Brandenburg's Imminent Obsolescence

Fall 2013

Olivia Bruner

November 11, 2013

Submitted to Dr. Wilfred Tremblay

In Partial Fulfillment for the Requirements of

COM 3390 Communication Law

> *It was a confluence of magnificent proportions, writes Michele Catalano in her blog entry "Pressure cookers, backpacks and quinoa, Oh my!" (Catalano, 2013). It all seemed innocent enough: Catalano was surfing the net for pressure cookers; at the same time, her husband was Googling backpacks. But on July 31, 2013, six members of the "joint terrorism task force" knocked on the Catalanos' front door to see if they were terrorists. Which begs the question: How did the government know what they were Googling? (Bump, 2013).*

Forty-four years ago the United States Supreme Court established a new incitement standard, *Brandenburg*, which is still in effect today. The doctrine, which germinated from the 1969 Supreme Court case *Brandenburg v. Ohio*, draws a clear distinction between advocating violence and incitement of illegal activity, when speech no longer warrants First Amendment protection (395 U.S. 444, 1969). Replacing the rather ambiguous clear and present danger test that had been in effect since 1919, *Brandenburg* places a premium on immediacy. Under the *Brandenburg* standard, the government cannot punish advocacy of an idea unless the speech intentionally and likely will result in "imminent" illegal behavior (395 U.S. 444, 1969). *Brandenburg* includes three requirements: (1) expressly advocating felonious behavior, (2) advocacy must call for immediate violation of the law, and (3) the act must be imminent and likely to occur. "With its new 'magic words': 'incitement to imminent lawless action,'" the *Brandenburg* doctrine "reset the boundary line of permissible censorship" (Montgomery, 2009, p. 156). Yet in the forty-four years since its inception, the Supreme Court has seldom referenced *Brandenburg* in its decisions (Miniter, 2008, p. 14). As the episode above illustrates, the

Brandenburg doctrine is becoming obsolete; in response, the federal government is resorting to surreptitious counter-terrorism measures.

With the advent of the Internet came the elimination of the traditional media gatekeeper. People, from Singapore to Santa Monica, can now directly communicate with one another in a "new speaker-audience relationship not contemplated by the Court that fashioned *Brandenburg*" (Montgomery, 2009, p. 163). But the same features that imbue the World Wide Web with the potential of being an open and robust forum have also expanded Jihadist terrorists' possibilities for communication. Terrorists now have increased access to receptive audiences; Jihadist terrorist groups are defter, more coordinated and skilled – capable of operating like freelance journalists and cyber organizations.

Terrorists' use of the Internet to disseminate propaganda introduces a new dimension of asymmetrical conflicts. Although there is no commonly held academic definition of asymmetrical conflict, Dr. Carsten Bockstette, an Officer at the European Center for Security Studies in Germany, provides a thorough explanation. In his words, asymmetrical conflicts are "conflicts between parties that show essential quantitative and/or qualitative dissimilarities in the battle space dimensions…usually waged in a changing, asynchronous and unpredictable manner" (Bockstette, 2008, p. 8). Bockstette maintains that the purpose of terrorism is to strategically manipulate the media in order to attain the maximum amount of publicity. Combining with the World Wide Web has enabled terrorism to reach a global audience. And with the Internet, the process of radicalization happens "more quickly, more widely, and more anonymously… raising the likelihood of surprise attacks by unknown groups whose members and supporters may be

difficult to pinpoint" (Mazzetti, 2006). Perhaps ironically, democracies offer terrorism the ideal basic conditions.

The same freedoms that build democracies enable terrorists to thrive, as does a pest in a parasitic relationship. Terrorists exploit democracy's uncensored media outlet in three main ways: for recruitment and education, fundraising, and planning operations and future attacks. As an unrestricted medium, the Internet of democratic societies contains information regardless of its veracity or the severity of its impact. Terrorists thus commonly overstate their significance and spread false information; in attempt to bolster their image, they discredit the Western Hemisphere's efforts to stabilize the Middle East. Indeed, "most Islamic terrorist Web sites focus their propaganda on making themselves look like persecuted and victimized underdogs, who have no choice but to turn to violence" (Healy, 2009, p. 170). Yet in the twelve years since the September 11, 2001 terrorist attacks, the number of terrorist prosecutions has drastically declined.

