FEAR OF A BLACK AND BROWN INTERNET: POLICING ONLINE ACTIVISM[†]

SAHAR F. AZIZ[*] & KHALED A. BEYDOUN[**]

ABSTRACT

Virtual surveillance is the modern extension of established policing models that tie dissident Muslim advocacy to terror suspicion and Black activism to political subversion. Countering Violent Extremism ("CVE") and Black Identity Extremism ("BIE") programs that specifically target Muslim and Black populations are shifting from on the ground to online. Law enforcement exploits social media platforms—where activism and advocacy is robust—to monitor and crack down on activists. In short, the new policing is the old policing, but it is stealthily morphing and moving onto virtual platforms where activism is fluidly unfolding in real time. This Article examines how the law's failure to keep up with technological advancements in social media poses serious risks to the ability of minority communities to mobilize against racial and religious injustice.

[*] Professor of Law, Chancellor's Social Justice Scholar, founding Director of the Center for Security, Race and Rights (csrr.rutgers.edu), Rutgers University School of Law. The author sits on the New Jersey Advisory Committee for the United States Commission for Civil Rights ("USCCR"). She thanks Marjorie Crawford, Judith Smith, and Caroline Young for their excellent librarian support. She also thanks Professors Orin Kerr and Stephen Dycus for their comments on earlier drafts.

[**] Associate Professor of Law, Wayne State University School of Law; Senior Affiliated Faculty, University of California at Berkeley, Islamophobia Research & Documentation Project ("IRDP"); and Co-director of the Damon J. Keith Center for Social Justice in Detroit, Michigan. The author also sits on the Michigan Advisory Committee for the United States Commission for Civil Rights ("USCCR"), and the Open Society Foundation ("OSF") Equality Fellowship supported his research.

CONTENTS

INTRODUCTION 1153
I. ONLINE ACTIVISM 1159
A. *History* 1159
B. *Emergence of Online Activism* 1161
1. Policy Brutality Against Black Communities 1162
2. Combating American Islamophobia 1164
II. ONLINE POLICING 1167
A. *Countering Violent Extremism* 1170
1. Online CVE Enforcement 1173
2. Eroding Democracy 1175
B. *Black Identity Extremism* 1177
1. Online BIE Enforcement 1178
2. Chilling Online Activism 1179
C. *Vulnerable Targets* 1182
III. PERILS AND PRESCRIPTIONS 1183
A. *Doctrinal Failures in Protecting Online Activism* 1184
1. Open Fields Doctrine 1184
2. Misplaced Trust Doctrine 1185
3. Reasonable Expectation of Privacy Doctrine 1185
4. Third-Party Doctrine 1186
5. The Stored Communications Act 1186
B. *Local Grassroots Initiatives to Regulate Police Online Surveillance* 1188
CONCLUSION 1190

INTRODUCTION

"Nothing was your own except the few cubic centimeters inside your skull."
—GEORGE ORWELL, 1984[1]

Social media has breathed life into speech and social movements across the world. Barriers of place and time are digitally overcome as political activism transcends borders, continents, and time zones. In the United States, "online activism"—the phenomenon whereby individuals transform social media platforms into forums for organized dissent and advocacy—has revolutionized political assembly. Online activism propels longstanding grievances against police brutality of African American communities, discrimination against Muslims, sexual harassment of women, and a myriad of other injustices once limited to traditional forums into global digital spaces in ways previously unimaginable.[2] Online activism has, in short, revolutionized the way people organize and mobilize against state or private injustices—and everything suggests that this phenomenon is still in its infancy.

Despite these seismic changes, some things remain the same. Government agencies still disproportionately police minority communities' collective political action. Black and Muslim activists are still presumed suspicious on account of their political dissidence,[3] and oftentimes benign activity gives rise to suspicion. But instead of just physically following and listening in on these Black and Brown activists, law enforcement now also surveil their social media accounts, virtual footprints, and online lives. This online footprint is more accessible and, in turn, it exposes marginalized groups to modern forms of monitoring that are more intrusive and potentially more injurious.

Social media surveillance is an emerging tentacle of the broader phenomenon of "big data policing."[4] Undercover agents and their proxies create fake accounts by which to infiltrate online groups focused on #BlackLivesMatter, #MuslimLivesMatter, #NoBanNoWall, and other social justice issues. Local

[1] GEORGE ORWELL, 1984, at 26 (Houghton Mifflin Harcourt new ed. 1989) (1948).

[2] To learn about the beginning of the #MeToo movement, see Karishma Verma, #DigitalActivism: Examining #YesAllWomen and Teaching Social Media Activism in Technical Communication 3 (Sept. 9, 2018) (unpublished M.A. thesis, Illinois State University), https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=2018&context=etd [https://perma.cc/J7DQ-EU5W]. To learn about Ferguson, see generally Yarimar Bonilla & Jonathan Rosa, *#Ferguson: Digital Protest, Hashtag Ethnography, and the Racial Politics of Social Media in the United States*, 42 AM. ETHNOLOGIST 4 (2015). For information on the Black Lives Matter movement, see *id.* at 9. For information on the Muslim Ban, see Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 634-36 (2017).

[3] This Article refers to Muslims along lines of individual self-identification.

[4] "Big data policing" refers to the use of algorithms and technological devices, including social media platforms, for policing purposes. For a detailed analysis of big data policing and its emerging use by domestic law enforcement, see generally ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

police departments and federal agencies pay millions of dollars to purchase online monitoring software that collects and mines social media content to identify purported suspicious behavior. Broad terms and coordinated hashtags[5]—such as #BlackLivesMatter, #ChapelHillShooting,[6] #Ferguson,[7] ISIS,[8] *mujahedin*,[9] *ummah*,[10] and protest—are used to target individual activists.[11]

This new form of systematic government surveillance has triggered legal debates about the constitutionality of such practices. In *Packingham v. North Carolina*,[12] the Supreme Court held that "the 'vast democratic forums of the Internet' in general, and social media in particular" are "the most important places . . . for the exchange of views."[13] Despite Justice Kennedy's observation that virtual platforms—like Facebook, Instagram, Twitter, and YouTube—are supplanting traditional public forums as the modern centers for political expression,[14] current speech doctrine is unsettled about how to treat and protect

[5] Hashtags are a device used on social media platforms, such as Twitter and Facebook, to follow or engage with discussions on specific topics or topic areas. For an account of how big data disparately impacts communities of color beyond the policing context, with a careful analysis of how big data results in discrimination, see Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677-94 (2016).

[6] This hashtag was used in reference to the brutal murder of three Muslim American college students in Chapel Hill, North Carolina, in February 2015. *See* Saeed Ahmed & Catherine E. Shoichet, *Three Students Shot to Death in Apartment near UNC Chapel Hill*, CNN (Feb. 11, 2015, 11:30 PM), https://www.cnn.com/2015/02/11/us/chapel-hill-shooting/index.html [https://perma.cc/SVS2-3ZFL].

[7] This hashtag refers to the watershed public protest that formed after Michael Brown was killed by a policeman in the Missouri town. *See* JENNIFER E. COBBINA, HANDS UP, DON'T SHOOT: WHY THE PROTESTS IN FERGUSON AND BALTIMORE MATTER, AND HOW THEY CHANGED AMERICA 72 (2019).

[8] The widely known acronym and hashtag refers to the Islamic State of Iraq and Syria, which emerged into the most menacing Islamic transnational terror network after the decline of its predecessor, al-Qaeda. For a comprehensive account of ISIS, see generally FAWAZ A. GERGES, ISIS: A HISTORY (2016).

[9] Freedom fighters (Arabic). *See Mujahidin*, OXFORD ENGLISH DICTIONARY (2d ed. 1989).

[10] The global Muslim community, oftentimes used aspirationally (Arabic). *See Ummah*, OXFORD DICTIONARY OF ISLAM, http://www.oxfordislamicstudies.com/article/opr/t125/e2427 [https://perma.cc/7C82-JEY9] (last visited Apr. 16, 2020).

[11] Iqra Asghar, *Boston Police Used Social Media Surveillance for Years Without Informing City Council*, ACLU (Feb. 8, 2018, 12:45 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/boston-police-used-social-media-surveillance-years-without [https://perma.cc/5G8B-JYWS].

[12] 137 S. Ct. 1730 (2017).

[13] *Id.* at 1735 (citation omitted) (quoting Reno v. ACLU, 521 U.S. 844, 868 (1997)).

[14] Kennedy referred to the online forums as the "modern public square," terminology that highlights their intimate link to the exercise of free speech. *Id.* at 1732.

online speech.[15] These virtual platforms remain privately owned and regulated, and thus the speech and activity that unfold on their pages are vulnerable to the political ideologies, terms of agreement, and censorship guidelines of their corporate handlers.

In addition to being vulnerable to private censorship and control, the speech that unfolds on these online platforms is accessible to third-party actors, including the government.[16] Advertisers peddle products in line with the profile, preferences, and content provided by users, and the government descends upon users' profiles and pages to police those perceived to be radicals, subversives, or on the brink of terrorism or extremism.[17] In almost every dimension of modern life, online forums have emerged as robust forums for contemporary citizenship, or what communications scholar Guobin Yang appropriately dubs "netizenship."[18] Online citizenship is not only a participatory enterprise but also a *productive* one. Netizens are perpetually producing content or "capital"[19] for the private forums that own the terrain and everything published within it. Online activists are an integral subset of the broader population of netizens, who—for a myriad of motives—capitalize on social media platforms to push ideas, build political community, and mobilize action.

As scholars within and beyond legal academia have noted, online forums are an established and still-developing terrain for activism and dissidence.[20] This is the case internationally—most lucidly illustrated by the "Arab Spring"

[15] For an analysis of how online speech could impact standing-free jurisprudence following the Supreme Court's ruling in *Packingham*, see generally Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353 (2018).

[16] By "third-party actors," the authors are referring to private and public parties beyond the online user and the company, such as corporations seeking to target their advertisements to users, or a government agency.

[17] Shoshana Zuboff dubs this monitoring of online users "surveillance capitalism," which encompasses corporations seeking to generate revenue by tracking individuals and state actors profiting off of the data availed online to advance policing objectives. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019) ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.").

[18] Guobin Yang, *China Since Tiananmen: Online Activism*, J. DEMOCRACY, July 2009, at 33, 34.

[19] This published content is a "critical raw material[] in the pursuit of *surveillance revenues* and their translation into *surveillance capital*. The entire logic of this capital accumulation is most accurately understood as *surveillance capitalism*, which is the foundational framework for a surveillance-based economic order: a *surveillance economy*." ZUBOFF, *supra* note 17, at 94.

[20] This Article focuses squarely on "online political activism" and adopts the general definition set forth by Yang: "Online political activism focuses on human [and civil] rights [and] political reform . . . ." Yang, *supra* note 18, at 33.

movements that blossomed in the beginning of the last decade[21] and, more recently, by the swelling online protests against authoritarianism in India.[22] It is also manifested on the domestic front—the focus of this Article—by the Me Too[23] and Black Lives Matter ("BLM") movements.[24] The internet is a venue for the broader culture of individual online activism that is not formally or ideologically tied to any one movement. The "relatively unlimited, low-cost capacity for communication of all kinds,"[25] on social media platforms especially, has enabled a broad and brave new world of activism—a world that, as technology proliferates and pushes its horizons, has hardly reached its full potential.

Online activism is becoming more entwined with daily life. During the last decade, online forums have not merely evolved into supplements for on-the-ground activism; for younger generations and "communities of color," they are also quickly becoming the principal spaces for organizing, advocacy, debate,

[21] The "Arab Spring" is the popular name given to the numerous revolutions that proliferated in the Mideast and North Africa in 2010, beginning with the Tunisian Revolution in 2010 and followed by the Egyptian Revolution that unseated the longstanding Hosni Mubarak regime in 2011 and the wave of other movements that followed and continue today. Sahar F. Aziz, *Egypt's Protracted Revolution*, 19 HUM. RTS. BRIEF, no. 3, 2012, at 2, 6; *see also* HEATHER BROWN, EMILY GUSKIN & AMY MITCHELL, PEW RESEARCH CTR., ARAB-AMERICAN MEDIA: BRINGING NEWS TO A DIVERSE COMMUNITY 14 (2012), https://www.journalism.org/2012/11/28/arabamerican-media/ [https://perma.cc/6WAR-XJ2C].

[22] The protests in India erupted after Parliament enacted the Citizenship Amendment Act, which restricts naturalized citizenship from Muslim immigrants from Afghanistan, Bangladesh, and Pakistan—a measure that manifested Prime Minister Narendra Modi's regime's staunch anti-Muslim posture. *See* Khaled A. Beydoun, Comment, *Modi's Crusade: Citizenship Amendment Bill Paves the Way for an India Without Islam*, NEW ARAB (Dec. 13, 2019, 5:05 PM), https://www.alaraby.co.uk/english/Comment/2019/12/13/Modis-Crusade-Building-an-India-without-Islam [https://perma.cc/D574-2YLA]; Ruchira Gupta, *A Modi Victory Puts India's 200 Million Muslims in Danger*, THE NATION (May 21, 2019), https://www.thenation.com/article/india-election-modi-bjp-pragya-singh-thakur/ (providing accessible analysis of political and ideological roots of Modi's Islamophobic agenda).

[23] For a timeline of how the Me Too movement was birthed and carried forward, see *#MeToo: A Timeline of Events*, CHI. TRIB., https://www.chicagotribune.com/lifestyles/ct-me-too-timeline-20171208-htmlstory.html [https://perma.cc/DTR8-VCHY] (last updated Mar. 11, 2020, 10:28 AM).

