Seminar: The First Amendment, the Internet, and Terrorism

Friday, June 3
2:30-3:45 PM
Alumni Hall Ballroom

Faculty Panel: Leslie Kendrick, Law School
Jennifer Petersen, Media Studies
Philip Potter, Politics

(Panelists' biographical information on p. 2)

Moderator: Richard Marks, '66

Focus of Discussion

This panel will explore a fundamental, vexing question of the digital age: when can—and when should—government clamp down on Internet speech intended to incite violent acts? Faculty experts will revisit U.S. Supreme Court decisions that will guide government policy and any new cases about incitement. The panel will also consider incarnations of the Court's "clear and present danger" test as it has evolved, and as it may be applied today, to Web-based speech intended to produce imminent violent acts. A starting question: these days, what is imminent?

This Reunions seminar is organized under auspices of
The Center for Media and Citizenship at the University of Virginia
(http://www.mediaandcitizenship.org/).
The Center was founded as a joint project by WUVA, Inc. and the Media Studies Department
in the College of Arts and Sciences.
WUVA Media (http://www.wuvaonline.com/) is supported by grants from
The Jefferson Trust, an initiative of the UVA Alumni Association,
and from the UVA Parents Fund Committee.

Our Panelists

Leslie Kendrick is the Albert Clark Tate, Jr., Professor of Law at the UVA Law School. Her research focuses primarily on freedom of expression. She teaches courses in torts, property and constitutional law. She received a B.A. in classics and English as a Morehead Scholar at the University of North Carolina at Chapel Hill, and earned her master's and doctorate in English literature at the University of Oxford, where she studied as a Rhodes Scholar. In law school at UVA, she served as essays development editor for the *Virginia Law Review*. Before joining the faculty in 2008, Kendrick clerked for Judge J. Harvie Wilkinson III of the U.S. Court of Appeals for the Fourth Circuit and for Justice David Hackett Souter of the U.S. Supreme Court.

Jennifer Petersen is an Associate Professor of Media Studies. She teaches in the areas of media history, documentary, and cultural studies of journalism. Her book, *Murder, Media, and the Politics of Public Feeling* (Indiana University Press, 2011), explores the emotional mediation of and legal responses to two of the most publicly visible and commented upon hate crimes of the late 1990s. She is currently writing a second book, *The Unspoken History of Free Speech: Media Technologies, Social Science, and the Law*. This book will analyze how legal conceptions of speech within First Amendment law changed over the previous century, from a strictly deliberative and linguistic definition to one that encompasses symbols, aesthetics, and emotion. Petersen earned her PhD in the Radio-Television-Film Department of the University of Texas at Austin. She also received an MA in Journalism from UT-Austin, and a BA in literature from University of California at Santa Cruz.

Philip Potter is an Assistant Professor in the Department of Politics. His research focuses on the domestic politics of international conflict and militant violence. He is a principal investigator for a Department of Defense Minerva Initiative project to map and analyze collaborative relationships among terrorist organizations. His book, *War and Democratic Constraint* (with Matthew Baum), is now available from Princeton University Press (http://press.princeton.edu/titles/10515.html). He has been a fellow at Harvard University and the University of Pennsylvania and holds degrees from UCLA and McGill University.

Recent Terror Events Committed in the U.S. and Likely Involving Internet Incitement

1. December 2, 2015, San Bernadino County Department of Public Health shooting. Perpetrators: married couple Farook (an American-born U.S. citizen of Pakistani descent) and Tashfeen Malik (14 dead; 22 seriously wounded).
2. April 15, 2013, Boston Marathon bombing. Perpetrators: Chechen brothers Dzhokhar and Tamerlan Tsarnaev (3 dead plus two police officers who died as the result of subsequent encounters; estimated 264 wounded).
3. November 5, 2009, Ft. Hood, Texas. Perpetrator: Maj. Nadal Hasan (13 dead; over 30 wounded). Prior to the shooting the FBI had intercepted at least 18 emails between Hasan and Anwar al-Awlaki (al-Qaeda in Yemen), some discussing jihad.