On the other hand, over the past decade, "the FBI and other federal agencies have referred more terrorism cases to the Justice department than ever before" (Miniter, 2008, p. 5). Some would argue that this anomaly is because terrorists are turning the U.S. legal system into a weapon that can be used against the American judiciary. In reality, district attorneys have cited three weaknesses of post-September 11 cases that explain why cases against terrorism were more likely to be won in the decade prior to the 2001 attacks than they are now. With the trend in terrorism being online communication, cases brought against alleged terrorists generally lack victims, possess insufficient compelling physical evidence and run into strong arguments that the suspect was simply exercising his First Amendment rights (Miniter, 2008, p. 9). Given these

realities, the federal government's motives for bypassing *Brandenburg* and instituting their own terrorism-suppressing tactics are understandable.

The Supreme Court's route to *Brandenburg* was both dogged and difficult. "In many cases, decided during or in the aftermath of World War I, the Court struggled to find the proper balance between the governmental interest in free speech" (Weaver, 2011, p. 4). In order to understand the development of law that led to the *Brandenburg* doctrine, an examination of pre-*Brandenburg* jurisprudence is essential. As aforementioned, *Brandenburg* replaced the clear and present danger test, which resulted from the landmark Supreme Court case, *Schenck v. United States* (249 U.S. 47, 1919). Schenck, a member of the United States Socialist Party, was convicted of attempting to violate the 1917 Espionage Act for ordering 15,000 leaflets condemning the U.S. war effort to be printed and circulated. Writing for the Court, Justice Holmes introduced the clear and present danger doctrine: "The question in every case is whether the words used are used in such circumstance and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent" (249 U.S. 47, 1919, p. 52). The fact that the United States was entrenched in World War I at the time was crucial to Justice Holmes.

Less than ten months after clear and present danger's inception, the doctrine was refined to include imminence and intent with the ruling of *Abrams v. United States* (250 U.S. 616, 1919). In 1918, five Russian-born immigrants were, like Schenck, convicted under the Espionage Act. The five defendants printed and distributed 5,000 flyers cheering on the Russian revolution and criticizing President Wilson, the United States, and its allies. While he stood by his decision in *Schenck*, Justice Holmes broke from the majority in the *Abrams* case with his dissenting opinion.

Holmes found that in *Abrams* "the defendants did not have the intent required by the Act to 'cripple or hinder the United States in the prosecution of the war.' There was nothing in the language of the leaflets, Holmes argued, that showed the men were specifically aiming to disrupt the war effort" (Montgomery, 2009, p. 8). Moreover, Holmes cited the First Amendment's declaration that "Congress shall make no law… abridging the freedom of speech" (U.S. Const. amend. I) which led to his marketplace metaphor rationale for the "free trade in ideas" and protection of speech (250 U.S. 616, 1919, p. 630). By incorporating the elements of imminence and intent into the clear and present danger doctrine, and advocating the marketplace metaphor for speech, Holmes' opinion in *Abrams* "had enormous influence on the development of the incitement standard eventually adopted by the Court in *Brandenburg*" (Montgomery, 2009, p. 8). Six years following the *Abrams* ruling, Justice Holmes was again in dissent in the case of *Gitlow v. New York*.

In 1925, Benjamin Gitlow, a New Yorker, was convicted of violating the state's criminal anarchy statue by inciting anti-government activity. The anti-war manifesto he was found guilty of distributing "advocate[d] and urge[d] in fervent language mass action [that would]… destroy organized parliamentary government," according to Justice Sanford, who wrote for the Court, and was therefore was dangerous enough for the government to forbid it (268 U.S. 652, 1925, p. 665). But Justice Holmes, in his dissent, asserted that "if the Court applied his conception of the clear and present danger test in this case, 'it is manifest that there was no present danger of an attempt to overthrow the government by force on the part of the admittedly small minority who shared the defendant's views'" (Montgomery, 2009). Moreover, Holmes proclaimed, "Every idea is an incitement… The only difference between the expression of an opinion and an

incitement in the narrower sense is the speaker's enthusiasm for the result" (268 U.S. 652, 1925 p. 673). Holmes argued that only when speech directly inspired immediate and concrete action, at an explicit time, could the government intervene. Since the Gitlow manifesto only *advocated* a violent government takeover, Holmes contended, it did not pose a clear and present danger validating government interference.