[24] For an analysis of how the BLM movement emerged online in July 2013 and how it capitalized on social media platforms (most notably Twitter) to generate momentum and carry out its message, see generally DEEN FREELON, CHARLTON D. MCILWAIN & MEREDITH D. CLARK, BEYOND THE HASHTAGS (2016), https://cmsimpact.org/wp-content/uploads/2016/03/beyond_the_hashtags_2016.pdf [https://perma.cc/SD3K-C33U].

[25] Reno v. ACLU, 521 U.S. 844, 870 (1997) ("Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.").

and dissent.[26] As one Muslim student at Oregon State University shared, "We don't hold signs and rally when [we're] angry about something anymore, but run to our phones and post it on social media."[27] These days, advocacy is as likely to unfold virtually as it is in physical spaces, and in the not-too-distant future, virtual spaces may be viewed not as divorced or distinct but rather as bona fide public forums.[28] However, the advocacy performed online and the speech posted on virtual platforms, despite being content created by online users, are commonly viewed as the property of private companies—and they are directly accessible to third parties, including the government.[29]

While online activism may be more accessible and democratic, it also poses a range of perils. Online communities that engage in speech tied to the prospect of Islamic "radicalization"[30] or that publish content tethered to fears of Black separatism and violence are targets of online policing. The protracted "war on terror"[31] and the age-old project of policing groups that challenge the state for its mistreatment of Black communities has followed the footsteps of the speaker from the park and the town square to Facebook and Twitter. Policing strategies keep tabs on users' online speech and advocacy as they pivot from traditional public forums to privately owned virtual forums.

[26] *See* MONICA ANDERSON ET AL., PEW RESEARCH CTR., ACTIVISM IN THE SOCIAL MEDIA AGE 4 (2018), https://www.pewresearch.org/internet/2018/07/11/activism-in-the-social-media-age/ [https://perma.cc/65H4-V7MB] ("[A] new survey by the Center finds that majorities of Americans *do* believe these sites are very or somewhat important for accomplishing a range of political goals.").

[27] This quote came from a student following Beydoun's campus-wide lecture at Oregon State University in Corvallis on March 4, 2019. To secure anonymity, the student's name is not provided.

[28] Justice Kennedy's dicta in *Packingham* suggested this, yet online companies are working diligently to maintain their privacy and distance from being classified as traditional or limited public forums. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) ("While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace . . . and social media in particular.").

[29] *See* ZUBOFF, *supra* note 17, at 94; Part III, *infra*.

[30] For an analysis of counterradicalization policing programs deployed within Muslim communities in the United States, see generally Sahar F. Aziz, *Policing Terrorists in the Community*, 5 HARV. NAT'L SECURITY J. 147 (2014).

[31] This Article defines the "war on terror" as the state campaign to police Muslim actors and communities that formally commenced after the 9/11 terror attacks, which—nearly twenty years later—has been presided over and advanced by three presidential administrations. *See* Sean Illing, *How America's "War on Terror" Was (Unwittingly) Designed to Last Forever*, VOX (Jan. 6, 2017, 9:30 AM), https://www.vox.com/conversations/2017/1/6/14166684/terrorism-iraq-war-al-qaeda-9-11-donald-trump-bush-obama-afghanistan [https://perma.cc/TA7A-RZPR].

Accordingly, this Article investigates how two policing programs in particular—Countering Violent Extremism ("CVE")[32] and Black Identity Extremism ("BIE")—are administered online,[33] as well as how they unfold to police online activists that use social media platforms to advocate on behalf of Muslim and Black communities.[34]

CVE government programs began in 2010 under the Obama Administration. They ostensibly aim to identify (Muslim) individuals whom law enforcement believe are vulnerable to recruitment by foreign terrorist organizations and "deradicalize" or off ramp them. Federal and state law enforcement agencies regularly meet with Muslim communities to purportedly empower them to prevent terrorism. Toward that end, law enforcement ask religious leaders, parents, and teachers to observe their congregations, children, and students in search of signs of so-called radicalization toward terrorism. While government documents portray CVE as an innocuous community policing project, advocates and civil rights lawyers argue that counterterrorism surveillance is the real purpose of CVE.[35] BIE programs, meanwhile, do not hide behind the cover of community policing. They constitute a more direct targeting of BLM activists, or individuals perceived to be tied to BLM, as a presumptive public safety threat.

In fleshing out the enforcement and impact of CVE and BIE online policing, we suggest that while these two strands of the broader online policing architecture may be novel with regard to technology and terrain, they are extensions of foundational racialized policing programs—namely, surveillance programs used against Black dissident groups shortly after the advent of the Bureau of Investigation in 1908, later renamed the Federal Bureau of Investigation and, most intensely, during the apex and aftermath of the civil

[32] President Obama established CVE on the federal level in 2011 and elevated it into the focal domestic war-on-terror program of his Administration. *See What Is CVE?*, U.S. DEP'T HOMELAND SECURITY, https://www.dhs.gov/cve/what-is-cve [https://perma.cc/LM5Q-TU7B] (last visited Apr. 16, 2020). For a description of how the Trump Administration has carried it forward, see Faiza Patel & Andrew Lindsay, *Countering Violent Extremism Programs in the Trump Era*, BRENNAN CTR. FOR JUST. (June 15, 2018), https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era [https://perma.cc/599D-TAUD].

[33] The BIE designation is outlined in the FBI report, leaked shortly after its publication. COUNTERTERRORISM DIV., FBI, BLACK IDENTITY EXTREMISTS LIKELY MOTIVATED TO TARGET LAW ENFORCEMENT OFFICERS (2017) [hereinafter BIE REPORT], https://privacysos.org/wp-content/uploads/2017/10/FBI-BlackIdentityExtremists.pdf [https://perma.cc/Y9AF-RPN2].

[34] Naturally, online users that advocate on behalf of Muslim and/or Black communities may not be Muslim or Black themselves and, in some respects, may be vulnerable to the same policing perils faced by Muslim and Black online activists as a consequence of their online speech.

[35] *See* Emma Green, *What Lies Ahead for Obama's Countering Violent Extremism Program*, THE ATLANTIC (Mar. 17, 2017), https://www.theatlantic.com/politics/archive/2017/03/countering-violent-extremism/519822/; *What Is CVE?*, *supra* note 32. *See generally* Aziz, *supra* note 30.

rights movement. Furthermore, this Article illustrates how forms of virtual surveillance are modern extensions of established policing models, driven by longstanding law enforcement presumptions that tie critical Muslim advocacy to terror suspicion and critical Black activism to political subversion. In short, *the new policing is the old policing*, but it is stealthily morphing and moving onto virtual platforms where activism is robust and fluidly unfolding in real time.

This Article proceeds in three parts. Part I provides an overview of the emergent phenomenon of online activism, which in this decade and beyond is poised to become a primary mode of individual and collective action both globally and on the home front. Part II analyzes the anatomy and administration of online policing at large and then carefully examines how CVE and BIE profiling are deployed against perceived Muslim "radicals" and Black "extremists." Part III looks across the policing divide and analyzes how the subjects of CVE and BIE policing are imperiled by the online administration of these programs—particularly by the current Trump Administration. The vulnerability of these online activists, particularly Black and Muslim users, is enhanced by the law's failure to protect them from racialized and politically motivated policing, combined with the corporate landscape that makes their content and user information easily trackable and transferable.

I. ONLINE ACTIVISM

When Americans proudly proclaim that their nation is a beacon of democracy, they point to their freedom to speak, write, organize, and protest without fear of government persecution. Indeed, American society is dynamic due to social and political movements enabled by First Amendment rights. Free speech and the assembly and association rights that emerge from it are a cornerstone—at least theoretically—of the essential American experience.[36] However, these liberties are not equally held, and as history and the present reveal, they are stratified along lines of the content of one's speech and the race, religion, and complexion of the subjects delivering it.

A. *History*

The means and extent by which these rights are exercised are shaped in large part by the latest technologies of the time. Political activism that used to require travel from town to town, for example, was soon replaced with the written word after the printing press was invented. The commercialization of radio in the early

[36] For a critical analysis of how the First Amendment freedom of assembly is denied and diminished for Black dissidents, written in response to the BLM movement, see Justin Hansford, Essay, *The First Amendment Freedom of Assembly as a Racial Project*, 127 YALE L.J.F. 685, 704 (2017-2018). Hansford also observes, "The First Amendment in the popular imagination purports to protect almost all species of dissent, irrespective of political content . . . . This doctrine seems impartial in theory. In practice, speakers who have opposed racial hierarchy have faced harsher treatment from authorities than those who have supported it." *Id.* at 689-90.

1920s and television in the 1940s radically transformed the ability of a speaker to communicate her message to people across the country.[37] By the 1950s, most Americans relied on television, radio, and newspapers for their information, and, political reformers and activists spread their messages to larger audiences through these mediums.[38]

During the 1950s and 1960s, for example, civil rights leaders, such as Martin Luther King Jr. and Malcolm X, strategically used television and radio to call on African Americans to resist Jim Crow laws and demand racial equality.[39] As white Americans watched images of police brutally attacking nonviolent African American protesters, the civil rights movement became a focal national issue.[40] Americans debated whether this clear display of government abuse threatened the freedom to speak, organize, and dissent.[41] While civil rights activism, facilitated by television, recruited large numbers of white Americans to join African Americans, it also prompted a government crackdown. Through agent provocateurs, informants, wiretaps, and physical surveillance, the FBI systematically surveilled and prosecuted African American activists as part of COINTELPRO.[42] But government agents had limited means to do their dirty work.

---

[37] *See* JAMES L. BAUGHMAN, SAME TIME, SAME STATION: CREATING AMERICAN TELEVISION, 1948-1961, at 2 (2007); Tom Lewis, *"A Godlike Presence": The Impact of Radio on the 1920s and 1930s*, OAH MAG. HIST., Spring 1992, at 26, 27.

[38] *See* BAUGHMAN, *supra* note 37, at 2, 24 (discussing relative popularity and proliferation of radio, TV, and newspapers from 1940s to 1950s).

[39] Alexis C. Madrigal, *When the Revolution Was Televised*, THE ATLANTIC (Apr. 1, 2018), https://www.theatlantic.com/technology/archive/2018/04/televisions-civil-rights-revolution/554639/ ("Martin Luther King Jr. was an excellent television producer. He had a keen sense of drama, the use of celebrity, and television's desire for villains and heroes. The organization he cofounded, the Southern Christian Leadership Conference, became the most successful civil-rights organization of the era by combining mass protests and media savvy."); *Malcolm X and the Media*, UMBC, https://fatwts.umbc.edu/malcolm-x-and-the-media/ [https://perma.cc/ER6S-LUGE] (last visited Apr. 16, 2020) ("Malcolm X was one of the most media-savvy black leaders of the period, readily employing television, magazines, and newspapers to spread the ideology of Islam and black nationalism.").

[40] *See* Madrigal, *supra* note 39 (describing how both civil rights activists and members of press were targets of segregationist violence).

[41] *See* Jacquelyn Dowd Hall, *The Long Civil Rights Movement and the Political Uses of the Past*, 91 J. AM. HIST. 1233, 1251 (2005) ("When the so-called classical phase of the movement erupted in the late 1950s and 1960s, it involved blacks and whites, southerners and northerners, local people and federal officials, secularists and men and women of faith. It also extended far beyond the South, and throughout the country it drew on multiple, competing ideological strand.").

[42] Jeffrey O.G. Ogbar, *The FBI's War on Civil Rights Leaders*, DAILY BEAST (Jan. 16, 2017, 12:15 AM), https://www.thedailybeast.com/the-fbis-war-on-civil-rights-leaders [https://perma.cc/7Q5L-6GYK] (explaining that COINTELPRO used "informants, agent provocateurs, infiltrators, legal and illegal wiretaps, break-ins, false correspondence, and 'bad-jacketing'" to "disrupt, misdirect, discredit, and neutralize" civil rights organizations).

In contrast to social media, however, television, radio, and newspapers were, and remain, top-down, one-way forums of communication between the speaker and the listener. Moreover, aside from a handful of minority owner and operated media, gatekeepers in the roles of television producers, radio hosts, and newspaper editors controlled the content published in these forums. And publishing one's ideas in the 1950s and 1960s remained an enterprise limited to elites and select segments of society. The advent of the internet in the late 1990s thus revolutionized communication in ways that made publishing and disseminating content far more accessible and, in turn, forever transformed the nature of social movements.[43] Not only was control over content granted to anyone who created a website or YouTube channel, but people could also communicate directly in groups via email and online chat forums.

B. *Emergence of Online Activism*

The emergence and mainstreaming of social media in the twenty-first century revolutionized speech, assembly, and activism. In 2006, when Twitter was created and Facebook first became available to the public, people could watch simultaneous livestreams, conversations, and online exchanges.[44] Activists in different parts of the country or on different continents could communicate, organize, and advocate in real time as a means of escalating and enlarging their movements.[45] Users could also read in real time protesters' tweets, the latest news, police statements, and observers' interpretations of unfolding events.[46] People in different locations and time zones now directly collaborate on issues of common concern. Local grievances are in turn amplified to attract global attention by bringing visibility and accountability to repression.[47]

Furthermore, the ubiquity of smartphones coupled with that of social media forums enables people in various authoritarian regimes around the world to connect online and express dissent about social, economic, and political

[43] *See infra* notes 46-49 (describing numerous ways different social movements have used online communication).

[44] Nicholas Carlson, *The Real History of Twitter*, BUS. INSIDER (Apr. 13, 2011, 1:30 PM), https://www.businessinsider.com/how-twitter-was-founded-2011-4 [https://perma.cc/GEL6-ZD6C]; Saqib Shah, *The History of Social Networking*, DIGITAL TRENDS (May 14, 2016), https://www.digitaltrends.com/features/the-history-of-social-networking/ [https://perma.cc/B88A-VCTB].