U.S. Supreme Court Cases Involving Alleged Terrorists' Speech

1. *Abrams v. U.S.* (1919).
https://supreme.justia.com/cases/federal/us/250/616/

The Court, 7-2, upheld a World War I era conviction, under the Sedition Act of 1918 (which, with the Espionage Act of 1917, remains on the statute books today), of four anarchists, all Russian immigrants. They had published leaflets condemning President Wilson for sending U.S. troops to czarist Russia to fight Bolsheviks. Justice Holmes, joined by Justice Brandeis, dissented. His dissenting opinion both evolved and departed from earlier WWI era espionage cases. In those cases Holmes had written opinions upholding convictions of alleged subversives for their supposedly dangerous speech. Holmes's departure from precedent, a powerful, spare dissent, set the course of modern First Amendment jurisprudence. He wrote:

> Congress certainly cannot forbid all effort to change the mind of the country. Now nobody can suppose that the surreptitious publishing of a silly leaflet by an unknown man, without more, would present any immediate danger that its opinions would hinder the success of the government arms or have any appreciable tendency to do so.
> …
> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition. To allow opposition by speech seems to indicate that you think the speech impotent, as when a man says that he has squared the circle, or that you do not care whole-heartedly for the result, or that you doubt either your power or your premises. But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution. It is an experiment, as all life is an experiment.

2. *Brandenburg v. Ohio* (1969). https://www.law.cornell.edu/supremecourt/text/395/444

The Court declared Ohio's "criminal syndicalism" statute unconstitutional. It held that the state could not prohibit advocacy of violence (in this case by the Ohio KKK) that did not rise to incitement. The Court re-fashioned – and essentially overruled or substantially modified – earlier cases, some involving the Communist Party, that relied on the so-called "clear and present danger" test. The Court stated: "[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe 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."

3. *Holder v. Humanitarian Law Project* (2010).
http://www.supremecourt.gov/opinions/09pdf/08-1498.pdf

The Court upheld a federal statute forbidding material support to foreign terrorist organizations so designated by the Secretary of State. Congress had concluded that any material support to a foreign terrorist group, even if the support were itself peaceful, aided the group in achieving its terrorist aims. The Humanitarian Law Project (and other plaintiffs) asserted that the First Amendment prevented Congress from stopping the Project from advising two such foreign groups seeking to establish independent states for the Kurds in Turkey and the Tamils in Sri Lanka. The Project proposed instructing these groups in using peaceful means of dispute resolution under international law. Implicitly, the Supreme Court's holding passed the "likely to incite imminent lawless action" test in *Brandenburg*. It is the only post-*Brandenburg* case upholding the government's right to bar speech (in this case, instructing groups in how to apply peaceful dispute resolution techniques).

Three Quotations

"Free speech doesn't make you a terrorist just because you disagree with the government. But if you start espousing violence and radicalizing your own people toward a violent act, the federal government is going to take notice." – Stephanie Douglas, who retired in 2013 as the FBI's top official overseeing foreign and domestic counterterrorism programs, quoted in the Washington Post, September 21, 2016, http://www.washingtonpost.com/sf/national/2016/05/21/armed-with-guns-and-constitutions-the-patriot-movement-sees-america-under-threat/?hpid=hp_rhp-top-table-main_no-name%3Ahomepage%2Fstory .

"The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact." Justice Robert H. Jackson, dissenting in the U.S. Supreme Court case of *Terminiello v. Chicago* (1949), https://supreme.justia.com/cases/federal/us/337/1/case.html .

