IN THE SUPREME COURT
OF THE UNITED STATES

No. 2011--2012

Chester Comerford, Petitioner-Appellant

v.

The United States of America, Respondent-Appellee

On Writ of Certiorari to the Court of Appeals for the 14th Circuit.

ORDER OF THE COURT ON SUBMISSION

IT IS THEREFORE ORDERED that counsel appear before the Supreme Court to present oral argument on the following issues:

1. Whether the federal government's issuance of an administrative subpoena requiring a commercial Internet Service Provider (ISP) to turn over the content of a subscriber's chat room dialogue violated the Fourth Amendment?

2. Whether Petitioner's facilitation of a chat room in which conversations pertaining to allegedly threatening the president occurred was protected by the First Amendment to the United States Constitution?

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT No. 01--76317

CHESTER COMERFORD, PETITIONER-APPELLANT

vs.

UNITED STATES, RESPONDENT-APPELLEE
Appeal from the United States District Court For the Central District of Olympus

Before KRUGER, Chief Judge, and Judges Sharon Lewis and Cheryl Foley.

OPINION BY KATIE KRUGER, Chief Judge, with Judge Foley concurring:

I

Overview

Petitioner Chester Comerford, a tenured law professor at a publically funded and operated law school known as Olympus State University School of Law, was arrested on January 17, 2011, in violation of 18 USC § 871 for conspiring to assassinate the President of the United States, Barack Obama. He was convicted and sentenced to 5 years in prison. Petitioner contends that the district court erred by denying his motion to suppress information obtained during an allegedly illegal search of an Internet chat room and that the United States violated his First Amendment rights. All issues raised are legal--there are no material factual disputes. Accordingly, we review all questions *de novo.* We AFFIRM the conviction.

III

The Facts

In September 2008, Petitioner started a website via his Internet Service Provider (ISP), DeNolf Communications. According to Petitioner, the main purpose of the site was "to provide a peaceful and private forum for concerned Americans to discuss whether Barack Obama was

born in America." This website was published in tandem with the formation of a group called "The Guardians of the Constitution" (the Guardians), of which Petitioner was the creator.[1] The website was the sole conduit used by the Guardians to disseminate information, conduct meetings, and recruit and enlist new members. To become a member, an individual would have to pledge to protect other members' anonymity, recruit new members, and donate ten percent of their annual income in monthly payments not under $100 U.S.D.

By election day 2008, the Guardians had ballooned to over 200 members. Membership grew even higher following the inauguration of Barack Obama as the nation's 44th president. It was easy to find the website through a search engine such as Google. Because it was easy to find the website, Petitioner established an elaborate high-tech security system to enter the Guardians' chat room. For instance, Petitioner administered an advanced encryption method through the use of "one-time pads," which are mutually known codes for two parties to communicate messages without intrusion via a neutral third-party site. This is not unlike secure credit card transactions that many individuals conduct on a daily basis via a third party secure website such as *Snookie*. These passwords were granted upon the members' payment of the monthly dues, and they changed twelve times a year. Beyond that, Petitioner sporadically re-routed the website address to protect members from archiving the same Internet address, generally known as "cookies," in their computers' histories for extended periods. In addition, all members agreed to certain common-sense methods of security such as never listing identities on the website, and to communicate in the chat room via fictitious screen names. These measures were meant to maintain the Guardians' members' anonymity and guard the chat room from uninvited eyes.

[1] The Guardians were affiliated with the *Birther* movement. "Birthers" question President Obama's citizenship. Under Article II, Section 1 of the US Constitution "No person except a natural born Citizen, or a Citizen of the United States, at the time of the Adoption of this Constitution, shall be eligible to the Office of President."

Visitors to the site could read materials about the Constitution and allegations pertaining to the president's true country of birth that were intended for public viewing. Members of the group occasionally referred others to the site so they could learn more about the cause. Guests were encouraged to inform the public and elected officials about the group's concerns. Suggested tactics included writing their members of Congress about the cause, starting petitions, picketing at appearances by Senator, and later President, Obama, writing letters to the editor, posting messages on-line, and going on television and radio talk shows. Their efforts to "expose" the president as foreign-born intensified after he was inaugurated.

In 2010, the Republican Party took control of the U.S. House of Representatives. Many Guardians expected that the Republicans to whom they had written or whose offices they had called would immediately investigate their claims about the president's true country of birth. When they did not, there was considerable "chatter" in the chat room among the Guardians about Republicans being "traitors" and "taking matters into their own hands." This was especially true in the time after the attempted assassination of Representative Gabrielle Giffords (D-AZ) in January, 2011. Several of the posts lauded Rep. Giffords' assailant as a "true American hero," "a patriot," and "a role model who we should emulate." The Guardian website featured a map that purported to list known public events planned by the president. Members were encouraged to "let their voices be heard" at such events. Some posts called for "showing that we mean business" and "letting him have it in person." One post, wondered if "there were an Oswald among them?" Petitioner responded that "the question is a good one – wish I knew the answer – but don't we all?" In another post Petitioner wrote "Thomas Jefferson thought a revolution was in order every 20 years" and that "violence can be a legitimate form of political action."

