This has been an excellent discussion.

Mr. Romero, I thought you pointed out many cases where the Federal Government has overreached in its power and abused that power. We want to make that sure we never do that again. I think that is one of the points of having this hearing.

Mr. Mudd, you talked a lot about the spreading of ideology. I agree with you it is a revolution in their mindset. Some of these websites and some of what is available on the internet is really horrific stuff. You point out some of these executions, beheadings, whether it is in the jihad Islamic world or whether it is the drug cartels. It is all readily available. It is pretty bad stuff.

I think, Mr. Romero, you answered my first question; and that is, at what point is internet speech not protected? I think the cases have been fairly clear it is imminent lawless conduct. Of course, that is a judgment call in many cases on the part of law enforcement as to what is imminent lawless conduct.

I also think there is a difference, obviously, between censoring speech and monitoring speech on the internet. I wanted to expand on that.

For instance, listed on Islamic websites is a “must own,” and it is available on Amazon.com, the Preparatory Manual of Explosives, third edition. It is about 570 pages, 166 explosives, readily available, on how to build a bomb. It is a little concerning when you see the Islamic website saying this is a “must own,” go to this website, when we have had 15 terror plots in the last year alone. In many of these cases, they are looking at doing just this, building explosive devices.

So I guess what I want to throw out to the panel with the limited time I have, I think we have covered the censor issue fairly well in terms of the standard. But in terms of monitoring this, like in the case of Hasan, which I wish they had shared that information with Fort Hood. They may have been able to stop that. But that is an information-sharing issue. What can we do to monitor the activities on these websites?

Mr. Mudd.

Mr. MUDD. I was afraid that was coming.

I would go back to a point I made earlier and maybe make the conversation a little more complicated. I think just looking at people who buy books, practically speaking, it is not doable. But I would go back to say, okay, what if you have somebody who—or a series of criteria that says we have somebody who, again, has cash tickets to Pakistan, is under the age of 30. He has had multiple trips over 30 days. I say over 30 days because I want to look for people who probably have had some training. Go through whatever criteria you want. Then, wait a minute, now he is up on the web buying a book.

I don’t want to argue one way or another. I just want to tell you that is the practical question I probably would have if I were back in Government, not whether somebody buys a book but whether you think it is okay, representing the will of the people, to look at people who have a series of behaviors that almost anybody I think would say, freedom of speech aside, I would say that is kind of worrisome.

Mr. MCCAUL. Anybody else care to take that on?

Mr. ROMERO. Sure. I think that the line drawing is very much a difficult question, no doubt. I think it is made even more difficult because we have granted our law enforcement intelligence officials such sweeping powers that they are literally adding more hay onto the haystack, making it harder to find the couple of needles.

We need not look any further than some of the internal reports from the FBI itself, the Office of Inspector General, about the misuse and overbroad use of National security letters. We see that already. Frankly, that, I think, should have us think again about whether or not we have given too many surveillance powers that make the haystack all the larger, make finding the real individuals who have shown some conduct to be suspicious to be the actual targets of our investigations.

I think, to your point, I am very much heartened by your point that we can leave censorship aside. It is both the right thing and it is also a practical thing. Censorship never works. You try to shut down any website, it will pop up anywhere else across the globe. The internet is a global phenomenon, and the best thing we can do is assure its robustness in our country and make sure that we use it to the best of our abilities.

Mr. MCCAUL. Following up on that, is there any point where content is so inappropriate that it shouldn't be allowed on the internet or is it just—are we looking more at the conduct of individuals?

Mr. ROMERO. Well, the Supreme Court has also ruled on these issues. There is established law dealing with issues of pornography, dealing with issues of obscenity, that we don't need new rules or regulations on it.

What we perhaps do need perhaps is a fuller discussion, as my colleague Mr. Morris said, about how we work with these new forms of communications and make sure that they have proper guidelines for their users, make sure that they themselves understand the importance of their civic responsibility.

