1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **John B. Morris, Jr.**
General Counsel

Center for Democracy & Technology

before the House Committee on Homeland Security,
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

FREE SPEECH AND ONLINE INTERMEDIARIES IN AN AGE OF TERROR RECRUITMENT

May 26, 2010

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 online terror recruiting are difficult ones, made challenging by the constitutional and statutory implications of any governmental attempts to regulate online 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 online 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 online terror recruitment, including (among others) seeking to directly prohibit speakers from posting such content and seeking to require online 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 online speech. The testimony then focuses on one possible response – seeking to make online websites and services responsible for policing user content for online terror recruitment activities, or otherwise be held liable for such content.

---

[1] The 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, D.C., and San Francisco.

This possible response is one part of a larger question of whether online "intermediaries" should be liable or responsible for content posted by their users. The term "online intermediary" encompasses conduits (such as ISPs) and platforms (such as social networks and video sharing sites) that allow users to access online 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 online. This intermediary liability protection has been extraordinarily successful and is directly responsible for the explosive and innovative growth of online services that we have experienced over the past decades. By protecting online 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 online.

A decision by Congress to step back from such protections and to impose obligations on service providers to police online content – even in the effort to fight terrorism – would have serious and harmful implications both for free speech online and for innovation and competition in online services. We urge this Subcommittee to exercise great caution as it considers what steps would be appropriate to respond to online 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 online could be counterproductive to the fight against terrorism. Online content gives insight into terrorist groups' intentions and methods. In a range of contexts, online 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 online 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.

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

Online 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:

---

[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.

> [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 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 Web site 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 web site owner removed the film from the Internet, but later restored it and the federal officials took no further action. In the damages action, the

---

[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).

[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).

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 antiabortion web site. 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 web site 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 case involving the "Pentagon Papers," even a strongly asserted claim of national security may not overcome the presumption against prior restraints.[19]

---

[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).

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

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 online 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 web site 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.

---

[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.

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

Internet service providers (ISPs), websites, online 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 online 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 online 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 online environment: Specifically, should technological intermediaries such as ISPs and online 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 online 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

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

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 online 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 online, 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 twenty-fours 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 online, 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]

In 1996, to address these concerns, Congress took strong action to insulate online 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

---

[27] Ryan Junee, "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.

[28] For 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 online service providers are not well-positioned to make these types of determinations.

[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.

development of tools (like filters) that maximize user control over what information the user receives online.

To advance its first goal, Section 230 gives intermediaries[30] strong protection against liability for content created by third party users.[31] Section 230 has been used by interactive online 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 U.S. and all over the world. It is no surprise that almost all "Web 2.0" innovation online has taken place in the U.S., 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.

---

[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.

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 demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity).
- 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 online 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.

For more information, contact John Morris, jmorris@cdt.org, Greg Nojeim, gnojeim@cdt.org, or Jim Dempsey, jdempsey@cdt.org, or at (202) 637-9800.

---

[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).