In mid-November 2010, Rae La Champ, a second-year student engaged in an in-class moot court project that Petitioner was running in a seminar on the First Amendment, contacted Bobby Bronner, the Dean of the Olympus State University School of Law. La Champ complained the project was "scary" and that the professor "had crossed a certain line of common decency." The dean assured La Champ that he would investigate the charges. Dean Bronner began by making an unannounced visit to Petitioner's class on the First Amendment. He "was surprised" to discover that Petitioner had the students working on a fictional case that involved a defendant who had been arrested for conspiring to assassinate a president-elect who the fictional defendant alleged was foreign born. After that class visit, the dean had the head of the law school's information technology office access the blackboard pages of Petitioner's classes.[2] This was done for his seminar on criminal law and for his seminar on the First Amendment.[3] These blackboard pages are the property of the law school.[4] Petitioner used these sites to post class assignments. A survey of the site found that roughly two-thirds of the assignments on the First Amendment website pertained to speech about threatening federal officials, while half of the assignments on the criminal law website site related to developing arguments related to the defense and/or prosecution of assassins of federal officials. Both blackboard sites contained links to a variety of political websites including that of the Guardians. Petitioner did not identify himself as a member of the group. "Unnerved" by how much the events seemed to mirror reality, the dean made an appointment to speak with Petitioner. At that session, Dean Bronner suggested that Petitioner introduce a greater variety of hypotheticals to his classes and opined

[2] Blackboard is a website that Professors can use to post assignments for their class to download and print. This saves paper and can be accessed by students who have a password. It is a common resource in higher education.

[3] This was accomplished by using a "trap door" built into the blackboard software rather than accessing Petitioner's password. Petitioner was unaware of the access and was unaware that it had been accessed by the dean.

[4] The blackboard home page states that: "Blackboard is an academic resource of the law school. It is not to be used for commercial or political purposes or to send unsolicited e-mail in any form. Individuals found to be in violation of this policy will be subject to disciplinary action." *Issued by the Office of the Law School.*

that "surely the students have learned a great deal about this subject and that it might be time for some new subjects." He asked if Petitioner had made clear that he was not advocating really killing President Obama. According to the dean's sworn court testimony, Petitioner grew agitated and told the dean to "mind his own bloody business" and "demanded to know who had contacted the dean." According to that same testimony, Petitioner "did not really address the question of whether he made clear that he was speaking in the abstract." When confronted with the materials on his class websites, Petitioner asserted that the dean "had no right to view his class websites" and "demanded that the dean pledge never to do so again." The dean refused and replied that the class websites were the property of the law school. Petitioner called Dean Bronner "a stooge for the foreigners who have taken over" and stormed out of the dean's office swearing "never to return again." Dean Bronner contacted legal counsel for the law school and began to review his options with respect to potentially disciplining Petitioner. In the meantime, Petitioner returned to classes the next week. According to La Champ, Petitioner did not change how he presented issues in class other than to say that "he was sorry that some of his students did not understand the First Amendment." His First Amendment class finished working on the moot court hypothetical which culminated in an in-class two week oral argument tournament held in early December. La Champ, the eventual winner of the competition, took her final exam for the class on the morning of December 17, 2010. The final consisted almost entirely of questions about assassination laws and scenarios that included threatening or actually killing a president. President Obama was not named.

On the afternoon of December 17, 2010, Adel Blue, a first year law student enrolled in a seminar taught by Petitioner on Criminal Law e-mailed the Secret Service (SS) that she was concerned that Petitioner was planning to assassinate President Obama. Blue described class

discussions and attached course materials relating to assassinating a president. Some of the alleged threats mentioned President Obama by name, and others did not. The final exam, in fact, consisted almost entirely of questions that required students to develop a defense that would justify assassinating a president. President Obama was not named. Blue noted that the president was scheduled to give the commencement address at Olympus State University in June of 2011 and that students and faculty of the law school had been invited.[5]

On December 18, 2010, a joint task force of the Secret Service (SS) and the Federal Bureau of Investigation (FBI) began to investigate Petitioner. This investigation, headed by Secret Service agent Carmen Pettitte, began by requesting that the law school turn over all information contained in the Blackboard websites for Petitioner's two courses. The Dean of the law school complied with this request. In addition, the Secret Service discovered that Petitioner had an Internet account with DeNolf Communications. DeNolf Communications, like all ISPs, store and have access to customer's websites or chat rooms, but never examine the actual content of those websites or chat rooms.[6] Further investigation of DeNolf Communications' records revealed that Petitioner ran the website and chat room which, along with the Blackboard websites, give rise to the immediate case. Finding the website was fairly easy. Chat room entry, however, was considerably more difficult. On December 19, 2010, task force members issued an administrative subpoena[7] to DeNolf Communications requiring DeNolf Communications to preserve and turn over all present and future content occurring in Petitioner's chat room for the next 90 days. That request was granted that same day by DeNolf Communications. On

[5] A check with the law school and the White House confirmed the scheduled speech.
[6] The DeNolf Communications service contract states that the company "will not monitor or disclose the content of websites or chat rooms that are maintained on its servers unless explicitly mandated by proper legal authority."
[7] An administrative subpoena is an investigative tool used by government agencies and allowed under federal law to obtain information directly from providers without having to establish probable cause or be approved by a Court. Administrative subpoenas differ from warrants in two substantial ways: (1) a warrant requires a showing of probable cause which is not needed for an administrative subpoena; and (2) government agencies have the authority to issue an administrative subpoena directly to an ISP whereas warrants must be approved by a neutral magistrate.