But the internet is our common forum. It is the new common grounds. It is the Boston Square. We want to keep that open and free. It is too essential to who we are now as Americans and as individuals in the 21st Century.

Mr. MCCAUL. I see my time has expired. Thank you.

Ms. HARMAN. I now yield 5 minutes to the Chairman of the full committee, Mr. Thompson of Mississippi.

Mr. THOMPSON. Thank you very much, Madam Chair. This is an absolute wonderful discussion.

Just to try to frame it a little broader, the House Un-American Activities Committee's hearing was held in this very room. So, from a historical analysis, somebody would say, wow, we are back here again.

So the public policy question I think for us is: How do we look at the internet in its present form and structure some guidelines or protocols that provide the intelligence community, law enforcement community, with tools necessary to identify situations that we deem harmful? The other public policy question is: Is it solely the burden of Government to do that, is it those sites themselves to help police it, or is there a public responsibility in some of this? If a member of the public got on a site and said, I think something

is wrong with this site, it looks like it is going somewhere, should we encourage them to report it to someone, or just what do we do?

I am kind of giving you three things to do, and I will back up. Dr. Hoffman, we can go down the line for comments.

Mr. HOFFMAN. Well, I may be horribly reductionist, but I think a lot of the reason we have this debate is—because I agree completely we shouldn't be censoring the internet. I am not even sure we should be monitoring it, either. I agree completely. But I think the problem is that we default toward these very intrusive approaches.

Because, for instance, unlike the United Kingdom, we don't have programs that seek to work with the community. We don't have a dedicated office anywhere in Government such as the Home Office in the United Kingdom has that works with local communities that attempts to identify processes of radicalization and recruitments and then interdict them on the ground—precisely as you say, sir—to enlist public support. We don't have a strategy like contest or an arm of it like the British do.

That is why I think it is so important to get our hands around what we do about the problem itself by enlisting the community and enlisting the public. Already, of course, it is not just the public. There are many private entities and NGOs that monitor the internet—SITE Intelligence Group, NEFA Foundation, the Investigative Project, and so on. So this is being done.

But the question is: How we can enlist the public and members of the community more to inoculate ourselves against this phenomenon without having any kind of approach or any strategy, without identifying anyone in the Federal Government to facilitate this process? I am not saying it is necessarily a Federal responsibility, either. I think a lot can be done by local and States' jurisdictions. But, in the absence of all that, we fall back on how we control the source of information. That I don't think is the issue.

Mr. THOMPSON. Mr. Jenkins.

Mr. JENKINS. Let me take a very pragmatic view here. Although this material on the internet is, as you pointed out, it is odious, it is offensive, it is troubling, it does assist in recruitment. On the other hand, the fact is it is producing very few active terrorists. The number of English language websites vastly exceeds the number of terrorists it has produced. So, as a marketing effort, it would be judged a failure.

Second, it is a source of intelligence.

Third, any type of shutdown would require an enforcement effort, a policing effort, that would end up in an on-line cat-and-mouse game that would simply divert valuable resources from investigative and intelligence functions. So we ought not create additional demands on our already-stretched resources, and so I would rather see us look at how we can devote those resources in a proper way to take advantage of the internet.

Let me give you just an interesting anecdote here. At jungle warfare school, there is an old sergeant that gives the same speech to every incoming class. He says, the jungle is not your enemy, not your friend. The jungle is neutral. Learn how to operate in the jungle. You can keep from getting hurt, and you occasionally turn it to your advantage.

The reality is that the new electronic jungle is what we are dealing with here. We are not going to make it go away. We are not going to be able to knock down the trees. We are going to have to figure out how to operate in it to keep from getting hurt and occasionally turn it to our advantage.

Mr. ROMERO. Chairman Thompson, first, I want to thank you for the history lesson about the history of this room. There were a number of ACLU board members and staff who were at this table those years ago. So it is delightful to be here in such a hospitable and much better climate than my organization was perhaps 40 years ago.

