Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State

HANNAH FUSON*

* Staff Member, Volume 49, and Senior Notes Editor, Volume 50, *The University of Memphis Law Review*; Juris Doctor Candidate, The University of Memphis Cecil C. Humphreys School of Law, 2020. Thank you to Nic Bradley for introducing me to the history of political surveillance in Memphis; to Naira Umarov, Professor Demetria Frank, Sarah V. Belchic, and Maggie McGowan Stringer for your thoughtful guidance while helping me develop this Note; to Thomas Greer, Nicole Milani, Caleb Sanders, and the Volume 50 Staff and Editorial Board for your invaluable assistance during the editing process; and to my parents, my friends, and Professor Amy Campbell for your constant support of my law school endeavors.

I. INTRODUCTION

Free political expression has been a core part of the American identity since the country's founding. Recognizing the importance of free speech and peaceful assembly to the survival of a democratic republic, the Framers of the United States Constitution enshrined these rights within the First Amendment.[1] The First Amendment thus empowers advocacy groups to organize and mobilize under the protection of law. But in practice, political protests often collide with another constitutional doctrine: the police powers of the State derived from the Tenth Amendment.[2] While law enforcement's ability to investigate crime is essential to protecting public welfare, current practices of police surveillance risk running afoul of the First Amendment's freedom of speech, association, and expression protections and the Fourth Amendment's protections against unreasonable searches and seizures.[3] This problem is illustrated by two events, almost forty years apart, which took place in Memphis, Tennessee.

---

1. The First Amendment reads, in pertinent part: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

2. The Tenth Amendment provides: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." *Id.* amend. X.

3. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* amend. IV.

During the Civil Rights Movement, the Memphis Police Department ("MPD") established a Domestic Intelligence Unit ("DIU") to monitor the activities of political activists.[4] From the mid-1960s until the mid-1970s, the DIU conducted surveillance and maintained files on activist groups of various socio-political creeds, most of which espoused anti-majoritarian views.[5] In 1976, Eric Carter, a Memphis State University[6] student, discovered that his roommate was an undercover police officer and that the DIU had been documenting his political activities as a Vietnam War protestor.[7] The revelation that the DIU had conducted further surveillance on additional activists soon followed.[8]

After MPD disbanded the DIU and began destroying its surveillance files, the American Civil Liberties Union of Tennessee ("ACLU of Tennessee") filed a class-action lawsuit in federal district court, *Kendrick v. Chandler* ("the *Kendrick* lawsuit").[9] The plaintiffs in the suit sought declaratory and injunctive relief from MPD's maintenance of files regarding non-criminal political activities, alleging that the DIU's surveillance practices violated the activists' First Amendment rights to "engage in lawful political expressions, associations[,] and assembly without being the objects of covert and overt surveillance . . .

4. *See* Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt at 3, Blanchard v. City of Memphis, No. 2:17-cv-2120-JPM-egb (W.D. Tenn. Aug. 10, 2018), ECF No. 120.

5. *See* Bruce Kramer, Surveillance of Protected First Amendment Activities: Kendricks v. Memphis Police Department (1978), https://www.aclu-tn.org/wp-content/uploads/2017/02/Kendrick-Summary.pdf (showing list of activist organizations under police surveillance).

6. Memphis State University is the former name of the University of Memphis. The University changed its name in 1994. *UofM History*, U. MEM., http://www.memphis.edu/about/umhistory.php (last visited Oct. 25, 2019).

7. Memorandum in Support of ACLU of Tennessee, Inc.'s Motion to Intervene as Plaintiff at 1, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-dkv (W.D. Tenn. June 30, 2017), ECF No. 12-1; Maria Hallas, *Victim of Illegal Police Surveilance Talks 40 Years Later*, LOCALMEMPHIS.COM (Mar. 9, 2017), https://www.localmemphis.com/news/local-news/victim-of-illegal-police-surveillance-talks-40-years-later/; *see also* Complaint at 6, Kendrick v. Chandler, No. 2-76-cv-00449 (W.D. Tenn. Sept. 14, 1976).

8. *See* Kramer, *supra* note 5 (describing the targeting of individuals involved in "Civil Rights, Union, and Negro Coalition activities").

9. *See* Complaint, *supra* note 7, at 1–11.

and without becoming the subjects of dossiers, reports[,] and files maintained by the [MPD]."[10]

In 1978, the court issued an Order, Judgment and Decree (the "Decree") that prohibited MPD from engaging in four categories of activities: (1) political intelligence;[11] (2) electronic surveillance for political intelligence;[12] (3) covert surveillance for political intelligence;[13] and (4) the harassment and intimidation[14] of any person exercising First Amendment rights. The Decree also provided regulations for permitted police conduct that might interfere with First Amendment rights, such as the maintenance and dissemination of information gathered during lawful criminal investigations.[15] The Decree, in full force and effect since September 14, 1978, remains active to this day. Almost forty

10. *Id.* at 4. The Complaint also alleged violations of Fourth Amendment rights to privacy and freedom from unreasonable searches and seizures; Fifth Amendment rights to privacy and due process; Ninth Amendment rights to privacy; and Fourteenth Amendment rights to due process, privacy, liberty, and equal protection. *Id*. at 7–8.

11. The Decree defines "political intelligence" as "the gathering, indexing, filing, maintenance, storage[,] or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations[,] or other exercise of First Amendment rights." Order, Judgment & Decree at 2, Kendrick v. Chandler, No. 2-76-cv-00449 (W.D. Tenn. Sept. 14, 1978). The Decree specifically prohibits MPD from "engag[ing] in political intelligence" and "operat[ing] or maintain[ing] any office, division, bureau[,] or any other unit for the purpose of engaging in political intelligence." *Id*. at 3.

12. The Decree specifically prohibits MPD from "intercept[ing], record[ing], transcrib[ing,] or otherwise interfer[ing] with any communication by means of electronic surveillance for the purpose of political intelligence." *Id.*

13. The Decree specifically prohibits MPD from "recruit[ing], solicit[ing], plac[ing], maintain[ing,] or employ[ing] an informant for political intelligence" and from "infiltrat[ing] or pos[ing] as a member of any group or organization exercising First Amendment rights [for the purpose of political intelligence]." *Id*.