"A strict observance of the written law is doubtless one of the high duties of a good citizen, but it is not the highest. The laws of necessity, of self-preservation, of saving our country when in danger, are of higher obligation. To lose our country by a scrupulous adherence to the written law, would be to lose the law itself, with life, liberty, property and all those who are enjoying them with us; thus absurdly sacrificing the ends to the means." Thomas Jefferson, explaining his justification under the Constitution for presidential power to authorize the Louisiana Purchase, from *Brest, Paul; Sanford Levinson; Jack M. Balkin; Akhil Reed Amar; Reva B. Seigel (2006). Processes of Constitutional Decisionmaking: Cases and Materials (Print) (6th ed.). New York: Aspen. pp. 65–67.*

Selected Articles *(texts are in the Appendix, beginning on p. 6)*

- The Washington Post, *We Shouldn't Stop Terrorists from Tweeting*
- The Washington Post, *Surprise! NSA data will soon routinely be used for domestic policing that has nothing to do with terrorism*
- Defense One, *China is Watching the FBI–Apple Battle Very Closely*
- The Wall Street Journal, *Why Encryption Fight Divides AT&T and Apple*

Further Reading

For those interested in exploring the seminar topics in greater depth, here are three books we recommend:

The Great Dissent: How Oliver Wendell Holmes Changed His Mind – and Changed the History of Free Speech in America, by Thomas Healy (2013). This wonderful book takes us along on Oliver Wendell Holmes's intellectual journey from enforcer of governmental speech restrictions to seminal advocate of broad free speech rights. Issues of subversion, violence, and incitement before the Supreme Court in the World War I era are hauntingly similar to challenges we face today. To understand freedom of expression under the First Amendment, start with this book.

The Terrorist's Dilemma: Managing Violent Covert Organizations, by Jacob N. Schapiro (2015). Phil Potter recommends this analysis of terrorist organizations, their variety, structure, control, and the vulnerabilities in each unique group. In Phil's words, "my instincts on these matters stem from the belief that militant organizations are more mundane than we often want to believe. By that, I mean that their behavior tends to closely resemble that of legal organizations. This book, though a bit technical in places, does a good job making that case."

The Shadow Factory, by James Bamford (2008). Pre-Snowden, this book described the National Security Agency's vast eavesdropping, warehousing, and data analysis of foreign and domestic communications. It also exposed system failures in U.S. intelligence involving communications monitoring; and Bamford warned, "[t]here is now the capacity to make tyranny total in America."

Appendix of Articles
The First Amendment, the Internet, and Terrorism

October 9, 2014

Opinion: We shouldn't stop terrorists from tweeting

By Daniel Byman and Jeremy Shapiro, *The Washington Post*
https://www.washingtonpost.com/opinions/we-shouldnt-stop-terrorists-from-tweeting/2014/10/09/106939b6-4d9f-11e4-8c24-487e92bc997b_story.html

Daniel Byman is a professor in Georgetown University's School of Foreign Service and the research director of the Center for Middle East Policy at the Brookings Institution. Jeremy Shapiro is a fellow in the Brookings foreign policy program. This piece draws on their work on foreign fighters in Syria that will appear in the forthcoming issue of Foreign Affairs.

A photo tweeted by the jihadist group Welayat Salahadden, allegedly showing Islamic State gunmen executing Iraqi soldiers in civilian clothes north of Baghdad. Social media has been a big recruiting tool for the Islamic State. (Welayat Salahadden/European Pressphoto Agency)

The Islamic State mixes primitive savagery and high-tech sophistication. Its fighters behead and crucify while they post photos of a child holding a severed head and tweet about cats. Although the content is abhorrent and helps the Islamic State radicalize and recruit in the West, the group's massive social media presence is also useful to those fighting terrorism.

The Islamic State's public relations campaigns are slick, even hijacking seemingly benign hashtags such as #WorldCup2014 to propagate the militants' message. And the propaganda is issued in multiple languages — including English, French, Russian and Turkish — to appeal to potential followers. Some of this content is spread from the top ranks of the Islamic State, but the jihadists also have thousands of online followers who retweet messages and create their own content, enabling them to effectively crowdsource jihad.