I think you raise exactly the right question, sir; and I think where we can look to some guidance is the newly completed and not fully released yet Senate Intelligence Committee report that tried to investigate about what went wrong with some of these investigations.

As far as we can tell from the redactions, they point out that they already did have individualized information on many of the individuals that were cited in your opening statement. There was a failure to share that information among relevant Federal agencies. There was a failure to communicate. There were mistakes made, misspellings of names that did not cross each other in databases.

That for me, sir, goes back to the question that perhaps the challenge is not that we lack certain surveillance powers that we need to fight the war on terror more effectively. Perhaps it means that we have too great surveillance powers which collect too much data, making the work of good law enforcement and FBI officials all the more difficult to cull through that volume. I think if we can narrow down the haystack, just to stick with my one metaphor, allow our officials to really comb through a much smaller haystack, they will be much more apt and able to really identify the individuals who might do us harm.

I think it is a place to have some discussions. I hear complaints from within the FBI itself that talk about the great volume. You remember Coleen Rowley, the FBI Director out of Minnesota, talking about the difficulty of all of these investigations that were initiated and that made the work of local law enforcement FBI officials all the more difficult. So perhaps we need to be talk about reining it in to make our law enforcement efforts more effective, not giving them more.

Mr. MORRIS. To address one of the questions you raised, Chairman Thompson, is all of the leading service providers that are really popular service providers in the United States, like YouTube or Facebook or really the whole gamut of Flickr for images and the like, they all have very prominently on the pages—on the video page—on every video page on YouTube is a “report abuse” button. Anyone who sees a video that is disturbed by the video or offended by it, they can click that button; and that immediately gets into a process where within a couple of hours a human will actually review the reported video.

So I do think that the leading sites are in fact allowing citizens to take action and to report things. None of these sites want to have content that is really—the videos of murders, I can’t imagine

any leading American site would want to have that on their server. So I think that is one way that citizens can interact.

But I would also just note, to echo something Mr. Romero said a few minutes ago, that trying to take this down, trying to really stomp it, will simply make it harder to monitor and harder to keep track of.

Fifteen years ago, there was a great concern about dial-a-porn in this country, sexy telephone calls. Parents were able to tell the telephone company, block all 900 numbers. So there was an easy solution. But Congress imposed more burdens on the dial-a-porn industry; and, in response, the dial-a-porn industry moved overseas. It made it so that it was much harder for parents to block access to the overseas dial-a-porn that kids still today could, in fact, access.

That is an example where, if you try to regulate speech too much, you will simply make it go somewhere else and it will still be available and in this context—in the terror recruiting context—it will be harder to monitor.

Mr. HOFFMAN. A couple of things I would think about, again, if you are going down the road of what to write and what to talk about. Let's say we are in a situation where we do takedown after takedown and 70 percent happen to be accessing a website hosted by a certain service provider. If I were the FBI Director or the Deputy, I would want to call that service provider and I would love for that service provider to have the protection to say I am not going to be sued if I take that down. So I don't know the technicalities of that, but that would not be an uncommon experience in the world I live in.

I am not referring to a phone call. I am referring to the fact a lot of these websites are everywhere. I don't know what latitude a service provider has when he gets that phone call to prevent himself from getting sued if he just randomly takes out a website.

Second, if you are a military commander—and we haven't talked about this, so I want to lay it on the table—in a place like Iraq, and you are dealing with an entity that is fighting U.S. soldiers and by the magic of electrons has a website hosted by a U.S. ISP, I would say that military commander ought to have the authority to take that out—and the latitude to do that.

Last, I might have gotten this wrong, but I must say I am not comfortable with the haystack analogy. The American people in some ways haven't asked for an FBI anymore, Federal Bureau of Investigation. They have asked for a Federal bureau that prevents events from happening. When we investigate or the Bureau investigates an event afterward, to the best investigators in the world, and that is not good enough.