[45] *See* Bonilla & Rosa, *supra* note 2, at 7 (discussing impact of social media globally and in context of #Ferguson).

[46] *See id.* (explaining impact of social media on people who were not in Ferguson following murder of Michael Brown).

[47] Social media platforms are especially revolutionary in authoritarian states where no public forums previously existed. *See, e.g.*, *Breaking Bongo*, RADIOLAB (Nov. 26, 2019), https://www.wnycstudios.org/podcasts/radiolab/articles/breaking-bongo (showcasing impact of Gabonese expatriates' social media activism and their attempts to discredit current Gabonese regime).

problems—dissent that is prohibited in physical spaces.[48] Widespread online mobilization culminated in the historic "Arab Spring" in 2011 that toppled entrenched dictators in Egypt, Libya, Tunisia, and Yemen.[49] That same year in September, the Occupy Wall Street movement began receiving widespread attention in the United States.[50] Leaders of the movement used social media to leverage public grievances following the Great Recession of 2008. Online activism led to large protests across the nation decrying growing economic inequality.[51] It was only a matter of time before social media would also enable mobilization against deeply entrenched anti-Black racism and skyrocketing anti-Muslim bigotry.

1. Policy Brutality Against Black Communities

That is precisely what happened when twenty-eight-year-old George Zimmerman was acquitted in 2013 for fatally shooting unarmed seventeen-year-old Trayvon Martin in Sanford, Florida.[52] In protest, three Black women started the BLM movement using the hashtag #BlackLivesMatter to bring attention to the longstanding devaluation of African Americans' lives.[53] Whether by police officers or private citizens, the killing of African Americans occurs without

[48] *See* Pien Huang & Yuhan Xu, *'Please Help Me.' What People in China Are Saying About the Outbreak on Social Media*, NPR (Jan. 24, 2020, 2:48 PM), https://www.npr.org/sections/goatsandsoda/2020/01/24/799000379/please-help-me-what-people-in-china-are-saying-about-the-outbreak-on-social-medi [https://perma.cc/RT9E-J3CY] (describing Chinese social media users' activities in face of government silence); *see also* Bonilla & Rosa, *supra* note 2, at 5 (noting that 56% of U.S. population carries video-enabled smartphones); Brian S. Krueger, *Government Surveillance and Political Participation on the Internet*, 23 SOC. SCI. COMPUTER REV. 439, 440 (2005) (explaining that in 2003 more than 60% of U.S. adult population was connected to internet).

[49] John G. Browning, *Democracy Unplugged: Social Media, Regime Change, and Governmental Response in the Arab Spring*, 21 MICH. ST. INT'L L. REV. 63, 63 (2013) (explaining that social media represents shift in how people communicate and share information and that this shift was most evident during Arab Spring). For a summary of the Arab Spring's impact on Egypt, see Sahar F. Aziz, *Bringing Down an Uprising: Egypt's Stillborn Revolution*, 30 CONN. J. INT'L L. 1, 3-7 (2014).

[50] *See* Sara Kunstler, *The Right to Occupy – Occupy Wall Street and the First Amendment*, 39 FORDHAM URB. L.J. 989, 989 (2012) ("The Occupy movement, starting with Occupy Wall Street in Zuccotti Park in New York City, captured the public imagination and spread across the country with a force and rapidity that no one could have predicted.").

[51] Anastasia Kavada, *Creating the Collective: Social Media, the Occupy Movement and Its Constitution as a Collective Actor*, 18 INFO. COMM. & SOC'Y 872, 872-73 (2015).

[52] Richard Luscombe, *George Zimmerman Acquitted in Trayvon Martin Case*, THE GUARDIAN (July 13, 2013, 10:08 PM), https://www.theguardian.com/world/2013/jul/14/zimmerman-acquitted-killing-trayvon-martin [https://perma.cc/JK5Y-2UG8].

[53] Katheryn Russell-Brown, *Critical Black Protectionism, Black Lives Matter, and Social Media: Building a Bridge to Social Justice*, 60 HOW. L.J. 367, 401 (2017).

accountability. Police officers are rarely prosecuted, and in those rare instances when they are, acquittal is nearly always the outcome.[54]

The following year in 2014, two more unarmed Black men—Michael Brown in Ferguson, Missouri,[55] and Eric Garner in New York City—were killed by police officers.[56] Videos of their deaths (and the deaths of other Black men) went viral on social media, accelerated by the hashtags #BlackLivesMatter and #Ferguson.[57] Street protests and demonstrations soon followed in cities across the country.[58] Ferguson became the focal point where a BLM Freedom Ride brought protestors from various cities to converge into a national protest.[59]

Social media has been instrumental in bringing the voices of the BLM activists, Black victims of police brutality, and families of the victims to the national stage.[60] From July 2013 to May 2018, the #BlackLivesMatter hashtag was used nearly thirty million times on Twitter at an average of 17,000 times

[54] Kami Chavis Simmons, *Increasing Police Accountability: Restoring Trust and Legitimacy Through the Appointment of Independent Prosecutors*, 49 WASH. U. J.L. & POL'Y 137, 139 (2015) ("[P]olice accountability measures may not result in punishment of individual officers who have employed excessive force, because even when seemingly damning evidence exists, prosecutions of officers have traditionally been rare and even when officers are prosecuted, convictions are difficult to secure.").

[55] Jon Swaine, *Michael Brown Shooting: 'They Killed Another Young Black Man in America*,*'* THE GUARDIAN (Aug. 12, 2014, 4:46 PM), https://www.theguardian.com/world/2014/aug/12/ferguson-missouri-shooting-michael-brown-civil-rights-police-brutality [https://perma.cc./L55P-KUBT] ("On Saturday afternoon, Brown was shot to death by a police officer while apparently walking, unarmed, from a convenience store to his grandmother's apartment in Ferguson, a working-class suburb north of St. Louis, the main hub of this midwestern state.").

[56] Amanda Holpuch, *Widow of Eric Garner Speaks at Protest Rally over NYPD 'Chokehold' Death*, THE GUARDIAN (July 26, 2014, 4:08 PM), https://www.theguardian.com/world/2014/jul/26/widow-eric-garner-speaks-rally-nypd-chokehold-death [https://perma.cc/ELL4-2ZK5].

[57] Rashawn Ray et al., *Ferguson and the Death of Michael Brown on Twitter: #BlackLivesMatter, #TCOT, and the Evolution of Collective Identities*, 40 ETHNIC & RACIAL STUD. 1797, 1797-98 (2017) ("Social media activism is purported as a major reason that the deaths of Michael Brown and Freddie Gray, among others, became international news. Incidents related to their deaths were video recorded and photographed with mobile phones and then uploaded to social media platforms.").

[58] Diantha Parker, *Protests Around the Country Mark the Moment of Ferguson Shooting*, N.Y. TIMES (Dec. 1, 2014), https://www.nytimes.com/2014/12/02/us/protests-around-the-country-mark-the-moment-of-ferguson-shooting.html (reporting on protests concerning Michael Brown's death and use of hashtag #HandsUpWalkOut to spread protest information).

[59] *What We Believe*, BLACK LIVES MATTER, https://blacklivesmatter.com/what-we-believe/ [https://perma.cc/VNB2-D79B] (last visited Apr. 16, 2020).

[60] *See* Munmun De Choudhury et al., *Social Media Participation in an Activist Movement for Racial Equality*, 2016 PROC. TENTH INT'L AAAI CONF. ON WEB & SOC. MEDIA 92, 92 ("Social media, especially Twitter, due to its pervasiveness and adoption, has provided the fundamental infrastructure to this activist movement.").

per day, according to the Pew Research Center.[61] Other commonly shared hashtags that mobilized protests against police brutality include #HandsUpDontShoot, #HoodiesUp, #IfTheyGunnedMeDown, #NoAngel, and #WeAreTrayvonMartin.[62] Along with the hashtags, social media activists posted pictures of themselves with their hands up, holding signs stating "don't shoot" and wearing hoodies.[63] Events across America spurred an unprecedented online movement calling for police accountability and dignity for Black lives, which had the reciprocal effect of driving forward the on-the-ground movement. Without the galvanization of online voices exposing injustices against Black lives, it is highly likely that the on-the-ground movement would have never taken form.

These myriad forms of online activism illuminate why the Pew Research Center found that 53% of Black social media users say social media sites are "personally important to them when it comes to expressing their political views or getting involved with issues they feel are important," as compared to between 32% and 36% of white users.[64] Similarly, about 80% of Blacks say social media sites "highlight important issues that may not get a lot of attention" and "help give a voice to underrepresented groups," as compared to about 60% of white users.[65] By amplifying their voices through social media, minority communities are able to challenge the negative stereotypes and tokenization of their identities that permeates mainstream media, over which they have much less influence because the gatekeepers of mainstream media outlets are predominantly white and upper class.

2. Combating American Islamophobia

Debunking stereotypes lies at the center of online activism by Muslims in the United States. "American Islamophobia" worsens each time a terrorist attack occurs in a Western city, regardless of whether the attack took place in the U.S. or beyond its borders.[66] When bombs go off in Barcelona, Boston, London, or Paris, Muslims are collectively punished through hate crimes, mosque vandalizations, school bullying, and employment discrimination. While some

[61] *See* ANDERSON ET AL., *supra* note 26, at 3.

[62] Bonilla & Rosa, *supra* note 2, at 8-9.

[63] *Id.* at 8.

[64] ANDERSON ET AL., *supra* note 26, at 7; *id.* at 11 ("There are also racial and ethnic differences around the idea that social media make[s] it easier to hold powerful people accountable for their actions – with blacks and Hispanics being more likely to agree with this compared to whites.").

[65] *Id.* at 10-11.

[66] This is the phrase the authors assign to the broader culture of anti-Muslim animus in the United States per the title of the book, KHALED A. BEYDOUN, AMERICAN ISLAMOPHOBIA: UNDERSTANDING THE ROOTS AND RISE OF FEAR (2018).

Muslims respond by retreating from the public sphere, many—particularly younger generations—have responded through increased activism.[67]

To counter the bigotry they experience in various aspects of their daily lives because they are presumed to be terroristic, disloyal, and dangerous,[68] Muslims are utilizing social media and hashtag activism.[69] For example, the rampant Islamophobia peddled by Republican presidential candidates in 2015 and 2016 produced a hostile anti-Muslim political environment.[70] Many Muslims, especially Muslim youth, responded by politically mobilizing online using hashtags, such as #MuslimLivesMatter, #NoBanNoWall, #NotInMyName, and #TakeOnHate.[71] The proliferation of anti-Muslim rhetoric and its deployment by many Republicans—most notably by then-candidate Donald Trump—propelled Islamophobia into the public consciousness as a primary civil rights concern and, in turn, spawned an unprecedented rise of online activism among Muslims.[72]

The momentum created from online activism transformed into protests in airports across the country when President Trump issued an executive order on January 27, 2017, banning tens of millions of Muslims from entering the United States.[73] Similar to what happened in Ferguson, information from families of

[67] *See* William Hobbs & Nazita Lajevardi, *Effects of Divisive Political Campaigns on the Day-to-Day Segregation of Arab and Muslim Americans*, 113 AM. POL. SCI. REV. 270, 274 (2019) (discussing changes in social media activity of people with Arab-sounding names following election of Donald Trump and terrorist attack in San Bernardino, California).

[68] For a theoretical analysis of how Muslims are disidentified as citizens and reidentified as terrorists during the war on terror, see Leti Volpp, *Citizenship Undone*, 75 FORDHAM L. REV. 2579, 2584 (2007).

[69] Cathy Lynn Grossman, *Hashtag Activists Battle Online Anti-Muslim Speech, but #DoesItWork?*, RELIGION NEWS SERV. (Nov. 13, 2014), https://religionnews.com/2014/11/13/twitter-muslim-islamophobia-isis/ [https://perma.cc/PS4U-T5BZ] ("Using names such as #TakeOnHate, #ISpeakOutBecause, and #NotInMyName, the pushback approach promotes the complexity, diversity and positive contributions of Islam and Muslims.").

[70] Hobbs & Lajevardi, *supra* note 67, at 271-74 (describing impact of Donald Trump's proposed "Muslim Ban" and Ted Cruz's proposal to surveil Muslim American communities).

[71] *Id.* at 274.

[72] Khaled A. Beydoun, *9/11 and 11/9: The Law, Lives and Lies That Bind*, 20 CUNY L. REV. 455, 456-57 (2017) (weighing impact of Donald Trump's election on Muslim Americans' relationship with society at large); *see* Sahar F. Aziz, *"Whosoever Sees an Evil" – Muslim Americans' Human Rights Advocacy*, OXFORD RESEARCH ENCYCLOPEDIA OF RELIGION (forthcoming 2020) (manuscript at 9-17), https://papers.ssrn.com/abstract_id=3507500 [https://perma.cc/4EBZ-CC22] (describing rise of civil and human rights advocacy post-9/11 in response to rising Islamophobia and anti-Muslim racism).