Although such death videos nauseate most of the world, they make the Islamic State look cool to a key demographic: angry young Muslim men susceptible to indoctrination. Throw in a bit of

sectarian hatred and a touch of promise about Islamic government, and the mix helps keep the Islamic State well supplied with impressionable foreign fighters.

On the other hand, the Islamic State's broadcasting of its brutality over social media makes it easier for people to support the United States and its allies' war with the militants, and it has sparked calls to block the jihadists from the Internet. In the United States, sites such as Facebook, Twitter and YouTube remove some offensive comments linked to terrorism, with support from government agencies. British Prime Minister David Cameron has gone one step further, saying the time has come to be "intolerant of intolerance" and boasting of government efforts to take down thousands of Internet pages.

How can democratic governments, with great concern for civil liberties and free speech, ever hope to impose their will on social media? In some cases, banning particular sites or individuals may make sense if the risk of recruitment and radicalization is high. But those risks have to be weighed against the intelligence value of having groups such as the Islamic State active on social media.

March 10, 2016

Surprise! NSA data will soon routinely be used for domestic policing that has nothing to do with terrorism

By Radley Balko, *The Washington Post*
https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism/?tid=pm_pop_b

A while back, we noted a report showing that the "sneak-and-peek" provision of the Patriot Act that was alleged to be used only in national security and terrorism investigations has overwhelmingly been used in narcotics cases. Now the New York Times reports that National Security Agency data will be shared with other intelligence agencies like the FBI without first applying any screens for privacy. The ACLU of Massachusetts blog Privacy SOS explains why this is important:

> What does this rule change mean for you? In short, domestic law enforcement officials now have access to huge troves of American communications, obtained without warrants, that they can use to put people in cages. FBI agents don't need to have any "national security" related reason to plug your name, email address, phone number, or other "selector" into the NSA's gargantuan data trove. They can simply poke around in your private information in the course of totally routine investigations. And if they find something that suggests, say, involvement in illegal drug activity, they can send that information to local or state police. That means information the NSA collects for purposes of so-called "national security" will be used by police to lock up ordinary Americans for routine crimes. And we don't have to guess who's going to suffer this unconstitutional indignity the most brutally. It'll be Black, Brown, poor, immigrant, Muslim, and dissident Americans: the same people who are *always* targeted by law enforcement for extra "special" attention.

This basically formalizes what was already happening under the radar. We've known for a couple of years now that the Drug Enforcement Administration and the IRS were getting information from the NSA. Because that information was obtained without a warrant, the agencies were instructed to engage in "parallel construction" when explaining to courts and defense attorneys how the information had been obtained. If you think *parallel construction* just sounds like a bureaucratically sterilized way of saying *big stinking lie*, well, you wouldn't be alone. And it certainly isn't the only time that that national security apparatus has let law enforcement agencies benefit from

policies that are supposed to be reserved for terrorism investigations in order to get around the Fourth Amendment, then instructed those law enforcement agencies to misdirect, fudge and outright lie about how they obtained incriminating information — see the Stingray debacle. This isn't just a few rogue agents. The lying has been *a matter of policy.* We're now learning that the feds had these agreements with police agencies all over the country, affecting thousands of cases.

On the one hand, I guess it's better that this new data-sharing policy is acknowledged in the open instead of carried out surreptitiously. On the other hand, there's something even more ominous about the fact that they no longer feel as though they need to hide it.

It's all another sobering reminder that any powers we grant to the federal government for the purpose of national security will inevitably be used just about everywhere else. And extraordinary powers we grant government in wartime rarely go away once the war is over. And, of course, the nifty thing for government agencies about a "war on terrorism" is that it's a war that will never formally end.

March 4, 2016

China Is Watching the FBI-Apple Battle Very Closely

By Adam Segal, *Defense One*
http://www.defenseone.com/ideas/2016/03/china-fbi-apple-encryption/126450/?oref=defenseone_today_nl

Even if the U.S. government abandons its insistence on a backdoored iPhone, Beijing may not.