14. The Decree prohibits four types of harassment or intimidation: (1) "disrupt[ing], discredit[ing], interfer[ing] with or otherwise harass[ing] any person exercising First Amendment rights"; (2) "disseminat[ing] damaging, derogatory, false or anonymous information about any person for the purpose of political intelligence, or attempt[ing] to provoke disagreement, dissention or violence between persons"; (3) "engag[ing] in any action for the purpose of, or reasonably having the effect of, deterring any person from exercising First Amendment rights"; and (4) "at any lawful meeting or demonstration, for the purpose of chilling the exercise of First Amendment rights or for the purpose of maintaining a record, record[ing] the name of or photograph[ing] any person in attendance, or record[ing] the automobile license plate numbers of any person in attendance." *Id.* at 3–4.

15. *See id.* at 4–6 (prohibiting the maintenance and dissemination of information unless for lawful criminal investigations).

years later, the Decree became the focal point of a second challenge to the MPD's political surveillance practices.

In 2014, MPD purchased Geofeedia, a data collator program which allows the user to monitor the physical location and content of postings across a range of social media platforms.[16] Two years later, the MPD's Office of Homeland Security ("OHS") began issuing joint-intelligence briefings[17] (hereinafter "briefings") on individuals and groups engaged in protests against the police. Many of these individuals and groups were loosely associated with the national Black Lives Matter ("BLM") movement, which rose to prominence in 2014 after the fatal shooting of Michael Brown in Ferguson, Missouri.[18] Between June 2016 and March 2017, OHS used Geofeedia and other technologies to surveil the Memphis-based affiliates of "the organizations that arose out of Ferguson," such as "Black Lives Matter" and "Take ['Em] Down [901],"[19] despite an absence of threats against the police in Memphis from any of the identified groups.[20] The briefings contained information about protests, panels, and meetings, including those held

16. Brentin Mock, *Memphis Police Spying on Activists is Worse Than We Thought*, CITYLAB (July 27, 2018), https://www.citylab.com/equity/2018/07/memphis-police-spying-on-activists-is-worse-than-we-thought/566264/. Geofeedia sources location data from platforms such as Twitter, Instagram, Facebook, YouTube, Flickr, Picasa, Yik Yak, and Sina Weibo. *Geofeedia*, LEIU, https://leiu.org/content/geofeedia (last visited Aug. 19, 2019).

17. The briefings incorporated "four categories of information: (1) 'police shootings/deaths,' (2) 'riots/protests,' (3) 'Black Lives Matter,' and (4) 'officer safety.'" Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 12 (citation omitted).

18. In 2013, the Black Lives Matter movement organized in response to a growing public concern over police misconduct. *See Herstory*, BLACK LIVES MATTER, https://blacklivesmatter.com/about/herstory/ (last visited Oct. 26, 2019). The following year, Black Lives Matter engaged in a large-scale protest in response to Michael Brown's death in Ferguson, Missouri. Shannon Luibrand, *How a Death in Ferguson Sparked a Movement in America*, CBS NEWS (Aug. 7, 2015, 5:39 AM), https://www.cbsnews.com/news/how-the-black-lives-matter-movement-changed-america-one-year-later/. The Ferguson protests provoked a national conversation about racial policing. The protests have also been credited with increasing the mainstream media coverage of police-related fatalities. *See* Eliott C. McLaughlin, *We're Not Seeing More Police Shootings, Just More News Coverage*, CNN (Apr. 21, 2015, 7:26 AM), https://www.cnn.com/2015/04/20/us/police-brutality-video-social-media-attitudes/index.html.

19. Deposition of Stephen Chandler at 10–11, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. July 24, 2018).

20. *Id.* at 10.

on private property; photographs and information on those involved in protest movements based on social media postings; and sensitive or classified information such as drivers' licenses, juvenile arrest records, photographs, dates of birth, addresses, mental health histories, and information from police databases.[21] OHS circulated the contents of the briefings to factions within and outside of MPD, including the U.S. Military, the U.S. Department of Justice, the Tennessee Department of Homeland Security, the Tennessee Valley Authority, Shelby County Schools, and private companies such as FedEx, AutoZone, and St. Jude.[22] OHS also created and maintained a database and prepared PowerPoint presentations on individual activists and protest groups for the MPD training academy and Command Staff meetings.[23]

In addition, the MPD Real Time Crime Center ("RTCC") used the briefings to initiate investigations into protest activities via social media. The RTCC used Geofeedia and another program called NC4[24] to monitor the origin locations of "chatter" about protest events across a number of social media platforms.[25] MPD also used a fake Facebook account under the pseudonym "Bob Smith" to access private or restricted-access social media pages and an undercover cellphone number to correspond with activists directly.[26] In response to information obtained through social media, MPD conducted on-site surveillance of community meetings and vigils at churches, recorded all anonymous

21. Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 12–14; Plaintiff's Undisputed Statement of Material Facts at 4–5, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. July 24, 2018), ECF No. 107-2.

22. *Id.* at 12.

23. *Id.* at 11.

24. NC4 is another data-mining tool used by law enforcement agencies. *See, e.g.*, NC4, *Fort Myers Police Department chooses NC4 Street Smart to Help Fight Crime*, PR NEWSWIRE (Mar. 29, 2018, 9:37 AM), https://www.prnewswire.com/news-releases/fort-myers-police-department-chooses-nc4-street-smart-to-help-fight-crime-300621350.html.

25. Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 12.

26. *Id.* at 9–10; Plaintiff's Undisputed Statement of Material Facts, *supra* note 21, at 7–9.

calls asking about protest permits, and used an event-correlation program to create a map of associations between individuals and events entitled "Black Lives Matter."[27]

On December 19, 2016, a local BLM off-shoot group known as the Coalition of Concerned Citizens (the "CCC") staged a "die-in" protest on Mayor Jim Strickland's front lawn.[28] In response to the die-in, Mayor Strickland issued an Authorization of Agency ("AOA"), which empowered MPD to arrest the individuals listed on the AOA—without first warning Mayor Strickland—should they trespass on his property again.[29] The list on the AOA also included the CCC's known "associates in fact," which MPD determined based upon social media contacts, arrest records, and/or sightings at "unlawful assemblies."[30] As such, the AOA list was not limited to the individuals present at the die-in protest. MPD also added the names on the AOA list to the City Hall Escort List (the "Escort List"), a pre-existing list of individuals whom, based on prior disruptive behavior or a perceived willingness to engage in disruptive behavior, required monitoring to be present in Memphis's City Hall.[31] The release of the AOA and Escort List—dubbed "the blacklist" by activists and the press[32]—served as the catalyst for the second lawsuit in *Blanchard v. City of Memphis*.