[73] For an analysis of the popular response to Trump's executive order, see Abed Ayoub & Khaled A. Beydoun, *Executive Disorder: Muslim Bans, Emergency Advocacy, and the Fires Next Time*, 22 MICH. J. RACE & L. 215, 226-33 (2017); and Sahar F. Aziz, *A Muslim Registry: The Precursor to Internment?*, 2017 BYU L. REV. 779, 784-85 (describing the multiple and systematic attacks on Muslims by Donald Trump in month preceding his election and issuance of the executive order).

people detained or stranded outside the country was shared under the hashtag #MuslimBan.[74] This hashtag enabled Muslim activists to simultaneously mobilize protests in multiple cities.[75] Photos and news reports of the protests that were posted and shared online fueled opposition to the executive order, which was eventually stayed by multiple courts and narrowed by the Supreme Court months later.[76] Online activism not only translated into street protests but also motivated more than ninety Muslim Americans to run for office in 2017 on the Democratic ticket in what came to be known as the "Blue Muslim Wave."[77]

But social justice activists are not the only ones using social media to mobilize people. Foreign governments, most notably Russia, have seized upon social media platforms and deployed "bots" to influence American voters.[78] Foreign groups designated as terrorists by the U.S. government also leverage social media to recruit young Muslims from across the world to travel to Iraq, Libya, and Syria to join their militias.[79] Al-Qaeda and ISIS produce high-quality videos, photos, and other content for online dissemination to spread their ideology.[80] Similarly, white-supremacist and far-right extremist groups use social media to propagate false stories about a purported Muslim "invasion," endemic Black crime against whites, and a Latino incursion from the southern border. Some of these groups, such as the Ku Klux Klan and the sovereign citizens movement, use violence in furtherance of their ideologies. Others, such as the alt-right

[74] Saeed Kamali Dehghan, *Iranian Cancer Researcher Sent Home After Being Denied Entry in Boston*, THE GUARDIAN (July 12, 2017, 10:20 AM), https://www.theguardian.com/us-news/2017/jul/12/iran-cancer-researcher-detained-us-travel-ban-mohsen-dehnavi [https://perma.cc/K2GD-7WQ2] (showcasing that pediatric cancer researcher was unable to enter United States despite valid visa).

[75] *See Protests Erupt at U.S. Airports as Trump Order Targeting Refugees & Muslim Immigrants Takes Effect*, DEMOCRACY NOW! (Jan. 28, 2017), https://www.democracynow.org/2017/1/28/protests_erupt_at_us_airports_as [https://perma.cc/7LLN-8MR9].

[76] *See* Trump v. Hawaii, 138 S. Ct. 2392, 2423 (2018) ("Because plaintiffs have not shown that they are likely to succeed on the merits of their claims, we reverse the grant of the preliminary injunction as an abuse of discretion.").

[77] Abigail Hauslohner, *Muslim American Candidates Hope for 'Sweet Justice*,*'* WASH. POST, Apr. 16, 2018, at A16.

[78] *See* Laurent Sacharoff, *Russia Gave Bots a Bad Name. Here's Why We Need Them More than Ever.*, POLITICO MAG. (Aug. 14, 2018), https://www.politico.com/magazine/story/2018/08/14/russia-gave-bots-a-bad-name-heres-why-we-need-them-more-than-ever-219359 [https://perma.cc/2SVT-XAEM] (examining how Russia's "bots"—algorithmic devices used to collect online users' data—also perform productive work and have positive value).

[79] *See* Peter R. Neumann, *Options and Strategies for Countering Online Radicalization in the United States*, 36 STUD. CONFLICT & TERRORISM 431, 436 (2013).

[80] *See* Scott Higham & Ellen Nakashima, *Balancing Security Against Free Speech*, WASH. POST, July 19, 2015, at A01 (discussing ISIS's use of popular social media platforms); Eric Schmitt, *U.S. Intensifies Effort to Blunt ISIS' Message*, N.Y. TIMES, Feb. 17, 2015, at A1 ("With the Islamic State and its supporters producing as many as 90,000 tweets and other social media responses every day, American officials acknowledge they have a tough job ahead to blunt the group's digital momentum.").

movement, aim to polarize the public in ways that lead to violence, as witnessed in the "Unite the Right" protests in Charlottesville, Virginia, in 2017 that killed one person and injured nineteen.[81]

With more than two billion Facebook users, 800 million Instagram users, and 330 million Twitter users, social media has become a staple of contemporary activism and expressions of dissent.[82] Again, it will become even more prominent as time passes and technology becomes more integrated and entwined with our daily lives.[83] But just as social media serves as a shield against government abuse and overreach, it can also be weaponized to exponentially expand government surveillance of citizens' speech, associations, and political activities. Consistent with historical precedent, racial and religious minorities are the first and most frequent targets.[84]

II. ONLINE POLICING

Social media provides a treasure trove of data about an individual's private and public life. If monitored over an extended period of time, the data reveal a detailed summary of a person's preferences, associations, religious affiliations, political beliefs, and daily activities.[85] As a result, privacy advocates warn of the dangers arising from law enforcement surveillance of social media posts.[86]

[81] Meghan Keneally, *What to Know About the Violent Charlottesville Protests and Anniversary Rallies*, ABC NEWS (Aug. 8, 2018, 4:44 PM), https://abcnews.go.com/US/happen-charlottesville-protest-anniversary-weekend/story?id=57107500 [https://perma.cc/NY4U-VT65].

[82] *See* ANDERSON ET AL., *supra* note 26, at 5 ("Social networking sites have also emerged as a key venue for political debate and discussion."); Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523, 524 (2018) (noting how police use social media to monitor public sentiment).

[83] The current coronavirus pandemic and the order to remain confined at home and practice "social distancing" highlight an extreme instance of when online activism is the lone avenue for public expression and dissent, as evidenced by criticisms of President Donald Trump's handling of the pandemic taking place online.

[84] Kashmir Hill, *The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook*, THE ROOT (Oct. 23, 2018, 1:30 PM), https://www.theroot.com/the-wildly-unregulated-practice-of-undercover-cops-frie-1828731563 [https://perma.cc/M9M6-RRGF] (noting that undercover tactics in modern technological age still foster "age-old risks of abuse of power" of discrimination and racial profiling).

[85] This virtual footprint left by individuals online is precisely why algorithms—"formally specified sequence[s] of logical operations that provide[] step-by-step instructions for computers to act on data and thus automate decisions"—are so precise in profiling the interests, habits, and preferences of online users. Barocas & Selbst, *supra* note 5, at 674 n.10.

[86] *See, e.g.*, Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectation of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 57 (2015); Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 247 (2012); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 141 (2014); Junichi P. Semitsu, *From Facebook to Mug Shot: How the*

Although the content is viewable by portions of the public, the Supreme Court has recognized that the extent to which data reveals intimate information about a person is relevant to the question of whether government monitoring requires a warrant or other heightened legal protections.[87] Nevertheless, current law permits police departments and federal agents to monitor and collect social media activity based on the reasoning that users voluntarily disclose information to third parties—namely Facebook, Instagram, Twitter, and other private companies.[88] Although it now appears that the law, responsive to changes in technology and culture, may be changing. Supreme Court jurisprudence so far suggests that citizens have no reasonable expectation of privacy from government surveillance of social media activity.[89]

Thus, it should come as no surprise that nearly 70% of police departments report using social media to gather intelligence for investigations.[90] Private companies receive tens of millions of taxpayer dollars annually to operate social media monitoring software for police departments.[91] Products such as Dataminr, Dunami, Geofeedia, Media Sonar, and SocioSpyder enable law enforcement agencies to continually monitor and store the social media activity of millions of people.[92] Furthermore, police officers use fake social media profiles to

Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance, 31 PACE L. REV. 291, 376-78 (2011); *see also Map: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CTR. FOR JUST. (July 10, 2019), https://www.brennancenter.org/our-work/research-reports/map-social-media-monitoring-police-departments-cities-and-counties [https://perma.cc/E3ZQ-6BFM] (describing how social media monitoring stifles civil liberties and civil rights, specifically First Amendment right of freedom of speech).

[87] *See* Carpenter v. United States, 138 S. Ct. 2206, 2216-17 (2018) (finding that cell phone GPS information is so personal that it requires warrant even though held by third party); Riley v. California, 573 U.S. 373, 393, 403 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."); United States v. Jones, 565 U.S. 400, 404-05 (2012) (finding that installation of and monitoring with GPS on vehicle constitutes search under Fourth Amendment).

[88] United States v. Miller, 425 U.S. 435, 443 (1976).

[89] *Id.* ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

[90] *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, *supra* note 86 (collecting data for 158 jurisdictions). Less than 15% of police departments have publicly available policies governing how such surveillance is conducted. *Id.*; *see* Semitsu, *supra* note 86, at 318 (noting how Facebook serves as a valuable investigative tool for government).

[91] Levinson-Waldman, *supra* note 82, at 552 n.159 (describing how social media monitoring has transformed into "big business").

[92] ELEC. PRIVACY INFO. CTR., SOCIAL MEDIA MONITORING: GOVERNMENT SURVEILLANCE OF PUBLIC SPACE 10 (2018), https://epic.org/privacy/surveillance/spotlight/0518/Social-Media-Monitoring.pdf [https://perma.cc/HD4J-F9LT] (reporting that "FBI has hired

infiltrate online activists' groups.[93] When challenged in court, investigators have successfully claimed that they primarily focus on catching terrorists, gang members, child predators, and gun traffickers.[94]

However, news reports reveal another focus—political activists. Police have collected information about demonstrations at a Denny's in California, a high school in Florida, a church in Illinois, and a parking lot in Wisconsin, and they disseminate the information to law enforcement fusion centers nationwide.[95] Absent federal or state laws regulating "undercover friending" through fake accounts, plaintiffs are unlikely to win legal challenges because the secrecy surrounding surveillance makes it nearly impossible to prove that such surveillance is conducted solely on account of the exercise of protected First Amendment rights.[96]

Likewise, the FBI reportedly closely monitors myriad groups of activists opposed to anti-Black racism, Islamophobia, and U.S. immigration policy.[97] Documents obtained through Freedom of Information Act ("FOIA") requests reveal a troubling criminalization of First Amendment-protected political dissent.[98] People associated with the Caravan Support Network are labeled anarchist extremists.[99] Activists engaged in the BLM movement are labeled

Dataminr to monitor in real-time more than 500 million daily tweets" and purchased SocioSpyder).

[93] JOHN LYNCH & JENNY ELLICKSON, U.S. DOJ, COMPUT. CRIME & INTELLECTUAL PROP. SECTION, OBTAINING AND USING EVIDENCE FROM SOCIAL NETWORKING SITES: FACEBOOK, MYSPACE, LINKEDIN, AND MORE (2020), https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf [https://perma.cc/7LA5-BKSX].

[94] Jon Schuppe, *Undercover Cops Break Facebook Rules to Track Protesters, Ensnare Criminals*, U.S. NEWS (Oct. 5, 2018, 6:08 AM), https://www.nbcnews.com/news/us-news/undercover-cops-break-facebook-rules-track-protesters-ensnare-criminals-n916796 [https://perma.cc/3VMD-BZ2V]. The use of informants to gather intelligence is not a violation of the Fourth Amendment, resulting in the admissibility of such evidence in a criminal prosecution. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 313-14 (1966).

[95] Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests*, THE INTERCEPT (Apr. 29, 2019, 11:25 AM), https://theintercept.com/2019/04/29/family-separation-protests-surveillance/ [https://perma.cc/8CD8-9QD9].

[96] Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151, 157 (2017) (noting that high-level secrecy of social media monitoring chills exercise of First Amendment rights).

[97] Chip Gibbons, *The FBI Is Setting Up a Task Force to Monitor Social Media*, THE NATION (Feb. 1, 2018), https://www.thenation.com/article/the-fbi-is-setting-up-a-task-force-to-monitor-social-media/; Jana Winter & Hunter Walker, *Document Reveals the FBI Is Tracking Border Protest Groups as Extremist Organizations*, YAHOO! NEWS (Sept. 4, 2019), https://news.yahoo.com/exclusive-document-reveals-the-fbi-is-tracking-border-protest-groups-as-extremist-organizations-170050594.html [https://perma.cc/5B8G-QLHW].

[98] *See* sources cited *supra* note 97 (describing FBI's targeting of political dissent).

[99] Winter & Walker, *supra* note 97 (stating that FBI considers such immigration groups to be anarchist extremist threats).

BIEs.[100] And Muslims who challenge U.S. foreign policy in Iraq, Somalia, Syria, Yemen, and other areas where foreign terrorist organizations operate are labeled Islamic extremists or violent extremists.[101] These labels trigger criminal investigations and prosecutions.

A. *Countering Violent Extremism*

The presumption that religious Muslims engaged in political dissent are susceptible to becoming terrorists undergirds the U.S. government's Countering Violent Extremism ("CVE") program. Since the September 11, 2001, terrorist attacks, Muslims have been the primary targets of U.S. counterterrorism enforcement—notwithstanding a rapid rise in right-wing extremism.[102] Pursuant to a preventive paradigm, law enforcement agencies at all levels of government surveil Muslims' lives in search of terrorist plots. Pervasive "Orientalist" and Islamophobic stereotypes cause agents to perceive religious activity as indicia of criminal intent.[103] When coupled with political beliefs critical of U.S. foreign policy or domestic government practices, a practicing Muslim is treated in ways eerily similar to Black political dissidents during the civil rights era (some of whom were also Muslim).

Informants or undercover agents infiltrate a Muslim's mosque, social groups, and political activities.[104] Rhetoric invoking Islamic tenets is treated as suspicious activity and consequently stored in a person's FBI and Department of Homeland Security ("DHS") files. A Muslim's financial transactions and international travel are scrutinized for any ties to terrorist suspects domestically or abroad.[105] The NYPD created the "Domain Awareness System" used to conduct targeted surveillance of Muslims by connecting databases of arrest

[100] BIE REPORT, *supra* note 33, at 3.

[101] *See* MITCHELL D. SILBER & ARVIN BHATT, NYPD INTELLIGENCE DIV., RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 31 (2007), http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf [https://perma.cc/JDC8-F2KN] (describing how Muslim political grievances between West and Middle East can lead to religious renewal and radicalization).