Almost by definition I thought the 2005 reform legislation now is a part of that. Because I went over as the first deputy in the National Security Branch, the CIA person over to the FBI. I thought the intent behind the legislation was, darn it, you guys better do intelligence better so you collect enough to make sure bad stuff doesn't happen. We don't want to see another attack where you say, you know, if we had collected more, we could have prevented something.

The lessons you learn on the inside from things like Fort Hood and from Times Square are: Don't make a mistake. Don't make a mistake. Don't ever make a mistake. So some of the dialogue might be, what do you expect when you create a National security service, in essence, and what kind of dialog do we have with the American people, when almost unspoken their expectations have evolved to the point where they want a Federal service that prevents and not just investigates?

Mr. THOMPSON. Thank you very much. You have been very generous with the time.

Ms. HARMAN. Thank you, Mr. Chairman.

Consistent with committee rules, we are recognizing the other Member who was here before the gavel; and that is Mr. Carney of Pennsylvania. We will follow that with Mr. Dent of Pennsylvania.

Mr. CARNEY. I try to be punctual, ma'am.

I have got to tell you folks, I appreciate you being here. This, for me, is very exciting, because this is my syllabus for my class in terrorism I taught at Penn State, and you are all here now in the flesh. This is great.

I actually have a couple of questions. One deals with sort of a practical approach we haven't talked about in terms of what sorts of things incite recruitment.

Let's apply that toward the argument we are having today about: Should we try the terrorists in civilian court or military court? What do you think from your opinions is more inciteful to them, what gives them more impetus to want to join up, seeing a trial in a civilian court or having a more secretive military tribunal proceeding go on?

We can start down the line here. Dr. Hoffman.

Mr. HOFFMAN. Well, sir, you have posed an enormously difficult question, because one of the problems is we don't understand how terrorists radicalize and recruit individuals. I would say there isn't any one set profile or any one set pattern, and that is why it is very difficult to counter. I couldn't tell you whether seeing a trial in a civilian court or a military commission has more effect in terms of radicalization and recruitment.

What I can say is that certainly the trials by military commissions have become—and Guantanamo as well—have become a hot-button issue that is used on many of these sites constantly to inflame opinion. But, at the end of the day, is the war on terrorism going to end whether we try people one place or the other? Amongst our implacable enemies, it doesn't matter. They don't see civilian courts as any benefit. But I think as a recruitment tool, though, we do see them constantly going back to Guantanamo, to military commissions, and so on.

Mr. JENKINS. I think we make a distinction between those we may apprehend abroad and how we treat those and under the specific circumstances there. Although I think we can, within the realm of even military commissions, guarantee a fairness.

If we are talking about U.S. citizens, we are talking about people here in the United States, as I pointed out in my testimony, the criminal justice system is working. These have been successful arrests and successful convictions.

I believe—and this is a personal view—that there is a utility in stripping these individuals of any political pretensions. As I indicated in testimony before another committee in the Senate when I was asked about Major Hasan, as to whether he was a terrorist or not, I said he is a terrorist, but the important thing is we have him on 13 counts of murder, and that will be the basis for the trial.

So I think there is utility in removing all pretensions of political from this and bringing individuals before a jury of their peers and saying, you are not being prosecuted for your beliefs. Beliefs are personal business. When those beliefs—how one imposes those beliefs on others is a matter of community concern. When that imposition takes the form of criminal acts, it is a matter of the law.

So I think our ultimate defense against terrorist recruiting is the application of the law.

Mr. CARNEY. Thank you.

Mr. Romero.

Mr. ROMERO. I very much appreciate your question. I must say that I am delighted to be able to make this segue, because it is the other passion that I work on quite extensively.

I personally have spent about 25 days at Guantanamo. I have been there close to a dozen times observing the military commissions. Let me be quite clear. They are a debacle. They will never work. They have never worked. If we don't believe that that is not going to inflame further incitement against Americans, we are fooling ourselves. The laws that govern the military commissions are a joke, even under the new revisions. They allow hearsay evidence. They allow forms of coerced evidence.