---

27. Plaintiff's Undisputed Statement of Material Facts, *supra* note 21, at 7–9.

28. Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 8. A "die-in" is a form of nonviolent public protest in which participants simulate death to elicit feelings of grief or shock. *See* Marina Koren, *A Brief History of Die-In Protests*, CITYLAB (Dec. 4, 2014), https://www.citylab.com/equity/2014/12/a-brief-history-of-die-in-protests/383439/. First used by environmentalists in the 1970s, die-ins became much more common in the twenty-first century among groups such as BLM. *See id.*

29. Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 8 & n.4.

30. *Id.* at 8 & n.5.

31. *Id.* at 9.

32. *See, e.g.*, *Lawsuit Filed Over City Hall 'Blacklist' Alleges Unlawful Videotaping, Tracking of Activists*, WMC ACTION NEWS 5 (Feb. 22, 2017, 9:12 PM), http://www.wmcactionnews5.com/story/34578066/lawsuit-filed-over-city-hall-blacklist-alleges-unlawful-videotaping-tracking-of-activists/; *BLACKLISTED: Memphis Police Surveillance and Kendrick v. Chandler—A Timeline*, ACLU TENN., https://www.aclu-tn.org/blacklisted-memphis-police-surveillance-and-kendrick-v-chandler-a-timeline/ (last visited Nov. 23, 2019).

On February 22, 2017, several activist plaintiffs (the "*Blanchard* Plaintiffs") filed suit in federal district court to enforce the 1978 Decree against the City of Memphis ("Memphis"). The Plaintiffs' Complaint alleged numerous violations of the Decree's restrictions on political surveillance, including the creation of the Escort List and the use of social media collators to surveil political activists.[33] The ACLU of Tennessee subsequently intervened as a plaintiff, arguing that (1) Memphis had violated the Decree for the reasons mentioned by the Blanchard Plaintiffs, and (2) as an original party to the Decree, the ACLU of Tennessee had standing to enforce the Decree's provisions.[34]

After the court granted partial summary judgment in favor of the ACLU of Tennessee, the case went to trial from August 20–23, 2018, to determine the extent to which MPD had violated the Decree.[35] On October 26, 2018, the court issued an opinion and order, finding that Memphis had violated the Decree by:

---

33. *See* Complaint at 5–6, Blanchard v. City of Memphis, No. 2:17-cv-2120-JPM-dkv (W.D. Tenn. Feb. 22, 2017), ECF No. 1.

34. ACLU's Motion to Intervene as Plaintiff at 1–2, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-dkv (W.D. Tenn. March 2, 2017), ECF No. 12. The court eventually dismissed the *Blanchard* Plaintiffs for lack of standing but determined that the ACLU of Tennessee, as a successor-in-interest to an original party to the suit, had standing to enforce the Decree. Order Granting Motion to Dismiss as to Blanchard Plaintiffs; Order Denying Motion to Dismiss as to Intervening-Plaintiff ACLU of Tennessee, Inc. at 12–16, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. June 30, 2017), ECF No. 41.

35. On June 18, 2018, both the ACLU of Tennessee and Memphis filed cross-motions for summary judgment. Order Granting in Part & Denying in Part the ACLU-TN's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 1. On August 10, 2018, the court issued an order denying in part and granting in part the ACLU of Tennessee's Motion for Summary Judgment and denying Memphis's Motion for Summary Judgment on the Issue of Contempt. *Id.* In that order, the court determined that the police had violated the Decree by engaging in political intelligence but identified genuine issues of material fact on the issues of (1) "whether MPD had operated any offices, infiltrated any groups, or disseminated any derogatory or false information about individuals or groups for political intelligence purposes; (2) whether any of MPD's actions purposefully deterred—or had the reasonable effect of deterring—any person from exercising their First Amendment rights; and (3) whether MPD had substantially complied with the Decree's restrictions on disseminating personal information to persons outside of law enforcement." *Id.* at 2. The court then conducted a bench trial, from August 20–23, 2018, to determine these issues. *Id.* at 34–35. The Honorable Judge P. McCalla presided over the trial. *Id.* at 1.

> 1) Conduct[ing] [political surveillance] as specifically defined and forbidden by the Decree;
> 2) Operat[ing] the [OHS] for the purpose of political intelligence;
> 3) Intercept[ing] electronic communications and infiltrat[ing] groups through the "Bob Smith" Facebook account;
> 4) Fail[ing] to familiarize MPD officers with the requirements of the Decree;
> 5) [Failing to] establish an approval process for lawful investigations into criminal conduct that might incidentally reveal information implicating First Amendment rights;
> 6) Disseminat[ing] information obtained in the course of investigation to individuals outside of law enforcement; and
> 7) Record[ing] the identities of protest attendees for the purpose of maintaining a record.[36]

The court issued sanctions against MPD through the form of remedial actions—such as training for responsible use of social media tools—to ensure future compliance with the Decree.[37] Finally, the court noted that "Memphis has an opportunity to remain the first, and perhaps only, city in the country with an established policy for the protection of its residents' privacy in the face of ever-expanding techniques of electronic surveillance."[38]

---

36. Opinion & Order at 2–3, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. Oct. 26, 2018), ECF No. 151.

37. *Id.* at 3.

38. *Id.* at 3–4. Memphis, however, is not the only city that has addressed the issue of police surveillance. Shortly after the resolution of the *Kendrick* suit, Seattle, Washington, passed an ordinance adopting many of the Memphis Consent Decree's limitations and restrictions on police surveillance practices. *See* Robert Spector, *When Policemen Becomes Spies*, SALT LAKE TRIBUNE (Feb. 10, 1985), http://www.aclu-tn.org/wp-content/uploads/2017/02/Kendrick-Documents-When-Policemen-Become-Spies.pdf. In its notorious "Spy Files" cases, the city of Denver, Colorado, addressed the matter of unregulated police surveillance of political activists in two ways: (1) through resolutions by the City Council and (2) through a class-action lawsuit against the City and County of Denver, which settled in 2003 after police agreed to adopt new surveillance policies. *See* Expressing Commitment of the City and County of Denver to Civil Rights and Liberties, Denver, Colo. Res. 13, 2002 Series (Mar. 18, 2002), https://acluco-wpengine.netdna-ssl.com/wp-content/uploads/2016/10/Denver-

