Statement of Anthony D. Romero
Executive Director
American Civil Liberties Union

On

“Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?”

Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

House Committee on Homeland Security

May 26, 2010
Good morning Chairwoman 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 fifty-three affiliates nationwide. 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 online 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

Without doubt, the rise of communications technologies presents challenges to those interested in preserving traditional civil liberties standards. Nearly fifty 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

---

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).
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 \textit{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.\textsuperscript{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 online 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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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:

\textsuperscript{3} \textit{U.S. v. Robel}, 389 U.S. 258, 264 (1967).
\textsuperscript{4} U.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.”
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 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

---

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.”
forms. 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”.

Some have argued that the online 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.

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.

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. 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.

---

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 an 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.
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 U. S. 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 US, 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 ten to twenty 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

---

\(^{18}\) An 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](http://avalon.law.yale.edu/18th_century/sedact.asp)).

\(^{19}\) An Act to Regulate the Immigration of Aliens into the United States, ch. 1012, 32 Stat. 1222.


terrorists or other criminal activity. Rather, its claimed success was in “wrecking the communist parties in this country” and shutting down “the radical press.”

- **State investigations.** The New York State Legislature initiated a two-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 arrested, 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

---

22 Id. at 387.
25 18 USC § 2385. See also Stone, Perilous Times.
27 CHURCH REPORT, at 7.
the event of a national emergency.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{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 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.\textsuperscript{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.\textsuperscript{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

\textsuperscript{28} Id., at 6-7.
\textsuperscript{29} Id., at 5.
\textsuperscript{31} 50 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.
\textsuperscript{33} See 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.
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 11th 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 online 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 counterproductive. 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

34 United States Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff
report noted, for instance, that “For those who want to know more about violent Islamist ideology, immense caches
of information and propaganda are available online,” 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.
35 Letter from Senator Joseph Lieberman to Dr. Eric Schmidt, Chairman of the Board and Chief Executive Officer,
36 Statement 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:
the Internet. But such a conclusion would not be unique to the Internet. “Each medium of expression … may present its own problems.” 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.

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.

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. Indeed, the “widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public.” 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.

Courts also understand that “the Internet represents a brave new world of free speech.” 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.” 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.” Congress further declared that it is the policy of the United States “to encourage the development of technologies which maximize user control over

37 Universal City Studios, Inc. v. Corley, 273 F.3d 429, 433 (2d Cir. 2001).
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).
45 Id.
Congress therefore immunized Internet providers and users from any liability for publishing “any information provided by another information content provider.”

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 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.

---