[102] *See generally* Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration Law After September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.U. ANN. SURV. AM. L. 295 (2002) (providing comprehensive analysis of disproportionately discriminatory effect that executive and legislative policies enacted after 9/11 had on Muslim populations within United States); Seth G. Jones, *The Rise of Far-Right Extremism in the United States*, CTR. FOR SECURITY & INT'L STUD. (Nov. 7, 2018), https://www.csis.org/analysis/rise-far-right-extremism-united-states [https://perma.cc/H8HH-M2SD].

[103] "Orientalism" refers to the master discourse theorized by Edward Said, which described how Occidental (or Western) scholars shaped ideas and images of the West in mirror opposite terms of the "Orient," which included the Muslim world. *See generally* EDWARD SAID, ORIENTALISM (1st ed. 1978).

[104] *See* Hassan v. City of New York, 804 F.3d 277, 285-86 (3d Cir. 2015).

[105] Sahar F. Aziz, *Caught in a Preventive Dragnet: Selective Counterterrorism in a Post-9/11 America*, 47 GONZ. L. REV. 429, 432, 441-42 (2011).

records, 911 calls, thousands of security cameras across New York City, license plate readers, and portable radiation detectors.[106] A similar program was created in San Francisco in 2005, under the rubric of domain management, that aimed to identify where Iranian immigrants lived in order to assign informants accordingly.[107]

This systematic focus on Muslim communities is normalized under the rubric of "Countering Violent Extremism" (the Bush Administration called the program "Countering Islamic Extremism," a name that the Trump Administration has revived).[108] In 2011, the Obama Administration published a counterradicalization strategy that acknowledged "the important role the Internet and social networking sites play in advancing violent extremist narratives."[109] As a result, the U.S. government planned to develop a separate, more comprehensive strategy for "countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience."[110]

Law enforcement agencies lead and fund CVE nationwide. Toward that end, the DHS, the FBI, and U.S. attorneys organize government meetings with Muslim communities across the country. They misrepresent such meetings as community engagement, when in fact the agencies' missions are to investigate, prosecute, and convict criminal suspects.[111] As a result, CVE is nothing more than a ruse to surveil Muslim communities and recruit informants.[112]

---

[106] Sara Kamali, *Informants, Provocateurs, and Entrapment: Examining the Histories of the FBI's PATCON and the NYPD's Muslim Surveillance Program*, 15 SURVEILLANCE & SOC'Y 68, 73 (2017) (describing how Domain Awareness System allows vast amounts of public data to be more easily accessed by counterterrorism police divisions).

[107] *Id.* (explaining use of Domain Awareness Systems in New York City); Carlos Torres, Azadeh Shahshahani & Tye Tavaras, *Indiscriminate Power: Racial Profiling and Surveillance Since 9/11*, 18 U. PA. J.L. & SOC. CHANGE 283, 294 n.80 (2015) (specifying that Chinese and Russian populations were also targeted because of their size and organization).

[108] Sahar F. Aziz, *Losing the 'War of Ideas:' A Critique of Countering Violent Extremism Programs*, 52 TEX. INT'L L.J. 255, 256-57 (2017) (stating that changing program's name reflects Trump Administration's desire to focus only on terrorism committed by Muslims).

[109] WHITE HOUSE, EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES 6 (2011), https://www.dhs.gov/sites/default/files/publications/empowering_local_partners.pdf [https://perma.cc/7ULJ-7DCQ].

[110] EXEC. OFFICE OF THE PRESIDENT, DEP'T OF HOMELAND SEC., STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES 20 (2011), https://obamawhitehouse.archives.gov/sites/default/files/sip-final.pdf [https://perma.cc/7VPL-AESV].

[111] *See generally* Khaled A. Beydoun, *Between Indigence, Islamophobia, and Erasure: Poor and Muslim in "War on Terror" America*, 104 CALIF. L. REV. 1463 (2016) (analyzing how CVE is disproportionately deployed within indigent, working-class, and heavily immigrant communities).

[112] *See generally* Aziz, *supra* note 30.

The White House Initiative on Countering Violent Extremism under President Obama expanded the online policing component. It sought to recruit family members, friends, or close acquaintances, because they "are the most likely to observe activities or behaviors suggesting an individual is being radicalized or has violent intent."[113] Accordingly, the government's CVE Interagency Task Force planned to "coordinate the development and dissemination of resources describing possible warning signs as well as steps families and friends can take if they believe someone close to them is becoming recruited or radicalized to violence."[114]

Critics of CVE warn that the government's criteria for suspicious behavior include Muslims' First Amendment-protected political dissent, religious belief and practice, and associations.[115] Benign activities—such as regularly attending dawn prayers, traveling to Yemen or Syria to visit family, sending remittances to family members abroad, or giving up smoking—are treated by police departments as indicia of suspicious activity warranting surveillance and investigation.[116] The most egregious case known so far involved the NYPD spying on mosques, cafes, cabdriver hangouts, Muslim student associations, Muslim nongovernmental organizations, hookah bars, and other places frequently visited by Muslims on the basis that such places are "radicalization incubators."[117]

---

[113] EXEC. OFFICE OF THE PRESIDENT, DEP'T OF HOMELAND SEC., STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES 11 (2016) [hereinafter 2016 STRATEGIC IMPLEMENTATION PLAN], https://www.dhs.gov/sites/default/files/publications/2016_strategic_implementation_plan_empowering_local_partners_prev.pdf [https://perma.cc/543M-M2HQ]; Melissa Sim, *Global Summit to Focus on Using Social Media to Battle Extremism*, ASIA ONE (Feb. 19, 2015), https://www.asiaone.com/world/global-summit-focus-using-social-media-battle-extremism [https://perma.cc/UHU7-Q4G9] (describing summit aimed to highlight domestic and international efforts to address terrorist-group recruitment via internet).

[114] 2016 STRATEGIC IMPLEMENTATION PLAN, *supra* note 113, at 11; *id.* at 2 ("Fundamentally, CVE actions intend to address the conditions and reduce the factors that most likely contribute to recruitment and radicalization by violent extremists. Where possible, CVE should be incorporated into existing programs related to public safety, resilience, inclusion, and violence prevention.").

[115] Aziz, *supra* note 108, at 263 ("Religious profiling, racialized counterterrorism enforcement, and discrimination against Muslims . . . infringe on the civil rights and liberties of Muslims . . . ."); Aziz, *supra* note 30, at 168 ("[A]ny law enforcement program defined by the ideology of the targets is flawed by design and a nonstarter, especially in light of the FBI's egregious violations of civil liberties . . . .").

[116] *See, e.g.*, SILBER & BHATT, *supra* note 101, at 31 (noting how radicalization may occur from traveling to Middle East or attending Islamic prayer services); *see also* Khaled A. Beydoun, *The Ban and the Borderlands Within: The Travel Ban as a Domestic War on Terror Tool*, 71 STAN. L. REV. ONLINE 251, 264-65 (2019).

[117] Torres, Shahshahani & Tavaras, *supra* note 107, at 292-93 (noting that FBI and other agencies engage in racial profiling by regularly mapping everyday activities of specific ethnic communities).

1. Online CVE Enforcement

Prior to the commercialization of social media in 2006, most government surveillance took the form of physical surveillance, wiretaps, strategically assigned and deployed informants, and searches of physical property.[118] Now, much of the intelligence gathered about Muslim activists and religious leaders is obtained through mining of social media data without the need for judicial warrants. Online counterradicalization programs[119] exploit "online content and interactions for the purpose of gathering information, gaining intelligence, and pursuing investigations."[120]

Criteria used to identify individual threats are being employed to search for Muslims and other minorities. For example, the Boston Police Department used Geofeedia to identify potential threats through social media searches of #MuslimLivesMatter and #ChapelHill, which were used to mobilize Muslims in protest of the killing of three Muslim students at the University of North Carolina.[121] Other keywords included terms commonly found in the news, such as al-Sham, Baghdadi, ISIL, ISIS, and Zawahiri, as well as common Islamic terms, such as *hijrah*, *kafir*, and *ummah*.[122] Not coincidentally, the hashtags circulated by Black activists, such as #BlackLivesMatter and #Ferguson, were also included in the police department's online search for threats.[123]

Online "counterradicalization" begins with undercover agents or informants surveilling targets based on Islam-related keywords or dissident speech

[118] *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (noting how "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes").

[119] Neumann, *supra* note 79, at 437-43 (detailing various components and types of counterradicalization programs).

[120] *Id.* at 433.

[121] Associated Press, *Social Media Surveillance Unfairly Targeted Muslims, Report Says*, FOX NEWS (Feb. 7, 2018), https://www.foxnews.com/tech/social-media-surveillance-unfairly-targeted-muslims-report-says [https://perma.cc/FWR7-JX2V] (noting that social media monitoring via Geofeedia has added little benefit to public safety while unfairly focusing on Muslims).

[122] *Id.* "Hijrah" means "migration" in Arabic and is used to reference the Prophet Muhammad's (PBUH) migration from Mecca to Medina in 622 AD to escape persecution. *Muhammad Completes Hegira*, HIST. (Feb. 9, 2010), https://www.history.com/this-day-in-history/muhammad-completes-hegira [https://perma.cc/5XMQ-Q7A2]. "Ummah" means "the community" in Arabic and is used to reference all Muslims in a particular city, country, or globally. *Ummah*, *supra* note 10. "Kafir" means "disbeliever" in Arabic. *Kafir*, OXFORD DICTIONARY OF ISLAM, http://www.oxfordislamicstudies.com/article/opr/t125/e1229 [https://perma.cc/348E-DT8Q] (last visited Apr. 16, 2020).

[123] *The Geofeedia Files: Boston Police and Social Media Surveillance*, PRIVACY SOS, https://privacysos.org/geofeedia-files-boston-police-social-media-surveillance/ [https://perma.cc/L6CD-57GD] (last visited Apr. 16, 2020).

referencing jihad, al-Qaeda, Hamas, ISIS, or other militant groups.[124] Counterradicalization then transitions to social media engagement for the purpose of gaining the unsuspecting target's trust.[125] Government agents declare their allegiance to ISIS and al-Qaeda as a means of urging the target to follow suit.[126] The agent then moves the conversation to a chat room or to direct communications to try to ensnare the target in a terrorist plot.[127] A number of these sting operations, which start by policing social media speech, have led to prosecution of online targets.[128] With entrapment laws firmly in favor of the government and a misplaced trust doctrine that legalizes the use of informants and undercover agents, Muslim activists are vulnerable prey for undercover agents and informants rewarded for catching terrorists online.[129]

In the international realm, the U.S. State Department's Center for Strategic Counterterrorism Communications ("CSCC") spearheads online policing of so-called "Islamic terrorists."[130] The CSCC "would use more than 350 State Department Twitter accounts, combining embassies, consulates, media hubs, bureaus and individuals, as well as similar accounts operated by the Pentagon, the Homeland Security Department and foreign allies."[131] Integral to the Pentagon's stated goal of streamlining countermessaging of foreign terrorists' propaganda, DHS and intelligence agencies are policing social media accounts that post content critical of the U.S. government and supportive of al-Qaeda, ISIS, and other militant groups in Muslim-majority countries.[132]

---

[124] *See* Associated Press, *supra* note 121 (reporting on Boston Police Department's use of program Geofeedia to conduct online surveillance targeting common Arabic words).

[125] Steven Brill, *Is America Any Safer?*, THE ATLANTIC (Sept. 2016), https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/.

[126] *Id.* ("Others argue that the FBI has overstepped constitutional boundaries in its drive to find out what people might be planning, often by entrapping suspected terrorists into actually creating attack plans they might otherwise never have thought of.").

[127] *Id.* ("Since 9/11 the FBI has organized more jihadist terror plots in the United States than any other organization." (quoting terrorism analyst Peter Bergen)).

[128] *See* Jack Healy & Matt Furber, *Convictions of 3 Linked to ISIS Put Community in a Spotlight*, N.Y. TIMES, June 4, 2016, at A9 (reporting on convictions of nine Minnesotans of Somali descent for supporting ISIS based on evidence obtained from online surveillance).

[129] Brill, *supra* note 125 (quoting former FBI director James Comey as stating that there have been many opportunities to try an entrapment defense in such cases, and none have been successful); *see also* United States v. White, 401 U.S. 745, 749-50 (1971) (reaffirming rule that there is no reasonable expectation of privacy for incriminating statements made to informant).

[130] Eric Draitser, *ISIS Online: A Pretext for Cyber COINTELPRO?*, GLOBAL RES. (Feb. 27, 2015), https://www.globalresearch.ca/isis-online-a-pretext-for-cyber-cointelpro/5433872 [https://perma.cc/W8ZY-DREA] (describing CSCC as coordinating existing counter-messaging efforts by Pentagon, Homeland Security, and intelligence agencies).

[131] Schmitt, *supra* note 80, at A1.

[132] FAIZA PATEL ET AL., BRENNAN CTR. FOR JUSTICE, SOCIAL MEDIA MONITORING: HOW THE DEPARTMENT OF HOMELAND SECURITY USES DIGITAL DATA IN THE NAME OF NATIONAL

2. Eroding Democracy

Democracies thrive when there is rigorous debate, access to information, free exchange of ideas, and government accountability. Government surveillance of such activities triggers a chilling effect. [133] Citizens self-censor out of fear that their expressed beliefs and political activities will invite government scrutiny that could adversely affect their lives.[134] Social media users aware that government surveillance occurs, therefore, are likely to exhibit restrictive deterrence whereby they refrain from lawful expressions of political dissent out of fear that such expressions will make them suspect.[135]

This is precisely what Justice Sonia Sotomayor warned in 2012 when she stated in her concurrence in *United States v. Jones*[136] that "[a]wareness that the government may be watching chills associational and expressive freedoms . . . [and may] alter the relationship between citizen and government in a way that is inimical to democratic society."[137] While the defendant's (successful) challenge of the warrantless use of GPS tracking technology is in some ways distinguishable from social media and was grounded in common law trespass doctrine, the harmful impact of government surveillance is the same.[138]

An empirical study by Professors Alexander O'Connor and Farhana Jahan found that "American [Muslims'] experiences with government surveillance are accompanied by increases in anxiety over future surveillance, avoidance discussing topics that may increase the possibility of surveillance, and avoidance of certain settings over concern it would lead to being reported to intelligence agencies."[139] Such coping mechanisms are consistent with the literature on

SECURITY 3 (2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf [https://perma.cc/6DZN-XYU2] (reporting on use of online surveillance by U.S. agencies related to immigration and travel to monitor foreign nationals from Muslim-majority countries).