Nearly two decades later, the Supreme Court's 9-0 ruling in *Chaplinsky v. New Hampshire* asserted, "[some] utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest" (315 U.S. 568, 1942, p. 572). Those who defend *Brandenburg* argue that it is essential to the protection of free speech, but in reality, pinpointing whether speech warrants its protection proves to be imprecise. The advocacy of terrorism arguably fits the sort of speech lacking social value that the *Chaplinsky* ruling describes.

The final decision that paved the way for the *Brandenburg* doctrine was *Noto v. United States*. Through its ruling, the Supreme Court revised the way states could prosecute citizens for advocating governmental coups, making it more difficult for them to do so. Furthermore, the *Noto* decision, which decreed: "the mere abstract teaching… of the mortal property or even the 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," tipped the judicial scale balancing free speech and public safety in the favor of free speech (367 U.S. 290, 1961, p. 297). This distinction would prove exceedingly tedious to define in actual practice.

Fast-forward thirty years to post-*Brandenburg* decisions and the Internet age. In 1997, the Supreme Court made its first major ruling on the regulation of Internet-circulated materials

with the case *Reno v. American Civil Liberties Union* (251 U.S. 844, 1997). With the Internet, the power of modern-day Shenck or Abrams to communicate with potential followers has expanded exponentially. Justice Stevens, writing for the Court in *Reno*, asserted that because the Internet houses "vast democratic forums" it is entitled to the highest level of First Amendment protection (251 U.S. 844, 1997, p. 868). Because of the Internet's resulting entitlement to extraordinary Constitutional protection, and the reality that it is often unclear if Internet publications are *actually likely* to incite imminent lawless behavior, it is little wonder *Brandenburg* hardly succeeds at prosecuting the modern day Schenck.

Case in point: United States v. Al-Hussayen (2003). In 2003, Sami Omar Al-Hussayen, a graduate student in computer science at the University of Idaho, was arrested and indicted by federal prosecutors for operating websites that advocated terrorism. The Al-Hussayen case represents "the first time that the government attempted to use the [material support to terrorism statutes] to prosecute conduct that consisted almost exclusively of operating and maintaining websites" (Williams, 2007, p. 2). But because Al-Hussayen's Internet activities did not satisfy *Brandenburg*'s imminence requirement, and the prosecution failed to convince the jury that Al-Hussayen's websites contained material support to terrorism, he was acquitted of the federal terrorism charges. Although the case succeeded in chilling Al-Hussayen's speech, from a legal viewpoint, it was a substantial defeat; the case demonstrates the difficulty of legitimately convicting online speakers.

Just as the nation's involvement in world wars influenced the handling of the *Schenck* and *Abrams* proceedings, America's current "War on Terror" is swaying judicial decisions and the actions of federal administrators. "As part of an effort to preempt terrorist activity, federal

prosecutors have broadly and 'creatively' interpreted the scope of two material support to terrorism statues [18 U.S.C. §§ 239A, 239B (2000).] in order to interdict suspected terrorists and their supporters before they have a chance to actually carry out their acts of violence" (Williams, 2007, p. 2). The federal government's response to the *Brandenburg* doctrine's unfruitfulness? Censorship by proxy.

Instead of confronting speakers directly, the federal government is soliciting private intermediaries as proxy censors to monitor the exchange of information. Internet Service Providers (ISPs) are being pressured by the federal government to screen online speech for potentially unlawful activity. ISPs are handed the power to directly investigate and terminate suspicious, illicit activity or report the issue to the appropriate governmental law enforcement agency. ISPs can disclose a range of subscriber information, including, but not limited to, names, addresses, billing histories, and records of session times and duration. The federal government "is increasingly recruiting companies, including ISPs, to serve its national security interests, resulting in a so-called 'Invisible Handshake' between the public and private sectors" (Montgomery, 2009, p. 25). It is both cheaper and simpler for ISPs to be tasked with monitoring online activity than for the government to attempt to do so itself. Hence, the *Brandenburg* doctrine is at risk; it is increasingly being superseded because of how difficult it makes securing prosecutions for subversive speech.