The most recent military commission, it just happened last week where I had a colleague—I was away at another business trip and couldn't go—where we are trying to charge a 15-year-old boy who was videotaped crying, with his hands over his head, charging him as an adult; the one in which we just kicked out three reporters from the military commissions because we don't want them to be covering it all that well. Astonishing.

If we don't think that breaking those basic rules which are firmly established in criminal court is not helping inflame further anti-American interests, we are fooling ourselves. Unfortunately, the Obama administration has its head as much in the sand on this issue as its predecessor administration. It would do well for us to take up that issue in much greater length.

Mr. CARNEY. Mr. Morris.

Mr. MORRIS. I am not sure my organization has taken a formal position on that, but personally I could not agree more that, for someone in America, arrested in America, they should be tried in our criminal justice system. For us to move away from the values and the Constitutional protections that this country is built upon I think can only hurt our country and help the terrorists.

Mr. CARNEY. Thank you.

Mr. Mudd.

Mr. MUDD. I am not sure I am the right person to comment on the legal issues. Others have.

One clear point about ideology. This revolutionary opponent wants to be seen on a par with us. We are the head of the snake. We should never give them that courtesy. Jihad is an honor for

them, and they want to be terrorists. So my point would be, where they are tried is in somebody else's inbox. You and I both have a role in portraying who they are as they are tried. This is critically important. They are chump-change, murdering criminals. They murdered women and men who will never see their children, and those children will never have a proper family. They are criminals. So wherever they are tried, we should be careful as a Government not to give the adversary what they want.

The flip side, we have a great opportunity here. The adversary has told us what they don't want. They haven't signaled it. They have told us. They struggle to explain why they murder innocents.

I would encourage you to look at what the second in charge, Iman al Zawahiri, says in his only internet interview. First question out of the box, it is his choice to take this question, spring of 2008. It is a question from Algeria. How do you explain the murder of innocents? They can't explain it. Research data, polling data across the Middle East, Muslim lands, will show you when there is an attack in Muslim lands where Muslims die, people start to say, I don't like these guys.

Mr. CARNEY. Thank you all.

Ms. HARMAN. How about one more short question?

Mr. CARNEY. I guess this could all be a one-word answer for you all, but it is probably going to require more. Can al-Qaeda or the terrorists or the jihadists win a strategic victory through the internet?

Mr. JENKINS. No, they can't. Look, it is about building an army of believers. While they have spread their ideology to a certain degree, they are locked in their own little universe of discourse. What will happen in the long run, I am persuaded, is that the ideology will never be defeated thoroughly, but in fact this movement will become increasingly irrelevant. When we are up to the 250th message from Osama bin Laden or Adam Gadahn, what relevance is that going to have to a young man in the Middle East looking for a job or some kid in the United States on the internet? The message by itself is not going to enable them to achieve a strategic victory. It hasn't thus far.

Mr. Mudd was correct in pointing out they are complaining about the failure of their messages to get through. They are reaching out on this. So no strategic victory for them.

Ms. HARMAN. Does anyone disagree with that?

Mr. MUDD. No.

Mr. HOFFMAN. I wouldn't disagree, Madam Chair, but, at the same time, I think through the internet—in response to Representative Carney, no. But I think what our enemies have constantly said, they have never said they are going to defeat us militarily—has never said. He said they are going to wear us down.

What worries me is that as long as they are still able to replenish their ranks, as long as they are able to attract an increasingly more diverse set of recruits, even in the ones and twos—I think Mr. Mudd and Mr. Jenkins are absolutely right. As a mass movement, al-Qaeda will never succeed.

I am not even sure that is al-Qaeda's goal. It is a very unique type of organization. They are terrorists, and terrorists are small in number, and they seek to win disproportionate victories. I think

what they see is just eventually wearing us down. In that sense, it will be a strategic victory, but this is something that sustains them. Until we are more effective at choking off the supply of recruits, this war will continue to go on.