[133] Elizabeth Stoycheff et al., *Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects*, 21 NEW MEDIA & SOC'Y 602, 611-12 (2019) (finding that knowledge of government surveillance chills American Muslims' online political speech).

[134] PATEL ET AL., *supra* note 132, at 3 (stating that fear of unfavorable visa determinations caused individuals to self-censor online). *See* Laird v. Tatum, 408 U.S. 1, 11 (1972) (discussing cases recognizing chilling effect where "the challenged exercise of governmental power was regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging").

[135] Stoycheff et al., *supra* note 133, at 611-12 (finding that individuals with knowledge of government surveillance were less likely to participate in online political speech).

[136] 565 U.S. 400 (2012).

[137] *Id.* at 416 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 565 U.S. 1189 (2012)).

[138] *See id.*

[139] Alexander J. O'Connor & Farhana Jahan, *Under Surveillance and Overwrought: American Muslims' Emotional and Behavioral Responses to Government Surveillance*, 8 J. MUSLIM MENTAL HEALTH 95, 101 (2014).

social-identity threat and stigma, which suggests that victims avoid behaviors, situations, or aspects of their identity that trigger negative stereotypes and discrimination.[140] Perceptions of government surveillance on account of religion also trigger anxiety among Muslims and adversely influence how they outwardly worship and outwardly express their religious identity and self-identity.[141] Muslims' sense of uncertainty and lack of control may also lead to higher levels of depression, paranoia, and disidentification with other Muslims.[142]

Self-censorship and chilling of dissent are consistent with political scientist Elisabeth Noelle-Neumann's spiral-of-silence theory.[143] She contends that individuals are motivated by fear of social isolation, and as a result they continuously monitor their environments to assess whether their beliefs align with or contradict the majority opinion.[144] The tendency of the person with a majority opinion to speak up and of the person with a minority opinion to be silent "starts off a spiraling process which increasingly establishes one opinion as the prevailing one."[145] As a result, "public opinion is the opinion which can be voiced in public without fear of sanctions and upon which action in public can be based."[146]

An empirical study on the impact of surveillance of social media users corroborates this phenomenon.[147] The study found that people were less likely to post a comment or to update their status with content with which they believed

[140] *Id.* at 97 (describing prior study demonstrating tendency of African Americans under surveillance to avoid showing interest in activities with which they are stereotypically associated). *See generally* SAHER SELOD, FOREVER SUSPECT: RACIALIZED SURVEILLANCE OF MUSLIM AMERICANS IN THE WAR ON TERROR (2018).

[141] *See* Khaled A. Beydoun, *Acting Muslim*, 53 HARV. C.R.-C.L. L. REV. 1, 50-63 (2018) (examining how Muslims perform religious identity in line with disincentives associated with war on terror suspicion and popular backlash).

[142] O'Connor & Jahan, *supra* note 139, at 96 (stating that government surveillance and post-9/11 discrimination caused American Muslims to experience "psychological distress").

[143] KEITH HAMPTON ET AL., PEW RESEARCH CTR., SOCIAL MEDIA AND THE 'SPIRAL OF SILENCE' 4 (2014), http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/ [https://perma.cc/B2QB-R39Q] (finding that Facebook and Twitter users were less likely to share their opinions regarding Edward Snowden leak online if they thought their followers were unlikely to agree).

[144] Elisabeth Noelle-Neumann, *The Spiral of Silence: A Theory of Public Opinion*, 24 J. COMM. 43, 43-44 (1974) (defining fear of isolation as fear of separation and "doubt about one's own capacity for judgment").

[145] *Id.* at 44.

[146] *Id.*

[147] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296, 298-99 (2016) (detailing study on social media users' willingness to post opinions on controversial national-security issues).

their followers would disagree.[148] When told the government was monitoring their social media, users became significantly less likely to speak out.[149] Their fear of isolation and social alienation thus extends to fear of authority and government.[150] That online expressions of opinion leave digital footprints traceable years later further exacerbates the spiral-of-silence effect.[151] Although more research is needed to understand the full extent of the chilling effect caused by online government surveillance, existing scholarship combined with preliminary empirical research about Muslims experiencing surveillance demonstrate the risks posed to First Amendment-protected activities and, by extension, to American democracy.[152]

B. *Black Identity Extremism*

Government surveillance of Muslims' online activism under CVE finds parallels in the surveillance of African Americans. Under the Black Identity Extremist ("BIE") designation revitalized by the FBI in 2017, a policing program has emerged in response to the on-the-ground and online resonance of the BLM movement.[153] The BLM movement inspired newfound consciousness and popular activism around police violence against Black communities.[154] The movement's success and appeal beyond traditional activist circles pushed the FBI to recreate the BIE designation, which cast Black activists that challenged police violence as presumptive extremists conspiring to engage in violent retribution against police officers.[155]

---

[148] *Id.* at 303.

[149] *Id.* at 307.

[150] *Id.*

[151] *Id.* at 298.

[152] *See* PATEL ET AL., *supra* note 132, at 4 (detailing DHS's use of social media to target protected protests).

[153] *See* BIE REPORT, *supra* note 33, at 7 (asserting that those under the BIE designation are likely to increase premeditated attacks against police officers in response to "perceptions of unjust treatment of African Americans").

[154] Justin Hansford, Opinion, *5 Years After Ferguson, We're Losing the Fight Against Police Violence*, N.Y. TIMES (Aug. 9, 2019), https://www.nytimes.com/2019/08/09/opinion/ferguson-anniversary-police-race.html.

[155] BIE REPORT, *supra* note 33, at 3. The BIE designation and policing had collateral effects. For example, it endorsed the Southern Poverty Law Center's "Black Nationalist" classification: "The black nationalist movement is a reaction to centuries of institutionalized white supremacy in America. Black nationalists believe the answer to white racism is to form separate institutions—or even a separate nation—for black people. Most forms of black nationalism are strongly anti-white and anti-Semitic." *Black Nationalist*, S. POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/ideology/black-nationalist [https://perma.cc/Q6YK-YNLP] (last visited Apr. 16, 2020) (listing Black Nationalist individuals and organizations as hate actors and groups).

1. Online BIE Enforcement

Like CVE, BIE surveillance is preventative in principle.[156] Subjects of interest have not committed a crime, and oftentimes they have not actively taken material steps toward plotting an attack against a police officer or engaging in a criminal act.[157] Despite the FBI's stated objective of preventing BIE attacks against police officers,[158] this aim may be a pretext to monitor and seek prosecution against Black activists through the prism of counterterrorism. Ostensibly, however, BIEs are not mere criminals, but rather, like their Muslim counterparts who are monitored through the lens of CVE policing, they allegedly are aspiring terrorists.

As a result, BLM activists who condemn police violence—on- and offline—are investigated as prospective terrorists depending on the gravity of their words, nature of their relationships, and organizational affiliations.[159] Through FBI tracking, the deployment of informants, and "rakers" that facilitate the collection of data about the subject's on- and offline activity,[160] BIE policing portrays a Black activist's political advocacy as tantamount to terrorism.[161]

---

[156] *See* Benjamin Fearnow, *FBI Ranks 'Black Identity Extremists' Bigger Threat than Al Qaeda, White Supremacists: Leaked Documents*, NEWSWEEK (Aug. 8, 2019, 4:41 PM), https://www.newsweek.com/fbi-leak-black-identity-extremist-threat-1453362 [https://perma.cc/D73B-S735] (reporting that FBI planned to use infiltration to mitigate BIEs' "existential threat" to domestic national security).

[157] George Joseph & Murtaza Hussain, *FBI Tracked an Activist Involved with Black Lives Matter as They Traveled Across the U.S., Documents Show*, THE INTERCEPT (Mar. 19, 2018, 11:29 AM), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/ [https://perma.cc/L4P5-9GRC].

[158] BIE REPORT, *supra* note 33, at 4 ("The FBI judges it is very likely BIE perceptions of police brutality against African Americans have become organizing drivers for the BIE movement since 2014, resulting in a spike of BIEs intentionally targeting law enforcement with violence.").

[159] Scott, *supra* note 96, at 153.

[160] "Rakers" are undercover police officers that infiltrate racial, religious, or activist communities. Their objective is to assimilate into these communities, build rapport with subjects of interest and their proxies, and directly collect or commission the collection of data on the subject of interest. *See generally* DIALA SHAMAS & NERMEEN ARASTU, MAPPING MUSLIMS: NYPD SPYING AND IMPACT ON AMERICAN MUSLIMS (2013) [hereinafter MAPPING MUSLIMS], https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf [https://perma.cc/RQ4G-LT59] (describing NYPD's use of rakers to monitor American Muslims from Philadelphia to New Haven).

[161] *See* Sam Levin, *Black Activist Jailed for His Facebook Posts Speaks Out About Secret FBI Surveillance*, THE GUARDIAN (May 11, 2018, 3:01 PM), https://www.theguardian.com/world/2018/may/11/rakem-balogun-interview-black-identity-extremists-fbi-surveillance [https://perma.cc/3U7X-J8XK] (reporting on failed prosecution of Rakem Balogun, Black activist portrayed in court by FBI as dangerous because of social media posts critical of police).

This is not only analogous to the philosophy of counterradicalization that drives modern CVE policing, but it is also identical to forms of preventative surveillance—most notably COINTELPRO—deployed against Black civil rights leaders and organizations in years past.[162] Shortly after the FBI renewed its BIE designation, Beydoun and law scholar Justin Hansford observed in *The New York Times*:

> [The BIE designation] could chill and criminalize a wide array of nonviolent activism in ways that have terrifying echoes [of] its infamous Cointelpro program, which investigated and intimated black civil rights groups and leaders, including Marcus Garvey and the Rev. Dr. Martin Luther King Jr. Under this program, F.B.I. agents concocted a false internal narrative connecting Dr. King to foreign enemies, allowing agents to justify threatening to publicize his private life and encouraging him to commit suicide. This is a reminder that while the "Black Identity Extremist" designation is new, the strategy of using a vague definition to justify broad law enforcement action is not.[163]

Through its BIE designation, the FBI has framed Black activists as a monolithic bloc that could instantly turn violent.[164] Unabashedly, this caricature seized upon vile stereotypes of Black identity, which shaped the FBI thought about Black dissidence at the height of the civil rights movement.[165] With its BIE label, "[n]ot only did the FBI create an entire movement based on race and give it a moniker that has only ever been used by law enforcement, it had to reach forty years into the past to connect its fictional movement" to Black dissident groups of the 1960s.[166]

By dangerously fusing an overbroad classification that caricatures Black activists as potential terrorists with the vague label of extremism,[167] BIE policing poses a range of civil liberty and security threats that unfold on- and offline.

2. Chilling Online Activism

As noted in Part I, activism and advocacy are as robust online as they are in traditional public forums. This is especially true for the BLM and ancillary movements, which fueled the popularity of online activism in the United States

[162] Khaled A. Beydoun & Justin Hansford, Opinion, *The F.B.I.'s Dangerous Crackdown on 'Black Identity Extremists*,*'* N.Y. TIMES (Nov. 15, 2017), https://www.nytimes.com/2017/11/15/opinion/black-identity-extremism-fbi-trump.html.

[163] *Id.*

[164] *See id.* (arguing that BIE designation "erroneously presumes a broad and disparate group of organizations with concerns about the criminal justice system represent a movement with a unifying ideology").

[165] *See id.* (identifying origins of BIE designation as arising from stereotype of Black violence).

[166] Hansford, *supra* note 36, at 703-04 (footnote omitted).

[167] Beydoun & Hansford, *supra* note 162 (listing troubling potential outcomes of BIE designation).

over the past decade.[168] By describing "a broad and disparate group of [Black] organizations with concerns about the criminal justice system [as a] movement with a unifying ideology,"[169] BIE policing threatens online activism in a myriad of ways.

The speech published and activism performed on social media platforms invites BIE surveillance and suspicion.[170] In part, the FBI introduced BIE policing as a response to the success of online advocacy addressing (anti-Black) police violence,[171] and it created new mechanisms for the virtual dragnet that descends upon the profiles and pages of online activists. Largely unaware that their online activism is being monitored—and even more unaware of the existence of BIE policing—users freely post content and avail their unfiltered views about police violence and more to suspecting FBI eyes. And, in doing so, they make the once-difficult task of collecting data about subjects of interest very easy for the FBI and their virtual interlocutors.[172]

BIE surveillance has spawned FBI prosecutions. Rakem Balogun, a Black activist from Dallas, Texas, was arrested and prosecuted for domestic terrorism in December 2017.[173] The IT professional and Second Amendment advocate was arrested shortly after publishing posts on Facebook stating that he saw signs at a rally with the words "the only good pig is a pig [police officer] that's dead" and expressing his belief that "[t]hey deserve what they got"[174] with regard to the killing of a Dallas police officer.[175] Balogun claims that he was "venting" online about his frustration with the wave of police killing unarmed Black women and men.[176] Despite their distasteful nature, Balogun's statements presented no evidence of any inclination on his part to attack a member of law enforcement. Nor did his statements indicate a direct connection with any organization or outfit that set out to attack police officers. In short, Balogun was

[168] *See generally* FREELON, MCILWAIN & CLARK, *supra* note 24 (describing online development of BLM and related movements).