Shadowing the standoff between the FBI and Apple over access to an encrypted iPhone used by one of the San Bernardino attackers is the question: What will China do? If Apple creates unique software that allows Washington access to the phone, does that open the door for Beijing to make similar demands on the company and all other foreign technology firms operating in China? As Sen. Ron Wyden of Oregon argued, "This move by the FBI could snowball around the world. Why in the world would our government want to give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor?"

Certainly, China watches U.S. statements and policy very closely. An early draft of China's counterterrorism law included provisions requiring the installation of backdoors and the reporting of encryption keys. In the face of criticism from the US government and foreign technology companies, Fu Ying, spokeswoman for the National People's Congress, defended the provisions as in accordance with "international common practices," adding that it was common for the Western countries, such as the United States and Britain, to request tech firms to disclose encryption methods. The final law, passed in December 2015, was much more ambiguous about what type of demands the government would make on technology companies, but it is clear that Chinese leaders are more than happy to exploit what is happening in the United States as rhetorical cover.

Yet we should be clear that what happens in the United States will have very little impact on what China ultimately decides to do. Beijing, like governments everywhere, wants to collect and analyze data for law enforcement and national intelligence reasons. The desire for data may only intensify under Xi Jinping's leadership; the Chinese Communist Party appears increasingly worried about domestic stability and the spread of information within the country's borders. For foreign

companies, refusal to cooperate with the Chinese authorities will increasingly lead to a loss of market opportunities.

Faced with competing pressures across the many jurisdictions that they operate in, there are no easy options for the companies. Any resolution will be political, not technical. The ideal outcome is a multilateral agreement that embraces privacy and the strongest encryption possible, but also allows government access to data for legitimate purposes.

The most workable solution within the United States may in fact involve sidestepping the question about whether governments (or companies) should be able to break encryption. As a recent report from the Berkman Center for Internet & Society at Harvard University argues, there are now massive amounts of data generated through the Internet of Things (cars, thermostats, surveillance cameras and hundreds of devices other connected devices) and the metadata (time, location, address, but not content) produced by cell phones and Internet communications. This data can be made available to law enforcement through established legal procedures, while leaving the encryption that protects phones and other devices alone.

This approach could be standardized across the Atlantic. Governments would leave encryption alone, but share other measures to collect data. With Privacy Shield, the new agreement that regulates the transfer of data by companies between the U.S. and the EU, and reports that the U.S. and UK are negotiating a new treaty that would allow easier access for law enforcement to data, there are promising signs that it is possible to develop trans-Atlantic agreements about how information might be shared across national borders.

China, however, remains the hard case. There is no indication that Beijing would be willing to forgo access to encrypted data on a phone, and, given cultural and political differences, little hope for rules and standards shared across the European, Chinese, and American economies. China and Apple seem to have reached a temporary détente. Beijing has so far not made any further public demands on Apple, and the Chinese market is increasingly important to the company's future, with revenues growing to $12.5 billion in 2015.

Yet Beijing has also made it clear that it expects foreign companies to follow its rules if they want to continue selling in the Chinese market. As China's cyber czar Lu Wei said in December, "As long as you don't harm China's national interests or Chinese consumers' interest, we welcome you and your growth in China." Apple is likely to be pushed, unwillingly, into forking its products, creating separate, less secure products for Chinese users. While this will be a bitter pill for Tim Cook and Apple to swallow, given their promises to defend the privacy of all users, it is likely to be the price of continuing to do business in China.

February 18, 2016

Why Encryption Fight Divides AT&T and Apple

Congress requires carriers to build surveillance capability into their networks

By Ryan Knutson, *The Wall Street Journal*

http://www.wsj.com/articles/at-t-verizon-have-different-obligations-than-apple-1455838171?mod=WSJ_TechWSJD_moreTopStories

For U.S. phone companies like AT&T Inc. and Verizon Communications Inc., the notion of resisting a court order like Apple Inc. Chief Executive Tim Cook recently did is probably inconceivable.