December 20, 2010, federal law enforcement officials began receiving the content of the chat room conversations. They did so without being detected by the Guardians. Formerly, live messaging, such as chat room conversations, was temporary and could not be tracked in the aforementioned manner. New technology, known as "instant messenger reflectors," allowed DeNolf Communications to store chat messages in an archival system as they were sent. This enabled third parties to review past posts. The government did not obtain a warrant, but instead complied with the administrative subpoena requirement of 18 U.S.C. §§ 2703(b)(1)(B)(i) and 2705(1)(B) of the Stored Communication Act (SCA).[8]

In time, it would turn out that the concerns about Petitioner's behavior were well founded. Undisputed evidence at trial established the following facts: On December 21, 2010, a chat room member, Casey Rider, an Olympus Law graduate and former student of Comerford's, initiated a conversation in which she expressed a desire to "rid us of this imposter and take back our country!" Rider stated in the chat room that it would be "easy" for anyone to find the president's travel schedule and to be on-hand when he gave a speech to a group at a fund-raiser or event such as a commencement address. In fact, she wrote that she "planned to attend such an event herself in the not so distant future and would really let him have it." Several members, including Petitioner, responded that "to let him have it would be a good idea." There was no clear statement or discussion of what the term "let him have it" meant. Nor was there any evidence that Rider had made specific arrangements to do so – but fellow Guardian Timothy Pegg, a resident of Olympus, noted that the president was due to give the commencement address at Olympus State University and a second Guardian, Will Thomas, offered to contact a travel agent. No Guardian posted a message taking Thomas up on his offer.

Petitioner, acting as the chat room moderator, was present at all times in the chat room.

[8] See Appendix II and Appendix III respectively.

After these chats of December 21, 2010, Rider enlisted the direct support of members Pegg and Thomas. On December 23, 2010, Rider created a bank account into which Pegg and Thomas were to transfer funds that Rider planned to send to a Swiss bank account associated with the Birther movement. From late December 2010 through mid-January 2011, both Pegg and Thomas, via multiple deposits from their personal banks, transferred $100,000 and $150,000, respectively, into Rider's domestic bank account. It is unclear what exact plans the group had for the money. Federal law enforcement officials subpoenaed bank account information for Petitioner, Rider, Pegg, and Thomas, thus confirming financial transactions by each. Subsequently, the United States froze these assets domestically, where they remain at present.

A raid of Rider's home found a cache of weapons located in a basement. This stash included semi-automatic pistols, long-range rifles, and tear gas. Neither Pegg nor Thomas were found to possess any weapons – though Pegg had a license to possess a firearm in Olympus and Thomas, a former U.S. Marine who had trained in and was decorated for marksmanship, claimed that he had not touched a gun since his honorable discharge and that he "did not believe in violence – he believed in the Constitution." The combination of Blue's e-mail to the Secret Service, and the ensuing investigation that produced the evidence mentioned above, led federal law enforcement officials to bring charges on January 17, 2011, against Rider, Pegg, Thomas, and Comerford for threatening to assassinate the president of the United States and for conspiring to assassinate the president in violation of 18 U.S.C. § 871. Rider, Pegg, and Thomas avoided a trial and pled guilty to threatening the president. They were sentenced to 30 months in prison. Petitioner proceeded to trial. Prior to his trial he moved to suppress all evidence obtained by the government from his Blackboard websites, the Guardian's chat room, as well as the fruits of such evidence, including the financial transaction records. Petitioner argued that the

government's warrantless entry into his chat room violated his Fourth Amendment rights. He argued that his arrest violated the First Amendment. After conducting a suppression hearing, a federal district court denied Petitioner's motion to suppress. That court found that Petitioner did not have a reasonable expectation of privacy in the chat room and it held that the United States did not violate the First Amendment. After trial, a jury found Petitioner guilty of conspiring to assassinate the president. The district court judge sentenced him to the maximum penalty under law: 5 years in prison and fined him $250,000.

III

Fourth Amendment Analysis

In drafting and ratifying the Fourth Amendment, our forefathers recognized the need to balance personal privacy with society's need for security. This led them to allow for searches and seizures – but to limit the circumstances under which such can occur. The immediate case calls upon us to rule on an exception to the Fourth Amendment argued by the government. In doing so, we act to further clarify what constitutes acceptable law enforcement in the Fourteenth Circuit, while being mindful of the fact that we arrive at the opposite conclusion on some of the same issues that were considered by our sister court, the Sixth Circuit.

This case presents three important Fourth Amendment questions. First, the threshold question of whether the Fourth Amendment applies to electronic surveillance, and, concomitantly, whether The Stored Communications Act (SCA), 18 U.S.C. §§ 2703 and 2705--which permits a governmental entity to compel a service provider to disclose the content of electronic communications without a warrant--is constitutional. Second, whether an ISP can provide third-party consent to the government so that it may access electronically-transmitted communications. Third, and alternatively, whether government agents reasonably relied on the

constitutionality of the SCA, and, therefore, acted in good faith. If they did not act in good faith the evidence used to convict Petitioner should have been excluded from his trial.