This statement from the *Blanchard* court aptly captures the essence of the problem: police are increasingly weaponizing high-tech tools[39] to surveil activists lawfully exercising their First Amendment rights. While the issues in the *Blanchard* action arise from, and are specific to, the 1978 Decree between the ACLU of Tennessee and the City of Memphis, the case's factual matrix is alarmingly common. A study conducted by the Brennan Center for Justice revealed that at least 150 law enforcement agencies, cities, and counties across the United

---

City-Council-Resolution-No.-13-02-adopted-March-18-2002.pdf; News Release, ACLU Foundation of Colo., ACLU and Denver Officials Agree to Resolve Lawsuit Over Police Spy Files (Apr. 17, 2003), https://acluco-wpengine.netdna-ssl.com/wp-content/uploads/2016/10/2003-04-17-ACLU-and-Denver-Officials-Agree-to-Resolve-Lawsuit-over-Denver-Police-Spy-Files-ACLU-press-release.pdf. Perhaps the most famous surveillance case to date originated in New York City following surveillance of the Black Panther Party and other political groups by the New York Police Department ("NYPD"). *See Handschu v. Special Services Division (Challenging NYPD Surveillance Practices Targeting Political Groups)*, NYCLU, https://www.nyclu.org/en/cases/handschu-v-special-services-division-challenging-nypd-surveillance-practices-targeting (last visited Nov. 22, 2019). The settlement of this case resulted in the "*Handschu* guidelines," an agreement governing the permissible scope of NYPD surveillance practices. *See id.* Recently, NYPD has been accused of violating these guidelines to surveil BLM protestors. *See* Ali Winston, *Did Police Spy on Black Lives Matter? The Answer May Soon Come Out*, N.Y. TIMES (Jan. 14, 2019), https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html (describing how NYPD violated the *Handschu* guidelines to surveil political groups).

39. While the primary focus of this Note is police abuse of social media collators and similar devices, other technological tools used by the police raise further constitutional concerns. *See* Tyler Sonnemaker, *Tracked and Hacked: Why Every Internet User Should Care About Cybersecurity and Digital Privacy*, MEDILL REPORTS CHICAGO (Jan. 28, 2019), https://news.medill.northwestern.edu/chicago/tracked-and-hacked-why-every-internet-user-should-care-about-cybersecurity-and-digital-privacy/ (describing new technology products used by law enforcement that raise serious privacy concerns). For example, a lawsuit filed in Chicago, Illinois, alleges that police used a Stingray device to intercept cell phone communications during a 2015 political protest. *See* Complaint at 1–2, Boyle v. City of Chicago, No. 1:17-cv-00244 (N.D. Ill. filed Jan. 12, 2017). Stingrays are cell site simulator devices that mimic the signals emitted by cell phone towers and intercept cell phone location data. *Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers (last visited Nov. 22, 2019). Although the present Memphis case does not allege the use of such a device against political protestors, purchase records show that MPD owns at least one Stingray. *See* Purchase Order by City of Memphis to Harris Corp., Standard Purchase Order 249404, 1 (Aug. 5, 2013) (on file with author). *See also infra* note 174 (explaining how cell site simulators can implicate real time location data and generally require a warrant for use).

States have acquired social media monitoring software.[40] An independent inquiry by the ACLU revealed that police in Oakland, California, and Baltimore, Maryland, employed Geofeedia to identify and monitor activists during BLM protests in 2014 and 2015.[41] In 2018, an Asheville, North Carolina, newspaper uncovered an Asheville Police Department surveillance operation targeting BLM and similar groups, which included using Facebook photos and videos to identify individuals at a 2016 protest for the purpose of issuing *ex post facto* misdemeanor citations.[42] While these examples are illustrative, they are far from exhaustive; new cases of police surveillance abuse continue to emerge.[43]

The *Blanchard* court also identified another important dimension of the issue: many jurisdictions lack established policies for regulating police conduct that interferes with the First Amendment rights

40. Rachel Cohn & Angie Liao, *Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide*, BRENNAN CTR. FOR JUST.: ANALYSIS & OPINION (Nov. 16, 2016), https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide. *But see* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target (noting that Geofeedia's marketing materials tout that over five hundred law enforcement agencies have purchased its product).

41. Jessica Guynn, *ACLU: Police Used Twitter, Facebook to Track Protests*, USA TODAY (Oct. 12, 2016, 3:06 PM), https://www.usatoday.com/story/tech/news/2016/10/11/aclu-police-used-twitter-facebook-data-track-protesters-baltimore-ferguson/91897034/; Cagle, *supra* note 40. The ACLU stumbled upon this revelation after acquiring marketing materials that Geofeedia shared with police departments. *See* Cagle, *supra* note 40. This revelation also spurred several requests under the federal Freedom of Information Act, 5 U.S.C. § 552 (2018), and state public records laws to determine the extent of Geofeedia use among police departments across the country. *See, e.g.*, Iqra Asghar, *Boston Police Used Social Media Surveillance for Years Without Informing City Council*, PRIVACYSOS (Feb. 7, 2018), https://privacysos.org/blog/new-report-shows-boston-police-used-social-media-surveillance-years-without-informing-city-council/.

42. *See* Joel Burgess, *Timeline: Monitoring of Asheville Civil Rights Groups Has Roots in Police Shooting*, CITIZEN TIMES (July 16, 2018, 3:56 PM), https://www.citizen-times.com/story/news/local/2018/07/16/timeline-asheville-police-apd-monitoring-operation-rooted-fatal-jai-jerry-williams-2016-shooting/782657002/.

43. *See, e.g.*, Mark Morales & Laura Ly, *Released NYPD Emails Show Extensive Surveillance of Black Lives Matter Protestors*, CNN (Jan. 18, 2019, 7:01 PM), https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance/index.html (describing the recent revelation that NYPD spied on BLM protestors from November 2014 to January 2015).

of political activists. And even where privacy policies are in place to prevent this type of police misconduct, these policies can go unenforced.[44] Because sanctions are rarely imposed for intelligence overreach, law enforcement agencies virtually have carte blanche authority to investigate political activists despite lacking probable cause of criminal activity.