The reason is legal.

In 1994, Congress passed the Communications Assistance for Law Enforcement Act which required that carriers build surveillance capability into their networks. That law was later expanded to cover voice calls placed over the Internet, but not all Internet communication. Other attempts to further expand the law to cover technology companies such as Apple have failed.

Mr. Cook earlier this week said Apple would oppose a federal judge's order to help the Justice Department unlock a phone used by a shooter in the San Bernardino attack, which killed 14 people last December.

These days, the nation's telecom carriers receive thousands of information requests from the government and law enforcement in both national security and civil and criminal matters.

In the last six months of 2015, Verizon and AT&T combined received more than a quarter-million requests from law enforcement agencies in civil and criminal matters and as many as 998 requests in the first six months of 2015 to access customer accounts for national security reasons, according to transparency reports published by the companies.

By comparison, Apple says it received 971 law enforcement requests for account data stored in a user's iCloud or iTunes account In the first half of 2015, the last data available, and provided at least some data to 81% of them. As many as 499 additional requests were related to national security, according to Apple's transparency report.

With much communications traffic shifting from the phone networks to data packets on the Internet, monitoring is becoming more complicated.

"Back in the day, it was AT&T—they had everything, so you just talked to AT&T," said Michael Sussmann, a former Justice Department official who is now a partner at Perkins Coie LLP. "On a phone company I know what a wiretap is: I listen to a call. But what's a wiretap on social network?"

AT&T CEO Randall Stephenson on Thursday reiterated comments he made last month that Congress should determine whether law enforcement should have the ability to access encrypted data on cellphones.

Congress "should decide the proper balance between public safety and personal privacy," Mr. Stephenson said in an emailed statement. "The rapid pace of technological innovation is challenging laws crafted in a very different era for totally different, and much less complex situations. Recent developments, in particular, bring home the need for legal clarity."
Senate Intelligence Committee Chairman Richard Burr (R., N.C.) has decided against a proposal circulating quietly on Capitol Hill to create criminal penalties for companies that decline to comply with court orders to decipher encrypted communications, a spokeswoman said Thursday night.

San Bernardino shooter Syed Rizwan Farook was provided a phone by his employer, which was allegedly subscribed to Verizon, according to government's legal filings. Verizon declined to comment on Mr. Farook's phone.

But the information that Verizon would be able to provide would only be records of phone and text message placed over its network. The carrier can't provide access to vast amounts of other data, such as message content or calls made over mobile apps like WhatsApp, Skype or the blue iMessages sent between two iPhones.

Phone carriers can see when data is traveling over their networks on a service like WhatsApp or Facebook, but they cannot see the content, experts say. That includes the "metadata," such as when a message is sent, or who it is sent to.

The government and law enforcement agencies can ask phone and Internet companies to turn over any customer information they possess, such as Facebook for messages retained on their services, and increasingly the government is asking tech companies to do so. But there is no requirement for phone companies or Internet firms as to how long the content of such data is to be stored. The requirement on phone companies is that the government has the ability to intercept traffic in real time.

Apple says it can provide customer data stored in its iCloud service, such as phone backups that can include stored photos, email, documents, contacts, calendars, and bookmarks. In the San Bernardino case, Apple has provided such data for Mr. Farook until Oct. 19, the last time his phone synced to his iCloud. That means there 44 days of data—such as iMessages and FaceTime calls—that may only exist on his locked iPhone.

In a speech at a cybersecurity conference last spring, former Sprint CEO Dan Hesse summed up the quandary for executives.

"Which CEO is more patriotic, the one who provides all of the information the government requests to help catch a criminal or prevent a terrorist attack?" Mr. Hesse said. "Or the CEO whose company creates tools that make it difficult for law enforcement or the government to acquire a customer's information, believing protecting civil liberties is a higher calling?"