After carefully weighing and considering all of the issues present in the immediate case, we find that (1) the SCA is constitutional, (2) federal agents substantially complied with the SCA when it subpoenaed Petitioner's records, and (3), even if the SCA is unconstitutional, the federal agents acted in good faith reliance on the statute. The lower court was correct not to suppress the evidence in question. In light of these findings, Petitioner's conviction is AFFIRMED.

We begin with the threshold question of whether Fourth Amendment protections apply to the electronic surveillance at hand. The fundamental purpose of the Fourth Amendment is to protect the privacy of individuals against arbitrary invasions by the government. "Not all government actions are invasive enough [however] to implicate the Fourth Amendment." *Warshak v. United States,* 631 F.3d 266 (6th Cir. 2010). However, when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable," the government must comply with the Fourth Amendment. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Evaluating expectations of privacy involve two discreet inquiries: "First, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search? [and] Second, is society willing to recognize that expectation as reasonable?" *Katz v. United States*, 389 U.S. 347 (1967). Petitioner asks this court to follow *Warshak* and find that Petitioner's Fourth Amendment privacy interests were implicated and that the SCA violated his rights by allowing the government to search and seize his electronic communication without a warrant. We decline Petitioner's invitation and disagree with the Sixth Circuit.

The SCA was adopted in 1986 as an attempt to define privacy interests in the emerging field of electronic communication. At the time of its adoption, use of the Internet as a mode of

communicating was limited to e-mail interactions. Government monitoring of electronic communication was far from routine. Since that time, both the use of the Internet as a mode of electronic communication and its monitoring by the state have proliferated to the point where both are ubiquitous. Mindful that it was regulating a moving target, Congress wrote the statute in a broad fashion that enables it to be applied to instant messaging and chat room conversations. SCA Section 2703(a) requires that a governmental entity issue a warrant to an ISP for electronic communication that has been stored for less than one hundred and eighty days. SCA Section 2703(b)(1)(B)(i), at issue here and in *Warshak*, allows the government to request disclosure by administrative subpoena, and without notice to the customer under SCA Section 2705(a)(1)(B) for ninety days when a supervisory official certifies in writing that "there is reason to believe that notification of the existence of the subpoena may have an adverse result" as listed in subsection (2)(A)-(E) including the "endangering of life or physical safety of an individual," "flight from prosecution," or "otherwise seriously jeopardizing an investigation or unduly delaying a trial."

Justice Scalia noted in *Kyllo v. United States*, 533 U.S. 27, 33-4 (2001) that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." But exposing communications to public view, either the old-fashioned way, or through technological advancements, shrinks the realm of guaranteed privacy. *Cf. Id.* Here, contrary to the dissent and the *Warshak* decision, Congress and federal law enforcement officials struck a proper balance between individual privacy interests of American citizens and the general public welfare interest of security and safety.

The issue here is whether Petitioner had a reasonable expectation of privacy in his chat room. The government obtained an administrative subpoena under 18 U.S.C. §2703(b)(1)(B)(i) compelling DeNolf Communications to preserve and release the content of all communication

occurring in Petitioner's chat room to federal agents. It was reasonable, given the facts and dangerous circumstances of this case, to delay notification to Petitioner. This is true in light of both what we *now* know of the conspiracy and what law enforcement officials knew *at the time.* Protecting the president is a compelling interest of utmost importance to the nation. It does not mean that it provides the government with an absolute license to take any action it deems appropriate. But the Fourth Amendment does not impose the barrier that Petitioner claims.

The SCA strikes a balance between privacy interests and public protection. Petitioner had no objective expectation of privacy in chat room communication conveyed to a third party (DeNolf Communications) and broadcast to the public. Although Petitioner may have manifested a subjective expectation of privacy by his attempt to exclude outside members from participating in his closed chat room sessions, his privacy interest fails the objective test. Society is not prepared to recognize as reasonable electronic communications that occur in chat rooms through third-party proxies, particularly when that communication involves criminal activity**.**

Two principles guide this analysis. First, whether society is willing to accept as reasonable an expectation of privacy in Internet communication. The fact that information is being passed through a communications network is a paramount Fourth Amendment consideration: one that mitigates any reasonable expectation of privacy that Petitioner may have had or thought he had. *See United States v. Miller*, 425 U.S. 435 (1976) (holding that Miller had no expectation of privacy in business records conveyed to and maintained by his bank); *Smith v. Maryland*, 442 U.S. 735 (1979) (holding Smith had no expectation of privacy in the numbers he dialed on his telephone, and the pen register employed by the government through the telephone company was not a search). Basic to this analysis is that information voluntarily conveyed to third-parties is not reasonably expected to be private. *Hoffa v. United States*, 385 U.S. 293 (1966)

(holding that Hoffa's privacy interest was not violated when an undercover officer was invited into his hotel suite, and the officer overheard incriminating conversation). Second, the Fourth Amendment must keep pace with the inexorable march of technological progress. *Cf. Kyllo v. United States*, 533 U.S. 27 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment").