Mr. MUDD. Two quick comments.

I agree with the comments from Brian Jenkins. I would caution if we have another major event in this country we all have a responsibility to keep cool and move forward. Because they will be looking at that as forget about how many people died. That will be the tragedy. The tragedy will be their ability to exploit our reaction. The reaction will be more dangerous in some ways than the action. Because they will be looking for the next Ghraib.

I can tell you I talked to a lot of people who went to Iraq. I am talking about terrorists. That was a devastating—far more—it was devastating to this country. Forget about it in terms of what we had overseas.

So I guess my one asterisk is we are still a country struggling to manage how we respond to catastrophic incidents of terrorism. They would like nothing more than to have us overreact and give them some internet successes that would really resonate, I think.

Mr. ROMERO. If I may just pick up one quick thread from Mr. Mudd. While I completely agreed with his earlier points about how we have shifted our expectations in our society after 9/11, I think it is an enormous mistake to lead the American people down a path where we have them believe that we can prevent the next terrorist attack. To have a Federal Bureau of Prevention is just not feasible or possible. It will happen. The next attack will certainly happen. Our political leadership, I think, have shrugged the responsibility by not talking competently and clearly with the American people to prepare them for the inevitability of a terrorist attack.

Anyone living in Israel or Britain or France or in the Basque section of Spain, none of those residents believe that there won't ever be another car bombing or another terrorist attack. Yet we lull our Americans into thinking that we can fight the impossible. I think the more we can inoculate the American public on the inevitability of the next attack, the better off we will be to keep our heads cool when it does indeed occur.

Mr. CARNEY. Thank you.

Ms. HARMAN. Your 12 minutes have expired.

I can't resist, though, saying to Mr. Romero, we are not shrugging our responsibility. One of the things this subcommittee tries to do, and the historic occupant of this space, as has been pointed out by our Chairman, is to change that legacy and make it one where we are protecting our Constitution, living our values, but also protecting our country. That is a very tricky thing to get done.

I agree with you that there is no such thing as 100 percent security. I never promised that. But surely we can use the right tools consistent with our Constitution to make Americans as secure as we possibly can. That is an oath we take, to protect and defend the Constitution, but also to protect and defend the security of the United States.

Mr. Dent for 5-ish minutes, like everyone else.

Mr. DENT. Thank you, Madam Chair.

Anwar al-Awlaki has been identified by our intelligence agency, as many of you have pointed out in your testimony, as a direct source of radicalization to a number of recent terrorist events, even going back as far as 9/11. As you know, al-Awlaki is located in Yemen, but he communicates with individuals in the United States through the internet. Do we address on-line radicalization efforts and threats from overseas differently from how we address those domestic radicalization threats?

Go down the line starting with Dr. Hoffman.

Mr. HOFFMAN. We address them differently. Of course, we have the Voice of America, which is the main communications arm of the United States Government.

I think one of our failings is we don't have a strategy for countering radicalization overseas as well. If you look at, for instance, Voice of America, over 90 percent of its budget is dedicated to newspapers, radio, and television, traditional means of communication. That is what I read every day and listen to.

People my age, in their 50s, are not joining terrorist organizations; and that is why I put up those two videos. It is young people that they are trying to enlist; and it is young people who are motivated, who are animated, who are inspired by MTV-like presentations.

Yet this has been one of much frustrations. I think for a brief period of time when Under Secretary Glassman was at the Department of State we did have the beginnings of a strategy and an effective effort to reach out to this core demographics of terrorists, the youth. But it has fallen by the wayside, as near as I can tell. That, I think, is the problem.

Rather than talking about censoring or monitoring the internet, we should be doing a much better job and a much more effective job at using the same medium to counter these messages. Yet, at least from my perspective, we do extremely little. It is not prioritized, and it has not been resourced in this struggle.

Mr. DENT. Thank you.

Mr. Jenkins.