The primary thrust of this Note is to demonstrate how modern police information-gathering and dissemination practices—such as those challenged in the *Blanchard* case—pose serious problems that merit proactive remedies aimed at restoring balance to the relationship between law enforcement and political activists. To achieve this objective, this Note demonstrates that the issues stemming from modern surveillance practices are a byproduct of a historic and ongoing imbalance in the power dynamics between the police and socio-political minority groups. In Part II, this Note explores the history of American political surveillance to provide insights into how this imbalanced power dynamic developed and how it continues to persist.[45] In Part III, this Note discusses relevant First Amendment and Fourth Amendment case law in order to emphasize the importance of the court's role in protecting citizens from invasive law enforcement practices.[46] Part IV analyzes how modern police surveillance practices can violate the First

44. The *Blanchard* case illustrates this phenomenon. *Blanchard*, however, is not the only instance of police departments violating a court order to surveil political activists. *See, e.g.*, Winston, *supra* note 38; Jim Dwyer, *Police Infiltrate Protests, Videotapes Show*, N.Y. TIMES (Dec. 22, 2005), https://www.nytimes.com/2005/12/22/nyregion/police-infiltrate-protests-videotapes-show.html?module=inline (describing the history of the settlement resulting in the *Handschu* guidelines and NYPD's subsequent violations of these guidelines to surveil Iraqi War protestors).

45. *See infra* Part II.

46. *See infra* Part III.

and Fourth Amendment rights[47] of political activists and offers suggestions for reformative solutions.[48] Finally, Part V briefly concludes.[49]

II. POLITICAL ACTIVISTS & LAW ENFORCEMENT: A HISTORY OF IMBALANCED POWER DYNAMICS

Political activists and law enforcement agencies have been at odds for most of American history. While surveillance problems are not unique to the modern era, the expansion of technology in the twenty-first century has brought new dimensions and unique challenges to the issue. This Part demonstrates how political surveillance is a historical problem that has been exacerbated by the influx of technology. Furthermore, it shows how the problem is traceable to an imbalanced power dynamic between the state and its socio-political minorities.

The antithetical relationship between politically dissident thinkers and a surveilling government body predates America's founding. Under British colonial rule, general writs[50] authorized agents of the

47. This Note is not the first to recognize that identity-based surveillance implicates both First and Fourth Amendment rights. *See, e.g.*, Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 114 (2007) (arguing for the broad use of a First Amendment Criminal Procedure framework to regulate government information-gathering); Matthew A. Wasserman, Note, *First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program*, 90 N.Y.U. L. REV. 1786, 1788 (2015) (arguing for the use of a First Amendment Criminal Procedure framework to analyze the post-911 Muslim surveillance program in New York City). These articles primarily discuss criminal surveillance procedures for cases implicating First Amendment religious rights. Other articles have discussed applying a hybrid framework for analyzing claims of excessive force during political protests. *See* Lenese Herbert, *Why Properly Policing a Movement Matters: A Response to Alafair Burke's Policing, Protestors, and Discrimination*, 40 FORDHAM URB. L.J. 1023, 1039 (2013).

48. *See infra* Part IV.

49. *See infra* Part V.

50. Founding Father James Otis famously challenged the constitutionality of these writs before the Superior Court of Massachusetts. *See* John Adams, Petition of Lechmere (Arguments on Writs of Assistance), *in* 2 LEGAL PAPERS OF JOHN ADAMS 106–47 (L. Kinven Wroth & Hiller B. Zobel eds., 1965); James Otis, *Against Writs of Assistance*, CONST. SOC'Y (Feb. 24, 1761), http://www.constitution.org/bor/otis_against_writs.htm.

Crown to search and seize the effects of political thinkers.[51] Publishers of materials that criticized government leadership became targets for increased scrutiny and punitive actions.[52] These practices—which ran directly contrary to the Enlightenment-era philosophical emphasis on protecting life, liberty, and property from unfettered government tyranny[53]—were repugnant to the men who became the Founding Fathers of America. As political activists, the Founding Fathers played a crucial role in leading the movement for American Independence.[54] Once independence had been achieved, the creators of America's fledgling government recognized the importance of balancing the interests of majority and minority political viewpoints to prevent oppression by one controlling faction.[55] The Framers of the Constitution thus created the Bill of Rights to enshrine individual protections for political protestors against unreasonable government interference.

During the twentieth century, developments in social and political theory changed the face of the government-activist relationship from its colonially inspired roots. In 1956, the Federal Bureau of Investigation ("FBI") began an extensive counterintelligence program ("COINTELPRO") to investigate and disrupt the activities of social

51. *See generally* Entick v. Carrington (1765) 95 Eng. Rep. 807 (KB); Wilkes v. Wood (1763) 98 Eng. Rep. 489 (KB). Although both of these cases arose in England, they were widely discussed in the colonies and likely inspired the Fourth Amendment. *See* Boyd v. United States, 116 U.S. 616, 626 (1886).

52. For example, James Franklin—the brother of Founding Father Benjamin Franklin—was arrested and imprisoned for publishing an anonymous letter criticizing the governor of Massachusetts. *See* Dennis S. Kahane, *Colonial Origins of Our Free Press*, 62 A.B.A. J. 202, 204 (1976). See also Alison Olson, *The Zenger Case Revisited: Satire, Sedition, and Political Debate in Eighteenth Century America*, 35 EARLY AM. LIT. 223, 223 (2000), for a description of the 1735 prosecution of John Peter Senger for publishing "seditious libel."

53. *See* JOHN LOCKE, *Chapter V: Of Property* § 27 and *Chapter VII: Of Political or Civil Society* § 87, *in* TWO TREATISES OF GOVERNMENT (1689).

54. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (recognizing James Otis's 1761 speech against the general writs, cited *supra* note 50, as "the first act of opposition to the arbitrary claims of Great Britain" which helped spark the American Revolution (quoting Riley v. California, 573 U.S. 373, 403 (2014)). *See generally* Independence Hall Ass'n, *The Sons of Liberty*, US HISTORY.ORG, http://www.ushistory.org/declaration/related/sons.html (last visited Oct. 27, 2018).

55. *See* THE FEDERALIST NO. 10 (James Madison).

and political activist groups that the FBI perceived to be threats to national security.[56] COINTELPRO's surveillance operations broadly encompassed a number of socio-political groups, from ideology-focused groups—such as the Communist Party—to White Supremacist groups––such as the Ku Klux Klan—to peaceful activist groups—such as the Southern Christian Leadership Conference.[57]

During its COINTELPRO operations, the FBI targeted a number of nonviolent civil rights groups under the banner of its "Black Nationalist-Hate Groups" campaign.[58] The program's objectives included "prevent[ing] the rise of a 'messiah' who could 'unify, and electrify,' the movement"; "prevent[ing] violence . . . by pinpointing 'potential troublemakers' and neutralizing them 'before they exercise their potential for violence'"; and "prevent[ing] groups and leaders from gaining 'respectability' by discrediting them to the 'responsible' Negro community, to the white community, . . . and to Negro radicals."[59] Many of the individuals targeted under the FBI's "Black Nationalist-Hate Group" surveillance program were prominent civil rights leaders, including Dr. Martin Luther King, Jr.[60] Other targeted individuals were ordinary citizens that supported movements against racial inequality,

---

56. *See* SENATE SELECT COMM. TO STUDY GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 3–6 (2d Sess. 1976), https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf. Although the FBI's original target in 1956 was the Communist Party of the United States, it expanded its efforts to the activities of many other groups throughout the 1960s. *See COINTELPRO*, FBI RECORDS: THE VAULT, https://vault.fbi.gov/cointel-pro (last visited Oct. 27, 2019).