The present case asks us to draw a line between citizens' rights and law enforcement needs in light of expanding Internet technology. The government contends that the warrantless investigation was legitimate because the Internet is akin to broadcasting information to the public, thus abandoning a subjective or objective basis for deeming such communication as private. The Internet consists of both private and public zones, but private zones (e.g., a house or hotel) may forfeit that privacy when intimate activities are exposed to the public. E.g., *Hoffa v. United States*, 385 U.S. 293 (1966). Moreover, information that is conveyed to third parties is subject to the same privacy-forfeiture analysis. In *United States v. Miller*, 425 U.S. 435 (1976), for example, the Supreme Court held the government's subpoena and seizure of Miller's bank documents did not violate his Fourth Amendment right. Miller had no legitimate expectation of privacy in the business records that he conveyed to and were maintained by the bank. *Id.*

The Court of Appeals for the Sixth Circuit, relying heavily on *Katz*, has recently ruled in *Warshak* that electronic communication which is posted to the Internet is analogous to the private mailing of letters or private telephone calls. We believe that this decision is erroneous. The fact is that today, unlike when *Katz* was decided, most people do not communicate privately by mail or home telephone. Individuals do not shut telephone booth doors to keep out prying ears; much electronic communication is exposed to large groups of individuals through third-party portals. Electronic communication occurs via cellular telephone, e-mail, instant messaging,

and chat rooms. Instantaneous communication is more akin to a conversation or public discussion which can be overheard, or conveying information to third parties, including the ISP, and thus not afforded privacy protections. Individuals who convey information, even mail, through private carriers have reduced privacy interests. *See United States v. Jacobsen*, 466 U.S. 109 (1984) (holding that federal agents did not infringe on Jacobsen's privacy right by testing powder without a warrant because a private carrier had opened the package, after it was damaged in transit, revealing that information to a third party). Individuals who reveal private information to another assumes the risk that that information will be revealed to law enforcement. *Id.* Petitioner ran that risk. The dissent, and *Warshak*, ignore the breadth of difference between what is reasonably private, and today's electronic modes of communication which forfeits privacy, making public communication conveyed by third-party providers not private. *Miller* controls here and, consequently, no Fourth Amendment privacy right was implicated. The agents did not need to obtain a warrant before obtaining information via an administrative subpoena about the content of conversations in Petitioner's chat room.

Since we hold that no Fourth Amendment interest was implicated and the SCA struck the appropriate balance, there is no immediate need to reach the government's good-faith argument. Because, however, this case may be appealed to the United States Supreme Court to address the circuit split on whether the Fourth Amendment was implicated and the SCA was unconstitutional, we write to agree with the Sixth Circuit's decision that should the SCA be found unconstitutional, the government agents acted in good-faith reliance on the SCA to obtain Petitioner's records and that access to his chat room was reasonable. *Warshak* citing *Illinois v. Krull*, 480 U.S. 340 (1987) (noting that the exclusionary rule's purpose of deterring law

enforcement officers from engaging in unconstitutional conduct would not be furthered by holding officers accountable for mistakes of the legislature).

The evidence should not have been suppressed. Petitioner's conviction is affirmed.

IV

First Amendment Analysis

The First Amendment question before the court today is one of increasing importance. Given the on-going lack of civility in our national political discourse and the actual violence that has been directed toward elected officials, the concept of a true threat is one which continues to evolve. The question before this court today is whether the First Amendment protects speech which threatens, whether directly or implicitly, the life of the president of the United States. It is with no great difficulty to hold that it does not.

Federal law makes it a crime to threaten the life of the president (18 U.S.C. §871). Most threats to the president, even if doomed to failure from the start, are easy to identify and punish. See *U.S. v. Lockhart*,382 F. 3d 447 (4th Cir. 2004). Petitioner presents a different problem as he never personally made any direct threat. However, the totality of his conduct is enough to conclude that it was reasonable for law enforcement officials to proceed as they did in this case.

"The hallmark of the protection of free speech is to allow free exchange of ideas—even ideas that the overwhelming majority of the American people might find distasteful or discomforting." *Virginia v. Black,* 538 U.S. 343 (2003). When we deal with pure political speech about the nation's leaders, courts will always look at restrictions with suspicion.

However, what is a threat must be distinguished from what is constitutionally protected speech. In *Watts v. U.S.,* 394 U.S. 705 (1969), the Supreme Court first defined the concept of what constitutes a "true threat" and as such falls outside of First Amendment protection. There,

the Court overturned the conviction of Mr. Watts as his threat was not one to be taken seriously. Watts had stated at a political rally that he would not submit to the draft and that if he were forced to serve and if he were given a gun, his first target would be the president. Given the context of the statement, it would be hard to take these words at face value. Watts was at a public rally. He stated that under no circumstances would he carry a gun. When he said if forced he wanted his sights on the president, the crowd reacted with laughter.

There is much in the record before us, however, which make the actions of Petitioner much more grave. Petitioner ran a chat room which fermented serious criminal activity. Several of his associates pled guilty to criminal charges based in large part on information gained from live chats moderated by the Petitioner. It was with his full knowledge and support that these plots were undertaken. These discussions were no joke and cannot be considered hyperbole. In addition, the degree to which Petitioner emphasized assassination and its defense in his courses, is compelling evidence that the government should be allowed to use in its criminal case against Petitioner. He cannot shirk his responsibility in a First Amendment cloak.

Exactly where the line is to be drawn between speech and action was enunciated by the Supreme Court in *Brandenburg v. Ohio,* 395 U.S. 444 (1969). The Court held that "a statute that purports to punish mere advocacy and to forbid, on pain of criminal punishment, assembly with others merely to advocate the type of described action, falls within the condemnation of the First and Fourteenth Amendments." *Brandenburg* explained that "the 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." This is precisely what Petitioner did. While he advocated for peaceful grass-roots political action on the public version of its web site, behind the scenes, Petitioner was part of a group being steeled to action.