Mr. JENKINS. I would echo those comments.

I do think we have to make a distinction between what we do overseas and what we do domestically. Overseas, we certainly can and ought to engage in counterpropaganda activities. We had an elaborate effort to do this in past struggles. We have not had in the same attention, resources, strategy to do that this time. We simply don't have the instruments. We haven't thought it through. So we don't have what I refer to as a front-end strategy. We pound on operational capabilities, but we really haven't thought clearly how we try to break that cycle before it comes to operational capabilities.

Domestically, we are going to be more restricted, appropriately, in what we can do in terms of Government information programs. Moreover, I believe that counter-radicalization is best done at the local level. I think it is entirely appropriate at the Federal level to examine the ramifications of radicalization and recruitment to terrorist violence, to understand how that takes place to improve our comprehension of that process.

I would be wary of the Federal Government program to deal with a Muslim American community as I would be wary of a Federal Government program to deal with any other community. This is best done at the local level. It is done by the community itself. It is facilitated—

Mr. DENT. Like at the mosque level? When you said “at the local level”, who?

Mr. JENKINS. Not even at the mosque level.

What is interesting, what we do know about the recruiting process, it is not a result of profound religious discernment. This is not a religious conversion that is taking place. You have got a lot of young people, as Dr. Hoffman correctly points out, who are solving all sorts of personal issues and see all sorts of personal opportunities in this to cross that line. So it is not religious. It is done by the community. It is done by the families. This is going to be largely invisible. You have families intervening to keep sons and daughters from going down dangerous paths. You have interventions by very close acquaintances. That is something the authorities are not going to have the knowledge of.

What you do have at the local level, however, is a reaching out by the authorities, in many cases through the police, to develop that understanding of their local communities, to make those communities aware of what is taking place, that there is recruiting going on, Somalis or others, and to provide an open line for communications.

Now those local police, those local authorities, answer to locally elected officials; and I think that is a much safer place for that to take place.

Mr. ROMERO. I think, first, on the ability to intercept international communications to Americans here, or vice versa, we have granted that power already under the amendments to the Foreign Intelligence Surveillance Act. In fact, we think we have granted too great a power, where your communications, should you go on vacation to Mexico and then you e-mail your office or your wife, can be intercepted by law enforcement officials without the proper judicial oversight that we would otherwise see. So I think from the law enforcement perspective and the legal powers—

Mr. DENT. Go ahead.

Mr. ROMERO. More importantly, I think to your point about radicalization overseas, what perhaps is most—of greatest fodder is the continued racial profiling domestically. Because we look bad. When we pull a kid off an airplane because he has a shirt with Arabic script on it, or we pull another one—that is a client of ours in a lawsuit—or we have another kid pulled off of an airplane because he is studying Arabic flashcards, that becomes fodder for just how bad we are against Muslims.

So I encourage your committee, as you think about other committees and other hearings, that the extent to which very extensive racial profiling against Muslims and Arabs in America is continued only hurts the efforts you are endeavoring to do in homeland security in this committee.

Mr. MORRIS. To look at your question from a narrow angle of service providers, the source of a video posted to YouTube ultimately is irrelevant. If it comes from overseas or if it comes from

a domestic service, if it violates YouTube's terms of service, they will take it down. So on that angle there is probably not a distinction for American-hosted service providers.

Actually, to answer something that Mr. Mudd raised, those service providers in fact do have statutory protection if they choose to take something down because it is offensive or violates their terms of service.

Mr. MUDD. Just on that really narrow operational question, if you sit at the FBI sort of executive table and the CIA executive table on counterterrorism operations, the way the services operate looking at terrorists through the internet, there is no comparison, fundamentally different. Anybody who thinks we have to have a domestic intelligence service, it is not correct. It is not a good forum to talk about that. But just—the foreign intelligence service focuses on knowledge and doesn't spend a lot of time saying, what is the law in Timbuktu for whether I can get somebody's hard drive? A domestic service says, what is right to do? Then how do I provide security, given what is right and lawful to do? Very different ways of attacking problems.