The federal government employs two main tactics in pressuring ISPs to control users' speech: professed "good corporate citizen" programs and the use of National Security Letters (NSLs). In 2002, the Electronic Communications Privacy Act of 1986 was revised and renamed the Cyber Security Enhancement Act (6 USC § 145), the provisions of which make it easier for

ISPs to voluntarily–through "good faith"–report questionable material to the government. "The 2002 amendments significantly reduced the requirements to reveal such information–changing the condition on providers' actions from one of "reasonableness" to one of "good faith" and omitting the condition that the emergency be immediate" (Montgomery, 2009, p. 36). The government is thus blatantly disregarding *Brandenburg* by not requiring harm to be immediate.

Through the issuance of National Security Letters (NSLs), the federal government can further pressure ISPs to comply with FBI requests "for subscriber information and toll billing records information, or electronic communication transactional records in [their] custody or possession" (Montgomery, 2009, p. 41). Initially, FBI agents were only given permission to target consumer information if doing so pertained to a legitimate investigation. A report conducted by the U.S. Department of Justice's Office of the Inspector General in 2007, however, exposed widespread corruption in the FBI's issuance of NSLs. According to the report, the use of NSLs after the September 2001 terrorist attacks increased drastically, from 8,500 in 2000 to 39,000 in 2003… and 47,000 in 2005 (Montgomery, 2009, p. 41). But just because the FBI issues an NSL does not mean that an investigation is valid. The causes of the increase, according to the report, are three-fold, and all are associated with the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) (115 Stat. 272, 2001).

First, rather than require the "information sought by the FBI through an NSL be connected to a 'foreign power or agent of a foreign power,'" the Patriot Act only insists relevance "to an authorized national security investigation" (Montgomery, 2009, p. 41). Second, the Patriot Act makes it so high-ranking FBI officials no longer have to approve the issuance of

NSLs; low-level FBI officials can now sign off on their use. Third, since 2003, NSLs have been given the right of issuance during preliminary investigations instead of full investigations only. As NSL use surges, the FBI's recordkeeping system fails to keep up; its issuing and tracking integrity is waning, and the Bureau frequently receives unauthorized consumer information.

Supporters of the Patriot Act assert that the law has been essential to preventing another terrorist attack of the likes of September 11, 2001. Because the legislation provides law enforcement access to private information (including emails, online search histories, and bank statements) without having to notify individuals, those in favor of the Patriot Act claim that it decreases terrorists' ability to function in America. Furthermore, the pro-Patriot Act crowd highlights that with the legislation communication between governmental agencies (the FBI and CIA) and private intermediaries has streamlined, allowing them to work together in an unprecedentedly efficient manner to prevent criminal activity or acts of terrorism ("The Patriot Act," n.d.). Ultimately, advocates of the Patriot Act believe that the concessions made on public privacy are justified; the limitations, they maintain, are a small sacrifice for increased protection of the American people.

Yet, rhetoric that is clearly protected under the *Brandenburg* doctrine is ever more endangered by the government's intense preoccupation with terrorism-related content online, and its persistent pressure on ISPs. The most evident ramifications of *Brandenburg*'s increasing obsolescence include the federal government's invasion into personal privacy via ISPs and its subsequent chilling effect on speech. When intermediates–ISPs–are burdened with policing citizens' Internet search history, subjective judgments about intent are inevitably made. Just refer to the opening anecdote: the fateful pressure cooker and backpack incident. Because ISPs

are prohibited from disclosing whose information they share with the government, speech is patently inhibited. With the current censorship by proxy-centric legislation, "the likelihood that ISPs will target constitutionally protected speech and invade user privacy to avoid any possibility of government sanction" increases (Montgomery, 2009, p. 48). And while the majority of the government's relations with ISPs occurs out of the public eye, whatever incriminating evidence that does surface is quickly suppressed–simply consider the fate of National Security Agency whistle-blower Edward Snowden.