A threat is an expression of an intention to inflict harm on another. Alleged threats should be considered in light of their entire factual context, including the surrounding events and reaction of the listeners (or followers).The fact that a threat is subtle does not make it less of a threat. The fact that the threat does not come directly from one group member does not diminish the responsibility of that member. A true threat is "one where a reasonable person would foresee that the listener will believe he will be subjected to physical violence upon his person…." See *Planned Parenthood v. ACLA,* 290 F.3d 1058 (9th Cir. 2002). The First Amendment protects speech that advocates violence, so long as it is not directed to inciting or producing imminent lawless action and is not likely to incite such action. See *Brandenburg, Supra.*

While advocating violence is protected under the First Amendment, threatening a person with violence is not. Furthermore, while the threats here emanating from the Guardians were unlikely to succeed, it is not necessary that a person intend to, or be able to carry out his threat; the only intent requirement for a true threat is that the defendant intentionally or knowingly communicates the threat. (See *U.S. v. Lockhart, supra* and *Planned Parenthood v. ACLA, supra*). Threats fall outside the purview of the First Amendment not due to the content of the message or the view point of the speaker, but to protect individuals from actual violence and from the fear of violence and the disruption that fear engenders. Even though the Petitioner did not carry out the threats personally, he did much to further the process. At a minimum, by providing a forum for the conspiracy and moderating discussion of the plan, he was a part of the criminal conspiracy. The fact that aiding and abetting an illegal act may be carried out through speech does not change the fact of its illegality. Freedom of speech loses constitutional protection when it is the very vehicle of the crime itself. Courts have found liability, in both the criminal and civil sphere where the line between advocacy and action has been crossed. See

Planned Parenthood, supra and *Rice v. The Paladin Enterprises*, 128 F.3d 233 (4th Cir. 1997) which held that the First Amendment does not pose a bar to liability for aiding and abetting a crime, even when such aiding and abetting takes the form of the spoken or written word.

In *Black,* the Supreme Court held that while a true threat must be subjectively intended as such, a threat accompanied by a purpose and intent to intimidate will allow for greater speech restrictions. That case dealt with the message of intimidation implicit in the act of cross burning. *Black* focused on the relative culpability of each defendant with regards to their individual intent to intimidate and thus cause harm. While most cross burnings will cause the requisite intimidation to meet the legal threshold, there are circumstances where the location and audience may negate any negative imagery. This is not true with regards to threats to undermine or overthrow the government or its leaders. In all circumstances, the intent is unambiguous.

The decision of the lower court is hereby AFFIRMED.

DISSENTING OPINION BY JUDGE SHARON LEWIS

I

Fourth Amendment Analysis

The question here is whether a reasonable expectation of privacy encompasses parts of the Internet. Here we revisit the age-old constitutional conundrum of whether the Framers intended for society to adapt to the Constitution or vice versa. While that epic debate will not end here, it seems to me, albeit not to the majority, that the Framers intended the Fourth Amendment to protect individuals' privacy conceptions, which would necessarily change with time, as opposed to an inflexible, artificial version conjured up in the late eighteenth century. The touchstone of this analysis is determining whether there was a reasonable expectation of privacy

in Petitioner's website. *See Katz v. United States*, 389 U.S. 347, 359. It boggles the mind to suggest that the Framers would have agreed that society has no privacy interest in our intimate conversations, particularly after the extensive efforts taken by Petitioner to limit access except to those welcome to the site. I agree, that Petitioner manifested a subjective expectation of privacy. I do not accept, however, that in analyzing whether this expectation was one "that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109 (1984).

I agree with *Warshak v. United States*, -- F.3d -- (6th Cir. 2010) to the extent that it holds that Internet subscribers enjoy reasonable expectations of privacy in the content of their electronic communication "stored with, or sent or received through, a commercial ISP," the government may not compel, nor may ISPs consent to the turning over of subscriber electronic communications without a warrant, and that the provisions of the SCA that allow the government to obtain electronic communication without a warrant are unconstitutional. *Warshak.*

The question of privacy in electronic communication is one of grave import and enduring consequence given the prominent role that the Internet (including e-mail, instant messaging, Facebook and chat rooms) plays in modern communication. *Katz*, 389 U.S. at 352 (suggesting that the Constitution must be read to account for the "vital role that the public telephone has come to play in private communication"). Live "chats" are comparable to phone or face to face conversations. The surveillance of Petitioner's conversations was akin to overhearing spoken statements in the privacy of one's home or in a closed telephone booth, and thus interfered with his reasonable expectation of privacy. *Cf. Hoffa v. United States*, 285 U.S. 293 (1966).

The facts of *United States v. Miller*, 425 U.S. at 443 (1976) are distinguishable. Miller voluntarily gave documents to his bank, and thus took the risk that the third party would reveal that information to the government. In the present case, Petitioner used DeNolf Communications

as an "intermediary," not as the intended recipient of the electronic communication. *See Warshak* (similarly distinguishing *Miller). Katz* found a reasonable expectation of privacy during a telephone call even if an operator had the ability to listen in. Such ability does not forfeit the right to privacy, nor does opportunity to eavesdrop give third-party conveyers the legal authority to release the private information of its subscribers to others, including the government.