[169] Beydoun & Hansford, *supra* note 162.

[170] Levin, *supra* note 161 (reporting that Black activist's Facebook posts criticizing police led to BIE surveillance and attempted prosecution).

[171] *See* BIE REPORT, *supra* note 33, at 3 (identifying Ferguson as origin of supposed rise of concerted violence against law enforcement and using such rise to justify BIE designation). The FBI would not directly acknowledge this, but the timing of its report and commitment to investigating BIEs came at the very height of the BLM movement's appeal and resonance.

[172] Beydoun & Hansford, *supra* note 162 (arguing that BIE policing "pave[s] the way for [the FBI] to gather data on, monitor and deploy informants to keep tabs on individuals and groups it believes to be B.I.E.s").

[173] Levin, *supra* note 161.

[174] *Id.*

[175] "On 7 July 2016, Micah Johnson ambushed and shot 11 law enforcement officers, killing five, in downtown Dallas, Texas, during a First Amendment protected protest . . . ." BIE REPORT, *supra* note 33, at 4. Balogun attended this very protest, which spurred the FBI's suspicion after his Facebook posts deriding police. Levin, *supra* note 161.

[176] Levin, *supra* note 161.

punished because of his online speech and community-organizing work, which called into question the recurring incidence of police killing Black people.[177] His Blackness activated the perceived menace of his online content and spurred the FBI to label him a BIE.[178]

Balogun's experiences illustrate the perils online activists face in the form of intensified surveillance and BIE prosecution. However, in addition to online activism attracting the attention of FBI agents, the looming fear of BIE surveillance also chills online advocacy. At the extreme, it may even spur Black activists to completely divest from online advocacy. In an essay critiquing how the First Amendment right to assembly is unequally extended and oftentimes denied to Black activists, Hansford observes, "Perhaps even more effective than curbing freedom of assembly on the streets is destroying these civil society organizations from the inside so that no one is organized enough to take to the streets to begin with."[179] Although concerned with assembly within traditional public forums, Hansford makes two observations salient to this Article's focus on speech within private virtual forums: First, intensified policing of Black activists online erodes their speech by chilling virtual activism and pushing users to divest wholly from it.[180] Second, BIE policing online aspires to breed mistrust and division within Black activist organizations and communities.[181]

Mirroring sentiments within the Muslim community regarding CVE, Black activists contend that BIE policing's genuine objective is to "monitor, disrupt, and divide" advocacy communities and organizations.[182] Past surveillance programs, like COINTELPRO,[183] wielded phone tapping and wire surveillance

[177] "For many black people, already accustomed to being uniquely vulnerable to police violence, the fear is that being viewed as potential terrorists for expressing legitimate political grievances might give police license to target them even more intensely than they already do." Alice Speri, *Fear of a Black Homeland: The Strange Tale of the FBI's Fictional "Black Identity Extremism" Movement*, THE INTERCEPT (Mar. 23, 2019, 8:31 AM), https://the intercept.com/2019/03/23/black-identity-extremist-fbi-domestic-terrorism/ [https://perma.cc /8XA6-SHSR].

[178] Balogun is the first publicly known individual to be arrested on BIE grounds. *See* Jacob Vaughn, *Dallas Activist May Be First Labeled "Black Identity Extremist" by FBI*, DALL. OBSERVER (July 31, 2019, 4:00 AM), https://www.dallasobserver.com/news/dallas-activist-rakem-balogun-may-be-first-targeted-under-fbis-new-black-identity-extremist-threat-label-11705688 [https://perma.cc/NV9T-6EUV].

[179] Hansford, *supra* note 36, at 704.

[180] *See id.* (warning that FBI surveillance could "chill and criminalize [Black] activists and protesters").

[181] *See id.* ("Perhaps even more effective than curbing freedom of assembly on the streets is destroying these civil society organizations from the inside so that no one is organized enough to take to the streets to begin with.").

[182] Beydoun & Hansford, *supra* note 162.

[183] One commentator dubbed BIE policing "COINTELPRO 2017." *See* Robyn C. Spencer, *Black Identity Extremists: COINTELPRO 2017*, BLACK PERSP. (Nov. 13, 2017), https://www.aaihs.org/black-identity-extremists-cointelpro-2017/ [https://perma.cc/2NBL-

to collect data on subjects of interest to advance criminal cases, but they also stirred up dissension and discord within Black organizations and communities. These aims, history reveals, are not separate but entwined objectives intended to stifle movements that challenge the state and punishing individuals who are materially connected to the movements or voicing support for overlapping demands for justice online.[184]

C. *Vulnerable Targets*

Online activists within the Black and Muslim communities are a heterogeneous population. Twenty-five percent of the Muslim population in the United States identify as Black,[185] comprising the largest plurality of the broader faith group. Thus, Black Muslims comprise one of the most vulnerable targets of online surveillance. Black Muslim online activists occupy an intersection where they are simultaneously susceptible to CVE and BIE surveillance[186] and to the monitoring of FBI agents and informants deployed by each program.[187] Furthermore, today's political activism reflects the unique challenges faced by Black Muslims and illustrates how Islamophobia shapes anti-Black racism inflicted by state actors (including the police) and private citizens.[188]

K6CF] (discussing links between BIE policing today and COINTELPRO policing by the FBI in the 1960s and 1970s).

[184] COINTELPRO was invested in "undermining and eradicating groups, movements, and individuals — almost all of which were part of the Left — it viewed as threats to national security and social order." Branko Marcetic, *The FBI's Secret War*, JACOBIN (Aug. 31, 2016), https://www.jacobinmag.com/2016/08/fbi-cointelpro-new-left-panthers-muslim-surveillance [https://perma.cc/VQD9-P7XL].

[185] DALIA MOGAHED & YOUSSEF CHOUHOUD, INST. FOR SOC. POLICY & UNDERSTANDING, AMERICAN MUSLIM POLL 2017: MUSLIMS AT THE CROSSROADS 9 (2017), https://www.ispu.org/american-muslim-poll-2017/ [https://perma.cc/AL4T-KCQV].

[186] Here, we use the term "intersection" in reference to Professor Kimberlé Crenshaw's theory of the phenomenon of intersectionality, whereby individuals with multiple subordinated identities occupy challenging social, cultural, and political circumstances. *See* Kimberlé Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color*, 43 STAN. L. REV. 1241, 1244-45 (1991) (discussing how race and gender intersect with other aspects of life, such as politics or physical location, resulting in women of color's experiences qualitatively differing from those of white women and men of color).

[187] The FBI designated Black Muslim groups as being of special BIE interest, specifically Black Moors. *See* BIE REPORT, *supra* note 33, at 4, 6.

[188] *See* Emmanuel Mauleón, *Black Twice: Policing Black Muslim Identities*, 65 UCLA L. REV. 1326, 1331-33 (2018) (investigating how Black Muslim populations face multiple forms of counterterror policing on account of their combined racial and religious identity). *See generally* Donna Auston, *Mapping the Intersections of Islamophobia & #BlackLivesMatter: Unearthing Black Muslim Life & Activism in the Policing Crisis*, SAPELO (May 19, 2015), https://sapelosquare.com/2015/05/19/mapping-the-intersections-of-islamophobia-blacklivesmatter-unearthing-black-muslim-life-activism-in-the-policing-crisis/ [https://perma.cc/NCT3-X9YE] (addressing how Islamophobia and anti-Black racism

Youth and young adults who engage in online activism are another disproportionately vulnerable group.[189] As examined in Part I, younger generations are more entrenched in the culture of online activism and have been instrumental in spearheading online political campaigns and movements. Despite their online acumen, young activists are especially vulnerable to the virtual traps of CVE and BIE surveillance for two reasons.

First, although young activists may be broadly aware of the phenomenon of online surveillance, they are largely unaware of the existence and architecture of CVE and BIE policing. This ignorance can be especially dangerous on several fronts of the online landscape. It disarms young activists when engaging with unknown elements online, particularly within the "direct messages" feature of social media platforms, where clandestine FBI agents or informants can fluidly discuss topics that entrap or incriminate. Young activists unaware of CVE and BIE surveillance are naturally ignorant of the "triggers" that induce FBI suspicion,[190] and thus they freely post without strategically filtering out language in their public content.

Second, young activists are more inclined to engage in more zealous online activism. For younger generations, the internet and social media platforms are not necessarily realms for escape but extensions of their on-the-ground daily experience and daily lives.[191] Young activists use social media platforms, like Facebook and Twitter, as vehicles for political venting and catharsis, which often manifests in overzealous content that, for Black and Muslim youth, can attract the watchful eyes of FBI agents. While political and popular debates about online speech rage forward, the prevailing reality for young Black and Muslim activists is that unfiltered online advocacy can and does spur CVE and BIE investigations.

III. PERILS AND PRESCRIPTIONS

Rapid technological innovation has expanded law enforcement's surveillance capabilities. No longer limited to physical surveillance, informants, and wiretaps,[192] the government can now secretly collect intimate details about people's lives from social media activity—all without a warrant. While the

function to simultaneously stigmatize Black Muslims and erase them, their experiences, and their narratives from the broader discussion of Muslim life in United States). For an analysis of CVE's impact on Black populations, see Beydoun, *supra* note 111, at 1474-77.

[189] For brevity, this Article identifies these demographics as "young activists."

[190] By "triggers," we are referring to words, images, or content that have a capacity for enhancing the prospect of CVE or BIE suspicion. For example, Balogun referring to the man who killed a policeman as a "hero" would be considered a trigger. Levin, *supra* note 161.

[191] *See* Fatimah Awan & David Gauntlett, *Young People's Uses and Understandings of Online Social Networks in Their Everyday Lives*, 21 J. INDEXING & METRICS 111, 127 (2013).

[192] For a leading history of police surveillance in the United States that precedes modern technological developments, see generally GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988).

means of surveillance have changed, the victims have not. Racial and religious minorities continue to be targets under the guise of national security. And Fourth Amendment jurisprudence and statutory privacy laws appear to grant law enforcement expansive powers to spy on these communities.

But just as social media has served as a sword for government surveillance, it is also a shield that citizens use to expose government abuse and shape public opinion to reform government. In contrast to largely unfavorable court rulings circumscribing privacy rights, grassroots mobilization to legislate privacy protections may be the most effective prescription to restore curtailed Fourth Amendment rights.

A. *Doctrinal Failures in Protecting Online Activism*

The Supreme Court's Fourth Amendment jurisprudence has yet to evolve to shield social media users from government surveillance of their speech and associations for law enforcement purposes. Three doctrinal impediments—the open fields, misplaced trust, and third-party doctrines—result in courts finding no reasonable expectation of privacy in communications to the public; undercover agents; or third-party companies, such as Facebook, Instagram, and Twitter.[193]

1. Open Fields Doctrine

In 1924, the Supreme Court in *Hester v. United States*[194] established the open fields doctrine in a case where officers submitted into evidence a jug of illegal moonshine that the defendant had abandoned on his front lawn.[195] The Court denied the defendant's motion to exclude based on its finding that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects' is not extended to the open fields."[196] The open fields doctrine thus allows law enforcement to collect information from social media posts and forums accessible by the general public or large groups of people without the need for a search warrant. In making these posts publicly available, the user as effectively waived her privacy rights.

---

[193] *See* United States v. Miller, 425 U.S. 435, 444 (1976) (holding that Fourth Amendment does not protect documents furnished to third party); United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (finding that defendant's reasonable expectation of privacy on social media ended when he disseminated posts to his "friends"); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1118-21 (2014).

[194] 265 U.S. 57 (1934).

[195] *Id.* at 58.

[196] *Id.* at 59 (quoting U.S. CONST. amend. IV); *see also* Oliver v. United States, 466 U.S. 170, 177 (1984) (citing Katz v. United States, 389 U.S. 347 (1967)) (reaffirming *Hester* and finding that Court's decision in *Katz* does not affect the open field doctrine because there is no reasonable expectation of privacy in public spaces).

2. Misplaced Trust Doctrine

Four decades later, in *Hoffa v. United States*,[197] the Supreme Court issued another seminal Fourth Amendment decision. Teamsters union leader James "Jimmy" Hoffa was convicted of bribing members of a jury in a previous criminal case against him. Hoffa had confided in his colleague, Edward Partin, about his jury tampering. Partin turned out to be a government informant. In challenging the admissibility of Partin's testimony, Hoffa argued that "Partin's failure to disclose his role as a government informer vitiated the consent that the petitioner gave to Partin's repeated entries into the suite, and that by listening to the petitioner's statements Partin conducted an illegal 'search' for verbal evidence."[198] The Court found that Hoffa's misplaced trust in his colleague did not nullify his voluntary disclosure of information to another person who may share it with others, reasoning that this "is the kind of risk we necessarily assume whenever we speak."[199] In the context of online activism, the misplaced trust doctrine permits prosecutors to use information gathered by informants and undercover agents through fake accounts and false identities.[200] So long as the basis for targeting a particular user or group is not *solely* on account of First Amendment-protected activities, which do not include criminal behavior, the use of informants online is as lawful as their use in person.[201]

3. Reasonable Expectation of Privacy Doctrine

In the seminal Fourth Amendment case *Katz v. United States*,[202] the Supreme Court ruled on the warrantless use of an electronic listening and recording device attached to the outside of the telephone booth from which the defendant had made calls.[203] In finding the government's eavesdropping unconstitutional, Justice Harlan's concurring opinion established the reasonable expectation of privacy doctrine. Specifically, it found that the Fourth Amendment "protects people, not places," and thus the trespass doctrine as applied in Fourth Amendment claims was no longer controlling.[204] The expectation of privacy must be subjectively and objectively reasonable in order for a court to find evidence inadmissible.[205] The *Katz* Court also reaffirmed the open fields

[197] 385 U.S. 293 (1966).