Just quickly, I am not a big believer in influence campaigns. They are hard to run, especially in a democratic society. We leak a lot. We are operating in an environment where, first, we don't have any legitimacy; and, second, these guys are destroying themselves already through blood and mayhem of 9 years.

2003 in Saudi Arabia, killed too many people.

Zarkawi had been something of a hero in Jordan. Suicide bombers at wedding in Jordan in 2005. Instantly, people say, what are we up for here? I mean, they sure don't like America, but they sure don't understand when people come in and kill their own.

Same thing happened in Iraq. We talk about the surge, which was significant. But we had the internal communications, which are now public, of al-Qaeda talking to Zarkawi saying, don't kill all those civilians. We have been down this road. He killed too many civilians, and the Awakening Council said, we're done with these foreigners. We're going to kill them.

The last thing I would say, if you want to read people who do this from a liberal society, Western society, you can get on the web at Contest Strategy—that is the formal name for it, Contest—from the British Home Office. Section 9 explicitly talks about the counter-radicalization campaign from the Home Office. You probably would be surprised of how open they talk about going against what we probably would characterize as domestic free speech. It is a great read, and the people who run that program are a serious talent.

Mr. DENT. Can I just ask one quick question to Mr. Jenkins?

You stated in your testimony, Mr. Jenkins, that the majority of the 131 U.S. homegrown terrorists identified by Iran are native-born or naturalized U.S. citizens or illegal permanent residents. Do you have any further breakdowns on these numbers by category?

Mr. JENKINS. I do have a report which has a breakdown of those for whom we have complete information on. Only a handful—by the way, there are two or three that were illegal in the sense that they had overstayed a visa or have entered the country illegally.

The breakdown between native-born and naturalized?

Mr. DENT. Naturalized, correct.

Mr. JENKINS. It is in a report, and I don't have it at the tip of my tongue.

Mr. DENT. Native-born, naturalized, and legal permanent resident. If you could get that to us after the hearing.

Mr. DENT. I am way over my time, so I yield back.

Ms. HARMAN. Thank you, Mr. Dent.

Thank you to an amazing panel.

We have had a number of hearings on this issue, just to point out for the record. Our last one was on community outreach. We are very sensitive to the issue of racial profiling. We are very sensitive to the issue of anti-Muslim or anti-Arab rhetoric.

I joked the last time—it is not really a joke—but that Jihad Jane was blond, with blue eyes, and that we should think about people in the future—and Mr. Dent's constituent; let's have it out here—from a variety of backgrounds with a variety of views—I know Mr. Jenkins strongly agrees with this—who will turn to violent extremism.

The issue for this hearing is, what role does the internet play in all this? I think we had quite a full discussion of what role it plays and what role it doesn't play and what the dangers are of getting involved in censorship on the internet. I was listening, and I actually agree.

On the other hand, I want us to be as creative as possible in trying to get ahead of this problem and trying to—perhaps you are right, Mr. Romero—reduce the haystack but to find a way consistent with our values and our Constitution to use the right law enforcement tools and intelligence tools to identify that small number of people who would really be capable of and intend to do us harm.

That is the challenge. I fear that if we don't work on this, and we do have another major attack, the victims—in addition to innocent civilians who will be murdered, the other victim will be our Constitution. So it is extremely important to work carefully ahead of the next problem to reinforce both security and liberty.

That is where my head is. That is what I think we should be doing. I think that that will overturn the legacy of this particular room, where the occupants around this table, or at least the Chairman of the committee, had a very different vision.

So I thank you for appearing. Please continue to help us. We need you, all of you; and we are going to call on you regularly, as we already do.

Finally, I think that the way we win this challenge against us is to win the argument; and the way we win the argument is to live our values.

The subcommittee hearing stands adjourned.

[Whereupon, at 11:52 a.m., the subcommittee was adjourned.]