DeNolf Communications and Petitioner were not equal partners that shared authority over the chat room, and therefore DeNolf Communications could not consent or agree to the search of Petitioner's website without a warrant. *Cf. Georgia v. Randolph*, 547 U.S. 103 (2006) (holding that a warrantless search of a shared dwelling over the express refusal of consent by a physically present resident cannot be justified as reasonable based on the consent of another resident); *United States v. Matlock*, 415 U.S. 164 (1974). Nor did Petitioner expose the content of his communication to DeNolf Communications, thereby forfeiting his objective right of privacy. *See Hoffa* (finding no Fourth Amendment violation by a secretly, wired government agent invited into a hotel room as a "false friend"). The federal government's uninvited access interfered with a crucial aspect of Petitioner's right of privacy to exclude the prying eyes of others. *See Jacobsen,* 466 U.S. at 113. Third-party access to information does not perforate individual expectation of privacy, especially when the third-party agrees in a service contract to not turn over information about the website or chatroom unless mandated by proper legal authority. If it did there would be no expected privacy in sealed packages or letters in the charge of the United States Post Office. If expected privacy exists with respect to when one enters and closes a phone booth and pays a toll and makes a call, or when one mails a letter, it surely exists in light of Petitioner's actions to shield his chat room from uninvited eyes.

Finally, the majority noted an alternative disposition of this case employing the good-faith exception because the government reasonably relied on the SCA in obtaining and accessing Petitioner's private electronic communication without a warrant. *See Warshak*, citing *Illinois v. Krull*, 480 U.S. at 360. The majority is wrong to employ the good-faith exception for two reasons. First, contrary to the finding of *Warshak*, the SCA is so conspicuously unconstitutional that a reasonable officer could not rely on its objective constitutionality. The SCA is internally inconsistent, requiring a warrant to obtain some protected information, but waiving that requirement for other information. "An officer cannot "be said to have acted in good-faith reliance upon a statute if its provisions are such that a reasonable officer should have known that the statute was unconstitutional." *Warshak*, citing *Krull*, 480 U.S. at 355. Reasonable federal agents would have understood that a warrant based on probable cause was required to compel production of and access to private electronic communication. The same requirement would have been necessary to eavesdrop and wiretap a telephone conversation. *Katz* 359.

More troubling, as noted by the concurring judge in *Warshak*, was that the U.S. did not access stored communication, but rather obtained access to ongoing conversations. This access mirrors the same activity that would require a warrant if communicated via telephone; no reasonable officer should have believed that it was permissible for the government to access ongoing, electronic communication surreptitiously and without a warrant. Second, the federal agents in the case before this court obtained access warrantlessly (albeit with an administrative subpoena) to Petitioner's private communication *after* the Sixth Circuit rendered its decision in *Warshak.* The chronology means that officers had been put on notice that it was not reasonable to rely on the constitutionality of the SCA. As such, the majority incorrectly suggests that good-faith reliance remains a viable way for the government to circumvent the Fourth Amendment.

Contrary to the majority holding that affords little privacy protection to electronic communication, I hold that there are privacy zones on the Internet subject to Fourth Amendment protections. While an individual's subjective privacy expectation still cannot guide this characterization, I believe that there are certain areas on the Internet that society has an interest in accepting as reasonably private, including Petitioner's website and electronic conversations.

II

First Amendment Analysis

I agree that civil discourse has broken down in our society. However, rather than allow greater restrictions on speech as a solution, I would assert that the marketplace of free ideas is much more able to regulate ideas than is the government. No one condones threats made to the life of the president. True threats should be prohibited and punished. But, the line between what is actionable and what is protected must be observed regardless of the political climate.

It is noteworthy that *Watts v. U.S.*, 394 U.S. 705 (1969) and *Brandenburg v. Ohio,* 395 U.S. 444 (1969) both came in 1969, at the end of a decade in which violence claimed the lives of three of the major political leaders of the times. Nonetheless, the Supreme Court firmly concluded that even speech that specifically advocates violence is on balance deserving of protection. More recently, the Ninth Circuit has held specifically that a First Amendment defense must be allowed for crime facilitating speech. See *United States v. Freeman,* 761 F. 2d. 549 (9th Cir. 1985). Petitioner's First Amendment defense offered at trial and to this court is persuasive. We should not retreat from the long-standing values expressed in these decisions – rather we should adopt a standard akin to that of *Freeman* for this circuit.

Watts made clear that any law which makes criminal a form of pure speech must be interpreted within the commands of the First Amendment. That Court recognized that any

restrictions on speech "must be interpreted against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials." That case, like this one, dealt with a so-called threat against the president. *Watts* nonetheless found that the threat in question did not fall outside of constitutional protection. The same logic should apply here. The "threats" which brought Petitioner to the attention of the Secret Service were contained in law school hypotheticals. This type of examination is used at law schools. Professors often use real names or circumstances in challenging their students to think critically and defend positions with which they might not agree. It is true that Petitioner's associates had deadly intentions, but one cannot infer intent on behalf of the petitioner from their intentions.