57. *See* S. REP. NO. 94-755, at 16–22.

58. *See id.* at 20–22 (targeting the Southern Christian Leadership Conference, the Student Nonviolence Coordinating Committee, the Deacons for Defense and Justice, and the Congress of Racial Equality, among others). The FBI also targeted members of "New Left" groups, which broadly included any public demonstrators that the FBI perceived to "show[ ] obvious disregard for decency and established morality," such as student groups protesting the Vietnam War. *Id.* at 7.

59. *Id.* at 21 (quoting Memorandum from FBI Headquarters to all SAC's 3–4 (Mar. 4, 1968))

60. *See id.* at 21 & n.93; Dia Kayyali, *The History of Surveillance and the Black Community*, ELECTRONIC FRONTIER FOUND. (Feb. 13, 2014), https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community. COINTELPRO operatives also targeted other civil rights leaders such as Dr. T.R.M. Howard, the founder of the Regional Council of Negro Leadership in Mississippi. Jeffrey O.G. Ogbar, *The FBI's War on Civil Rights Leaders*, DAILY BEAST (Apr. 11, 2017, 4:10 PM), https://www.thedailybeast.com/the-fbis-war-on-civil-rights-leaders.

entrenched poverty, or institutional oppression.[61] Through its COINTELPRO operations, the FBI effectively began the modern trend of law enforcement covertly surveilling socio-political minorities using spyware technology, such as pre-planted listening devices and wires worn by undercover agents.[62]

In 1971, federal operations officially ceased after the exposure of the FBI's COINTELPRO program, and a congressional investigation soon followed.[63] When the Senate Select Committee on Intelligence asked the FBI to justify its surveillance practices, the FBI offered two reasons for its actions: (1) protecting national security and (2) preventing violence.[64] However, the Senate Select Committee on Intelligence found that neither reason could justify the surveillance of nonviolent socio-political groups and that maintaining the existing political and social order was the implicit purpose of the FBI's COINTELPRO program.[65] The Senate Select Committee on Intelligence ultimately condemned COINTELPRO as "a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence."[66]

Both before and after COINTELPRO officially ended, local police departments in major cities conducted their own surveillance operations targeting advocacy groups. In the 1960s, officers with the New York Police Department ("NYPD") successfully infiltrated socio-political activist groups and posed as journalists to gather information

61. *See, e.g.*, S. REP. NO. 94-755, at 56 (describing the targeting of a county employee who had attended a fundraiser for the Mississippi Summer Project and a Black History Week program).

62. *See id.* at 7–12. *See generally* Spector, *supra* note 38.

63. *See* FBI RECORDS, *supra* note 56 (noting that COINTELPRO operations ended in 1971); *see also* Michael Isikoff, *NBC Reporter Recalls Exposing FBI Spying*, NBC NEWS (Jan. 8, 2014, 5:09 PM), https://www.nbcnews.com/news/investigations/nbc-reporter-recalls-exposing-fbi-spying-n5901 (describing how a group of activists broke into the FBI's Philadelphia field office and stole a number of files that would expose the COINTELPRO operations).

64. S. REP. NO. 94-755, at 5–6.

65. *Id.* at 6–7.

66. *Id.* at 3.

about various left-wing movements.[67] Around the same time, Memphis, Tennessee, experienced a similar series of surveillance operations. COINTELPRO-era law enforcement officers recruited high-level informants[68] and planted undercover MPD officers within local political activist groups.[69] Local surveillance operations persisted into the 1970s until the discovery which gave rise to the *Kendrick* lawsuit.[70] The 1978 Decree settling the *Kendrick* lawsuit attempted to restore the balance between the rights of Memphis-based political groups and the investigative powers of MPD. Furthermore, the Decree reflected a growing national concern that such extensive interference with individual First Amendment rights by law enforcement was intolerable in a democratic society.[71]

The turn of the twenty-first century saw the balance shift once again. Terrorist attacks on September 11, 2001, heightened national security interests in domestic political surveillance.[72] Following the 9/11 attacks, local officials softened the existing rules and regulations

67. *See* Matt Apuzzo & Adam Goldman, *NYPD Secrets: How the Cops Launched a Spy Shop to Rival CIA*, SALON (Sept. 1, 2013, 3:30 PM), https://www.salon.com/2013/09/01/when_the_nypd_became_a_spy_agency/. In 1971, a group of criminal defense lawyers representing members of the Black Panther Party uncovered evidence of the surveillance operations during a trial for criminal conspiracy. *Id.* This discovery led to a class action lawsuit in *Handschu v. Special Services Division*. *See id.* The case settled in 1985 by establishing protective guidelines (the "*Handschu* guidelines") for future NYPD surveillance practices. *Id.; see also* Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1389–92 (S.D.N.Y. 1985).

68. For example, law enforcement recruited Memphis-based civil rights photographer Ernest Withers to covertly surveil the activities of Martin Luther King, Jr., and other high-profile civil rights leaders. *See generally* MARC PERRUSQUIA, A SPY IN CANAAN: HOW THE FBI USED A FAMOUS PHOTOGRAPHER TO INFILTRATE THE CIVIL RIGHTS MOVEMENT (2018).

69. Tonyaa Weathersbee, *1960s Activists Say Police Spying Isn't New. The Internet Just Gave it a Makeover*, COM. APPEAL (Aug. 22, 2018, 5:02 PM), https://www.commercialappeal.com/story/news/2018/08/22/weathersbee-activists-aclu-police-surveillance/1046660002/ (describing MPD officer Marrell McCollough's infiltration of local activist groups during the Civil Rights movement and comparing his infiltration to the modern-day creation of fake Facebook profiles).

70. *See* sources cited *supra* notes 4–11 and accompanying text.