[198] *Id.* at 300.

[199] *Id.* (quoting Lopez v. United States, 373 U.S. 427, 465 (1963)) (citing Lewis v. United States, 385 U.S. 206 (1966)).

[200] *See* Semitsu, *supra* note 86, at 346-49.

[201] *Id.*

[202] 389 U.S. 347 (1967).

[203] *Id.* at 351.

[204] *Id.*; *see* Olmstead v. United States, 277 U.S. 438, 465 (1928), *overruled by Katz*, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[205] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

doctrine, stating, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[206]

4. Third-Party Doctrine

Since the *Katz* decision, courts have wrestled with establishing a consistent standard for examining whether information or items collected are subject to a reasonable expectation of privacy to require a search warrant. The doctrine became increasingly untenable as technology rapidly evolved and things like telephones and televisions became ubiquitous. In two seminal Fourth Amendment cases—*United States v. Miller*[207] in 1976 and *Smith v. Maryland*[208] in 1979—the Supreme Court established the third-party doctrine. According to this doctrine, information voluntarily submitted to a third party—in these cases banks and telephone companies, respectively—is not subject to Fourth Amendment protection because there is no reasonable expectation of privacy.[209] Put simply, if a customer gives information to a bank, telephone company, internet service provider, or other business, then she has waived any privacy rights to such information.

In the era of "big data" and the ubiquity of technology, the obvious problem with the third-party doctrine is the Hobson's choice it poses. A person either has to completely disconnect from society in order to preserve his privacy or live in the real world of electronic information to receive basic services yet forfeit nearly all of his privacy. For this reason, Justice Sotomayor pointedly stated in her concurrence in *Jones* that the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[210] Justice Alito recognized this problem but argued that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[211]

5. The Stored Communications Act

Unfortunately, Congress has thus far failed to amend the Electronic Communications Privacy Act of 1986 ("ECPA") in response to these privacy

[206] *Id.* at 351 (majority opinion).

[207] 425 U.S. 435 (1976).

[208] 442 U.S. 735 (1979).

[209] *Id.* at 744-46 (applying third-party doctrine to use of pen registers to record phone numbers dialed by defendant); *Miller*, 425 U.S. at 443-34 (applying third-party doctrine to bank records).

[210] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); Semitsu, *supra* note 86, at 301 (noting that information collected by Facebook is disseminated to approximately 500,000 third-party application developers).

[211] *Id.* at 429 (Alito, J., concurring).

concerns. The ECPA amended the Wiretap Act[212] and created the Stored Communications Act ("SCA")[213] and the Pen Register Act.[214] The SCA, which most squarely implicates online activism, limits the type of electronic communications the government can access without a warrant. Under § 2703, the government cannot access the content of an email sent within the past 180 days without a warrant if it is stored on a third party's server.[215] If it seeks content of emails older than 180 days, it can do so through a subpoena, but the user must be notified of the request, which allows for the opportunity to quash the subpoena in court.[216] Noncontent information, such as websites visited and email addresses of persons with whom the user corresponded, is accessible with a warrant or via a court order.[217] However, the order is issued pursuant to the lower standard of "specific and articulable facts showing that there are reasonable grounds to believe" the records requested are "relevant and material to an ongoing criminal investigation."[218]

Because the SCA was passed twenty years before Twitter and Facebook were publicly launched, the law is woefully outdated.[219] Courts have struggled to determine whether the SCA applies to social media posts to a private group, posts visible only to friends on the user's account, and to private messages.[220] The reasoning often centers on whether there is a reasonable expectation of privacy notwithstanding the user's disclosure of information to third parties such as Facebook, Twitter, and other social media services.[221] In *Warshak v. United States*,[222] the Sixth Circuit in part upheld the constitutionality of § 2703 of the SCA but declared the SCA unconstitutional to the extent that it allows warrantless seizure of email.[223]

Although the Supreme Court has yet to rule on a Fourth Amendment case involving social media information, lower courts in civil cases have held that private and direct messages in social media forums are subject to SCA protection. In *Crispin v. Christian Audigier, Inc.*,[224] a federal district court in California held that private messages are the functional equivalent of emails,

[212] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, secs. 101-110, §§ 2232, 2510-2514, 2516-2521, 3117, 100 Stat. 1848, 1848-59 (codified as amended in scattered sections of 18 U.S.C.).

[213] *Id.* § 201, 100 Stat. at 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2710).

[214] *Id.* § 301, 100 Stat. at 1868-72 (codified as amended at 18 U.S.C. §§ 3121-3126).

[215] 18 U.S.C. § 2703(a) (2018).

[216] *Id.* § 2703 (b)(1)(B)(i).

[217] *Id.* § 2703 (c)(1).

[218] *Id.* § 2703 (d).

[219] *See* Borchert, Pinguelo & Thaw, *supra* note 86, at 36.

[220] *Id.* at 59.

[221] *Id.* at 58.

[222] 532 F.3d 521 (6th Cir. 2008) (en banc).

[223] *Id.* at 523.

[224] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

such that disclosure requires the user's consent.[225] Although *Crispin* was a civil suit, its holding would require a judicial warrant in criminal cases where the government wants the content of private messages sent within the previous 180 days or a subpoena for messages older than 180 days. Left unanswered in the *Crispin* decision is whether posts in private groups or to a limited number of people on social media are subject to the SCA or are treated as not subject to privacy protections pursuant to the open fields doctrine.

That same year, the Suffolk County Supreme Court of New York found in *Romano v. Steelcase Inc.*[226] that social media postings to a limited number of people are not subject to privacy protections because the user has assumed the risk that those persons may share the posts with others.[227] As a result, there is no reasonable expectation of privacy that would bar a civil litigant from obtaining the information by way of a subpoena. The same reasoning could apply in a criminal case in which the prosecutor requests from Facebook and Twitter social media posts sent by the defendant to a limited number of people.

B. *Local Grassroots Initiatives to Regulate Police Online Surveillance*

Due to these numerous doctrinal limitations, privacy advocates have recommended a federal regulation that would require a warrant for data analysis of information collected from public surveillance.[228] Absent a federal law, legal challenges in court turn on whether social media users can prove the government's surveillance is based on race, religious affiliations, political beliefs, associations, or other statuses protected by the First and Fourteenth Amendments. In the rare instances when plaintiffs can garner the evidence to prove unlawful intent, they must still show harm beyond a subjective chilling. The Supreme Court in *Laird v. Tatum*[229] found that the plaintiff had no standing because he could not show "specific present objective harm or a threat of specific future harm" arising from the Army's large-scale data gathering program in the 1960s.[230]

However, if Muslims and Black activists can show that the government's online surveillance caused them to decrease their political organizing and activism as well as self-censor, then they may be successful in their constitutional legal challenges. This was the Third Circuit's reasoning in *Hassan v. City of New York*[231] in finding that the plaintiffs' religious affiliation was a

[225] *Id.* at 973 & n.17.

[226] 907 N.Y.S.2d 650 (Sup. Ct. 2010).

[227] *Id.* at 433-34.

[228] Scott, *supra* note 96, at 163 ("At the federal level, a straightforward regulation should be implemented that requires a warrant to perform data analysis of information collected through mass public surveillance.").

[229] 408 U.S. 1 (1972).

[230] *Id.* at 14.

[231] 804 F.3d 277 (3d Cir. 2015).

substantial factor in the police department's selection of surveillance targets.[232] The court noted, "*Laird* doesn't stand for the proposition that public surveillance is either *per se* immune from constitutional attack or subject to a heightened requirement of injury . . . ."[233]

While courts have offered little relief, challenges to online surveillance at the local level, where community organizations have mobilized to promote legislation regulating police surveillance, have been more successful. In Oakland, California, grassroots organizations successfully lobbied for passage of a new ordinance that requires the police department to submit "technology impact reports" to Oakland's Privacy Advisory Commission.[234] The reports disclose adoption of any new surveillance technologies, such as cellphone trackers or license plate readers.[235] Citizens can then partake in decision-making on whether such technologies should be used in their communities.

The discovery of social media monitoring by various police departments has also led to the creation of a multicity legislative initiative by a coalition of national advocacy organizations called the Community Control Over Police Surveillance ("CCOPS").[236] CCOPS seeks to pass local laws that increase transparency and restrain police surveillance, including use of undercover social media accounts.[237] Such laws, if adopted, would redefine the expectation of privacy to bar indiscriminate social media monitoring, impose public oversight, and regulate the usage of new technologies. They would prohibit law enforcement's collection or sharing of social media content regarding people not

[232] *Id.* at 292.

[233] *Id.*

[234] Sidney Fussell, *Oakland Passes Nation's Strongest Surveillance Technology Ordinance Yet*, GIZMODO (May 2, 2018, 6:10 PM), https://gizmodo.com/oakland-passes-nations-strongest-surveillance-technolog-1825725697 [https://perma.cc/U6DX-55MY] ("Oakland police and other city agencies will have to submit a 'technology impact report' to Oakland's Privacy Advisory Commission if they plan to implement new surveillance technologies, like license plate readers or cellphone trackers.").

[235] Scott, *supra* note 96, at 162 (discussing Oakland ordinance designed to limit unneeded mass surveillance by requiring public comment before deploying new surveillance technology).

[236] *See* Laura Hautala, *These Laws Make Police Get Public Buy-in on Surveillance Tools*, CNET (May 28, 2019, 5:00 AM), https://www.cnet.com/news/these-laws-make-police-get-public-buy-in-on-surveillance-tools/ [https://perma.cc/S3HS-DLJF] ("Many of the community oversight laws are based on Community Control over Police Surveillance, or CCOPS, a legal model designed by the American Civil Liberties Union.").

[237] Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU (Sept. 22, 2016, 2:45 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software [https://perma.cc/D2EB-Y9A8] ("The ACLU of California has received thousands of pages of public records revealing that law enforcement agencies across the state are secretly acquiring social media spying software that can sweep activists into a web of digital surveillance.").

suspected of specific, articulable criminal activity. Nor would social media surveillance based on race, religion, national origin, or protected speech and association be legally permissible under these proposed local laws. The end result would be citizens taking control over whom the government can subject to surveillance rather than relying on courts.

While local communities are pursuing different strategies for holding their police departments accountable for online policing, federal law enforcement remains largely untethered by law. Until a systematic approach is adopted, Muslim and Black communities will remain the "usual suspects" targeted in a burgeoning online policing paradigm.

CONCLUSION

"[T]ruth's a menace, science is a public danger. As dangerous as it's been beneficent."

—ALDOUS HUXLEY, BRAVE NEW WORLD[238]

Popular and scholarly debate rages forward about whether social media has brought, on balance, more good than bad—more danger or beneficence—for individuals and society at large.[239] There is, perhaps, no definitive response to this question, largely because this brave new virtual world may very well still be in its infancy and is poised to become far more advanced and encompassing.

What we do know, through the marshaling of surveillance programs like CVE and BIE policing online, is that this question of beneficence and danger may hinge squarely on the subject. Posed to the counterterror arms of the state, the answer is clear: the virtual world—by exposing the various forms of activism within it—has made their job of monitoring, data collection, and informant deployment far more efficient and effective. However, when posed to the targets of online policing, the response—if the individual is even cognizant of the existence of CVE or BIE programs—is riddled with accounts of anxiety, fear, and danger.

Amid the perils posed by virtual surveillance, the positive impact of online activism cannot be denied. The BLM movement and the ancillary and individual advocacy it inspired[240] have mainstreamed a new consciousness against anti-Black racism in the United States and beyond. For Muslim activists, social media platforms have afforded a "new source of public opinion and citizen

[238] ALDOUS HUXLEY, BRAVE NEW WORLD 234 (Harper Perennial 1989) (1932).

[239] For a critical assessment of social media speech, see generally Kyle Langvardt, *A New Deal for the Online Public Sphere*, 26 GEO. MASON L. REV. 341 (2018), in which the author highlights false news, private censorship, ideological polarization, and online addiction as primary dangers arising from virtual speech.

[240] *See* FREELON, MCILWAIN & CLARK, *supra* note 24, at 5.

mobilization"[241] against the Islamophobia ushered in by populist politicians,[242] the threat of CVE in Muslim communities across the country, and other concerns, which may not have been possible without Facebook or Twitter. Yet for Black, Muslim, and other activists of color, the longstanding history of surveillance has followed them online.[243]

The truth may be menacing. Advances in digital science and the "datafication of our lives"[244] already foreshadow dangers that, on balance, may outweigh the benefits. On the one hand, these advances enable the freer use of words, activities, and associations, but on the other hand, they have been wielded as weapons against the online activist. This *brave new world* of online activism today, despite the transformative doors it opens for silenced and sidelined communities, has enabled the ubiquity of a policing presence once limited to the realm of fiction.

[241] Yang, *supra* note 18, at 35.

[242] For an analysis of how then-candidate Trump deployed Islamophobia as a campaign strategy to win the 2016 presidential election, see Khaled A. Beydoun, *"Muslim Bans" and the (Re)making of Political Islamophobia*, 2017 U. ILL. L. REV. 1733, 1756.

[243] Scholars, including Hansford, have observed how white dissidents—and, more notably, white supremacists inclined toward violence—have hardly garnered the attention of law enforcement, offline or online. "Coextensive with the criminalization of racial justice protesters is the long history of state noninterference with the assembly rights of white supremacist actors." Hansford, *supra* note 36, at 705.

[244] Scott, *supra* note 96, at 163 (discussing potential downsides of heavy social media use and extensive data gathering performed on internet users).