Even if one were to find some kernel of truth in the threats made in this case, the fact is that in cases where liability has been found to hinge on inciting speech, the requirement of intent has always been present. See *Planned Parenthood v. ACLA,* 290 F.3d 1058 (9th Cir. 2002) and *Rice v. The Paladin Enterprises,* 128 F.3d 233 (4th 1997). The intent standard in the civil context requires that criminal conduct be the natural consequence of the speech in question. Criminal intent to aid and abet requires that the speaker has a purposeful attitude leading to the commission of a crime. It is impossible to assign such criminal intent from this record. All petitioner did was discuss scenarios with his students while being a member of the Guardians. Petitioner was the moderator of the Guardians' website where violence was discussed but there is no way to prove intent from Petitioner's silence.

Porter v. Ascension Parish School Board, 393 F.3d 608 (5th Cir. 2004) and *U.S. v. White,*___F. Supp. 2d ___ (D. IL. 2011) provide recent instances which parallel the situation we

find here. In *Porter*, the plaintiff brought a violent drawing that another person had drawn to school. The drawing featured obscene and racial epithets and a depiction of violence aimed at the school principal. The Court of Appeals for the 5th Circuit properly began its inquiry with the threshold question of whether a speaker intended to communicate a potential threat. Finding no intent to communicate obviated the need to assess whether the speech constitutes a "true threat."

The same logic applies here. The Petitioner did not intend to communicate any threat toward the president. Nor is there any evidence that the president knew of the threats. For those reasons the case should be dismissed much as it was in *U.S. v. Patillo,* 431 F.2d 293 (4th Cir. 1970). All speech in question in the case at bar came either in the classroom or a classroom website (both of which were not open to non-students) or on a password protected chat room (which was specifically closed to all non-members). In *White,* the district court correctly stated that "the general rule in the case law is that speech that is broadcast to a broad audience is less likely to be a true threat, not more." In almost all cases where true threats are found, the threat is directed by someone to someone. Web-based discussions, which lack any normal boundaries of space and time, remove much of the menace from words since they lack any face-to-face encounters.

This case is especially important given the variety of standards being employed by the lower courts to define a true threat. The First and Eighth Circuits have identified and cataloged the variety of approaches taken. See *U.S. v. Fulmer,* 108 F.3d 1486 (1st Cir. 1997) and *Doe v. Pulaski County,* 306 F. 3d. 616 (8th Cir. 2002). Today's opinion, taken with past cases, indicates the extent to which the circuits are split. This conflict merits guidance from above.

For the aforementioned reasons, I respectfully dissent.

Appendix I

18 U.S.C. § 871

Threats against President and successors to the Presidency

(a) Whoever knowingly and willfully deposits for conveyance in the mail or for a delivery from any post office or by any letter carrier any letter, paper, writing, print, missive, or document containing any threat to take the life of, to kidnap, or to inflict bodily harm upon the President of the United States, the President-elect, the Vice President or other officer next in the order of succession to the office of President of the United States, or the Vice President-elect, or knowingly and willfully otherwise makes any such threat against the President, President-elect, Vice President or other officer next in the order of succession to the office of President, or Vice President-elect, shall be fined under this title or imprisoned not more than five years, or both.

Appendix II

18 U.S.C. § 2703

Required disclosure of customer communications or records

. . .

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

. . .

B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

. . .

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Appendix III

18 U.S.C. § 2705

Delayed notice

(a) Delay of Notification.—

(1) A governmental entity acting under section 2703 (b) of this title may—

. . .

B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703 (b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

4th Amendment Cases Cited

1) *Hoffa v. United States*, 385 U.S. 293 (1966).
2) *Katz v. United States,* 389 U.S. 347 (1967).
3) *United States v. Matlock,* 415 U.S. 164 (1974).
4) *United States v. Miller,* 425 U.S. 435 (1976).
5) *Smith v. Maryland,* 442 U.S. 735 (1979).
6) *United States v. Jacobsen*, 466 U.S. 109 (1984).
7) *Illinois v. Krull,* 480 U.S. 340 (1987).
8) *Kyllo v. United States,* 533 U.S. 27 (2001).
9) *Georgia v. Randolph*, 547 U.S. 103 (2006).
10) *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010).

1st Amendment Cases

1) *Watts v. U.S.*, 394 U.S. 705 (1969).
2) *Brandenburg v. Ohio,* 395 U.S. 444 (1969).
3) *U.S. v. Patillo,* 431 F.2d 293 (4th Cir 1970)*
4) *United States v. Freeman*, 761 F. 2d. 549 (9th Cir. 1985).
5) *Rice v. The Paladin Enterprises,*128 F.3d 233 (4th Cir. 1997).
6) *U.S. v. Fulmer,*108 F.3d 1486 (1st Cir. 1997).
7) *Planned Parenthood v. ACLA,* 290 F.3d 1058 (9th Cir. 2002).
8) *Doe v. Pulaski County,* 306 F. 3d. 616 (8th Cir. 2002).
9) *Virginia v. Black,* 538 U.S. 343 (2003).
10) *Porter v. Ascension Parish School Board,* 393 F.3d 608 (5th Cir. 2004).
11) *U.S. v. Lockhart,* 382 F. 3d 447 (4th Cir. 2004).
12) *U.S. v. White, ___ F. Supp. 2d ___* (D. IL 2011)

* Note that there is a 1971 decision in the case of *U.S. v. Patillo* in which the full circuit heard the case en banc. That decision followed the same analysis as the 3 judge panel's 1970 ruling but contained no discussion of the facts. To be clear the 1971 opinion is NOT directly in the record.