Federal officials are taking counter-terrorism tactics into their own hands, pursuing what they cannot get directly (the admissible prosecution of a speaker who advocates terrorism without violating *Brandenburg*) by compelling Internet intermediaries to hand over users' private information. Wartime anxiety steered judicial decisions leading to the *Brandenburg* doctrine, and it is impelling the government now. The nation's War on Terror–induced paranoia directly instigates censorship by proxy, which chills speech and encroaches on the public's privacy. Given the way the government is manipulating its administration, it is possible that *Brandenburg*'s obsolescence is not only imminent but a reality already.

References

Abrams v. United States, 250 U.S. 616 (1919). (Lexis/Nexis, http://www.lexis.com/).

Bockstette, C. (2008). Jihadist terrorist use of strategic communication management Techniques. *European Center for Security Studies*, 28.

Brandenburg v. Ohio, 395 U.S. 444 (1969). (Lexis/Nexis, http://www.lexis.com/).

Bump, P. (2013). Google pressure cookers and backpacks, get a visit from the feds. *Yahoo News*. Retrieved September 17, 2013, from http://news.yahoo.com/google-pressure-cookers-backpacks-visit-feds-140900667.html

Catalano, M. (2013, August 2). pressure cookers, backpacks and quinoa, oh my! *Medium*. Retrieved September 17, 2013, from https://medium.com/something-like-falling/2e7d13e54724

Chaplinsky v. New Hampshire, 315 U.S. 568 (1942). (Lexis/Nexis, http://www.lexis.com/).

Cyber Security Enhancement Act of 2002, 6 USC § 145 (2002). (Lexis/Nexis, http://www.lexis.com/).

Gitlow v. New York, 268 U.S. 652 (1925). (Lexis/Nexis, http://www.lexis.com/).

Healy, M.H.. (2009). How the legal regimes of the European Union and the United States approach Islamic terrorist web sites: a comparative analysis. *Tulane Law Review*, *84*(1), 165–194.

Kreimer, S. (2006). Censorship by proxy. *Scholarship at Penn Law*, 91.

Material Support to Terrorism Statutes, 18 U.S.C. §§ 239A, 239B (2000). (www.law.cornell.edu/uscode/)

Miniter, R. (2008). Is Terror Winning in the Courts? Retrieved from http://www.theacru.org/Is%20Terror%20Winning%20In%20The%20Courts.pdf

Montgomery, C. (2009). Can Brandenburg v. Ohio Survive the Internet and the Age of Terrorism?: The Secret Weakening of a Venerable Doctrine. Retrieved from http://moritzlaw.osu.edu/students/groups/oslj/files/2012/03/70.1.montgomery.pdf

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). (Lexis/Nexis, http://www.lexis.com/).

Schenck v. United States, 249 U.S. 47 (1919). (Lexis/Nexis, http://www.lexis.com/).

The Patriot Act. (n.d.). *www.greene-co.com/files/Patriot_act.doc*. Retrieved November 16, 2013, from http://webcache.googleusercontent.com/search?q=cache:xxDIS3Qx3qMJ:greene-co.com/files/Patriot_act.doc+&cd=5&hl=en&ct=clnk&gl=us&client=firefox-a

United States v. Al-Hussayen, No. 3:03-cr-00048-EJL (D. Idaho Feb. 13, 2003). (www.humanrightsfirst.org).

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (Lexis/Nexis, http://www.lexis.com/)

Weaver, R. L. (2011). Brandenburg and Incitement in a Digital Era. *Mississippi Law Journal*, *80*(4). Retrieved from http://mississippilawjournal.org/wp-content/uploads/2012/04/3_Weaver_Final_Edit.pdf

Williams, A. F. (2007). Prosecuting Website Development Under the Material Support to Terrorism Statutes: Time to Fix What's Broken. *NYU Journal of Legislation and Public Policy*. Retrieved from http://works.bepress.com/cgi/viewcontent.cgi?article=1003&context=alanfwilliams&sei-

redir=1&referer=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3Djihadist%2Bterrorism%2Band%2Bbrandenburg%2Btest%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%3Dscholart%26sa%3DX%26ei%3D-KE0UpHIHpDA9gSL6YDoBw%26ved%3D0CCkQgQMwAA#search=%22jihadist%20terrorism%20brandenburg%20test%22