71. *See* SENATE SELECT COMM. TO STUDY GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 3 (2d Sess. 1976), https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf.

72. *See* NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 1–3 (2008).

for political surveillance to accommodate law enforcement's need for counterterrorism investigations.[73] Meanwhile, Congress passed a series of acts redefining the federal limits for individual privacy[74] while law enforcement agencies across the country sought sophisticated technological solutions for counterterrorism surveillance. [75]

The explosive growth of surveillance technology coincided with another technological development: the social media revolution. Social media changed the way political groups interact with their communities, and monitoring tools developed by companies such as Geofeedia now enable law enforcement to conduct surveillance on a wide-scale, systematic basis.[76] Police are increasingly employing these tools to surveil groups that are exercising First Amendment-protected rights.[77] Furthermore, the proliferation of fusion centers—collaborative offices

73. *See, e.g.*, Handschu v. Special Servs. Div., No. 71 Civ. 2203, 2003 WL 21961367, at *1 (S.D.N.Y. Apr. 7, 2003) (permitting local authorities to adjust the previous guidelines to accommodate law enforcement's counterterrorism investigative needs).

74. Edward J. McAndrew, *Five Laws and Regulations that Emerged from 9/11*, BALLARD SPAHR LLP (Sept. 9, 2016), https://www.ballardspahr.com/eventsnews/mediacoverage/2016-09-09-five-laws-and-regulations-that-emerged-from-9-11.aspx (listing post-9/11 federal laws such as the Aviation and Transportation Security Act, the USA Patriot Act, the Foreign Intelligence Surveillance Act, and the Homeland Security Act of 2002).

75. *See generally* LOIS M. DAVIS ET AL., RAND CORP., LONG-TERM EFFECTS OF LAW ENFORCEMENT'S POST-9/11 FOCUS ON COUNTERTERRORISM SURVEILLANCE AND HOMELAND SECURITY (2010), https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG1031.pdf (discussing the development of fusion centers, the expanded use of technology, and the increased focus on domestic terrorism surveillance following 9/11).

76. *See* KIDEUK KIM ET AL., URBAN INST., 2016 LAW ENFORCEMENT USE OF SOCIAL MEDIA SURVEY 1, 3 fig.2 (2017), https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf (noting that seventy percent of the 539 law enforcement agencies surveyed use social media for intelligence gathering in investigations); Cagle, *supra* note 40 (noting Geofeedia's claim that over five hundred law enforcement agencies use its product for surveillance).

77. *See* Nicole Ozer, *Police Use of Social Surveillance Media Software is Escalating, and Activists are in the Digital Crosshairs*, ACLU N. CAL. (Sept. 22, 2016), https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48#.36tadpuea.

for federal, state, and municipal law enforcement agencies to share information gleaned from investigations—has made the dissemination of information more widespread.[78]

Electronic surveillance practices such as those MPD employed in *Blanchard* are now becoming a commonplace problem in modern America.[79] Electronic monitoring can provide police with a powerful investigative tool to combat crime, but the capabilities of social media and data-mining tools pose serious concerns for the interpretation and treatment of any gathered information.[80] Notably, technology's power to source vast amounts of data creates the risk that this power will be

78. *See generally* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013) (discussing fusion centers and the privacy problems caused by fusion center operations).

79. *See supra* notes 37–41 and accompanying text.

80. *See infra* Part IV.

abused[81] and that peaceful activists will suffer actual injuries as a result.[82]

---

81. One concern is that this power is facilitating racial and political profiling. Although modern surveillance practices have the potential to affect law-abiding citizens of all groups and persuasions, members of racial and political minority groups are targeted more frequently. *See* Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523, 525–29 (2018). The surveillance of BLM activists in numerous cities across the country illustrates this phenomenon. *See generally* Amna Toor, Note and Comment, *"Our Identity is Often What's Triggering Surveillance": How Government Surveillance of #BlackLivesMatter Violates the First Amendment Freedom of Association*, 44 RUTGERS COMPUTER & TECH. L.J. 286 (2018) (providing an in-depth discussion of law enforcement's focus on BLM). In this regard, law enforcement appears to be drawing from the COINTELPRO-era practices of monitoring law-abiding, socio-political minorities and labeling outspoken activists as extremists. *See* 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; Julia Craven, *Surveillance of Black Lives Matter Movement Recalls COINTELPRO*, HUFFPOST (Aug. 20, 2015), https://www.huffingtonpost.com/entry/surveillance-black-lives-matter-cointelpro_us_55d49dc6e4b055a6dab24008 (noting that modern surveillance practices have been influenced by COINTELPRO); *see also* sources cited *supra* notes 56–60 and accompanying text. Like its COINTELPRO-era counterparts, modern law enforcement justifies its surveillance of BLM and other targeted activist groups for the traditional reason: protecting public safety. *See, e.g.*, Opinion and Order, *supra* note 36, at 19 (describing "public safety" as the City's justification for its actions in the case). While these ends are generally important, the means of achieving them—by targeting nonviolent spokespersons fighting against systemic inequality—suggest that law enforcement's implicit purpose is to maintain the status quo.

This premise finds support when one considers the central message of BLM—reforming law enforcement's treatment of African Americans—since law enforcement agencies frequently target BLM activists for surveillance. *See Herstory*, *supra* note 18. The two groups stand on diametric ends of an issue, but the power dynamics in play are far from equal. What little power BLM and similar grassroots groups have to combat institutional oppression derives entirely from political advocacy, a protected First Amendment right. By contrast, law enforcement's power to suppress the voices of its critics is immense. Police officers have the power and resources of the state at their disposal, including an arsenal of advanced technological tools. *See supra* notes 41–43 and accompanying text. By fixating on racial and political minority groups, law enforcement's selective surveillance practices risk facilitating digital racial profiling and enabling politically motivated or partisan-based surveillance. *See* Nasser Eledroos & Kade Crockford, *Social Media Monitoring in Boston: Free Speech in the Crosshairs*, PRIVACY SOS (2018), https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/. For an example of the problems this causes, see Steve Lieberman, *Clarkstown Says Police Unit Profiled, Violated Rights*, LOHUD (Aug. 31, 2016, 7:09 PM), https://www.lohud.com/story/news/local/rockland/clarkstown/2016/08/31/clarkstown-police-profiling-lawsuits/89648312/.

III. RELEVANT FIRST AND FOURTH AMENDMENT JURISPRUDENCE

First and Fourth Amendment jurisprudence further frames the relationship between political activists and law enforcement. Through its First Amendment decisions, the United States Supreme Court has sought to provide a framework for analyzing government regulations that infringe upon protected First Amendment expressive and privacy rights.[83] Likewise, the Court's Fourth Amendment jurisprudence provides a set of constitutional rules to govern law enforcement's methods of gathering information using technological tools.[84] Occasionally,

82. For example, modern police have mischaracterized some peaceful activist groups as "extremist," recalling COINTELPRO-era practices. *See* Craven, supra note 81 (noting that modern surveillance practices have been influenced by COINTELPRO); *What is a "Criminal Extremist"?*, ACLU COLO., https://aclu-co.org/spyfiles/criminalextremist/ (last visited Nov. 19, 2019). An "extremist" designation undeniably carries social and political stigmas. *See* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 647 (2004) ("The stigma and reputational harm that flow from being wrongly associated with terrorism are undeniably severe."); *see, e.g.*, Shirin Sinnar, *Questioning Law Enforcement: The First Amendment and Counterterrorism Interviews*, 77 BROOK. L. REV. 41, 66–80 (2011) (describing the stigmatizing effect of counterterrorism surveillance on U.S. Muslims after 9/11). Activists rely on public support for their causes, and the stigma associated with an "extremist" designation can be highly detrimental to a socio-political group's advocacy. By mislabeling peaceful groups as extremists, law enforcement agencies undercut the groups' public credibility and dilute the designation's true meaning within the domestic terrorism lexicon.

Additionally, by narrowing surveillance to focus upon peaceful activist groups, police run the risk of overlooking actually dangerous "lone wolf" extremists. *See* Eledroos & Crockford, *supra* note 81. Lone wolf extremists are individuals that commit acts of violence—usually in the name of a political, social, or religious ideology—without an affiliation to any group. *See* Katie Worth, *Lone Wolf Attacks Are Becoming More Common—And More Deadly*, FRONTLINE (July 14, 2016), https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/. The focus on groups rather than individuals may be attributable to law enforcement's preconceptions of historic terrorism dynamics. Politically motivated lone wolf attacks were once unusual and rarely successful occurrences; however, these attacks have grown more frequent and more deadly in the twenty-first century. *See id.* Historically, law enforcement has struggled to identify these genuine threats to public safety before the threat manifested in the form of violence. *See generally* Beau D. Barnes, *Confronting the One-Man Wolfpack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism*, 92 B.U. L. REV. 1613 (2012). For an extensive discussion of lone wolf extremists, see generally Khaled A. Beydoun, *Lone Wolf Terrorism: Types, Stripes, and Double Standards*, 112 NW. U. L. REV. 1213 (2018).

83. *See infra* Section III.B.1.

84. *See infra* Section III.B.2.

First and Fourth Amendment principles intersect in cases where surveillance practices implicate First Amendment rights.[85]

This Part demonstrates how the courts have developed remedies for resolving historic tensions in the political activist and law enforcement relationship. Implicit within the Court's jurisprudential history is the concept of balance: when law enforcement overreaches its power and intrudes too far into constitutionally-protected spaces, the court system has played an important role by stepping in to restore balance.

A. Development of the Modern First Amendment Framework

The Framers of the Constitution included the rights to free speech, assembly, and petition in the First Amendment.[86] These rights—referred to collectively as "expressive" rights—support fundamental values such as obtaining individual self-fulfillment, attaining the truth, increasing participation in decision-making, and striking the proper balance between stability and change.[87] Noting the importance of free expression to democratic society, the Supreme Court developed its First Amendment jurisprudence around a central framework that assesses the likelihood that government practices will chill the expressive rights of individuals.[88]

However, the Court's First Amendment jurisprudence further makes clear that free expression rights are not without limits. One such limitation to First Amendment expressive rights is the clear and present danger doctrine. In the early twentieth century, nationalist and anti-communist sentiment prompted a legislative trend to enact criminal syndicalism statutes punishing expressive advocacy against the United States government.[89] Convictions under these statutes largely framed

85. *See infra* Section III.B.3.

86. U.S. CONST. amend. I.

87. Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963).

88. *See* Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring) ("Such unwarranted inhibition upon the free spirit . . . has an unmistakable tendency to chill that free play of the spirit . . . ."). Generally, the Court has observed heightened chilling of First Amendment activities where government discretion is broadest. *See generally, e.g.*, Dombrowski v. Pfister, 380 U.S. 479 (1965).

89. *See, e.g.*, Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217 (1917) (codified as amended at 18 U.S.C. §§ 791–794, 2388 (2018)).

the Supreme Court's early modern First Amendment jurisprudence by prompting the development of the clear and present danger standard.

In the 1910s and 1920s, the Court considered a series of cases challenging criminal convictions for individuals that disseminated materials or undertook actions discouraging participation in United States military recruitment efforts.[90] Through these cases, the Court established that speech which creates a "clear and present danger" loses its First Amendment protections when the speech incites consequences adverse to legislative policy.[91]

This concept gained further dimension in *Whitney v. California*.[92] In *Whitney*, a defendant was convicted under a state syndicalism statute for helping establish the Community Labor Party of California, a group charged with unlawfully disseminating materials encouraging violent government overthrow.[93] The Court upheld the conviction despite Whitney's protests that she had vocalized her aversion to the group's violent resolutions and never helped create an instrument of terror or violence.[94] It found no constitutional violation where Whitney had joined and furthered an organization that the state deemed menacing to public peace and welfare.[95]

In the mid-twentieth century, however, the Court moved away from a rigid application of the clear and present danger doctrine—which favored the constitutionality of criminalizing anti-establishment speech—towards a more flexible test balancing individual and government interests.[96] The result was a gradual shift away from affirming convictions for mere advocacy or participation in a subversive political group without more concrete activity aimed at inciting violence. In *Brandenburg v. Ohio*, the Court crystallized the modern formulation of

90. *See generally* Whitney v. California, 274 U.S. 357 (1927); Gitlow v. New York, 268 U.S. 652 (1925); Abrams v. United States, 250 U.S. 619 (1919); Debs v. United States, 249 U.S. 211 (1919); Frohwerk v. United States, 249 U.S. 204 (1919); Schenck v. United States, 249 U.S. 47 (1919).

91. *See Abrams*, 250 U.S. at 623–24; *Debs*, 249 U.S. at 215–16; *Frohwerk*, 249 U.S. at 206; *Schenck*, 249 U.S. at 52.

92. 274 U.S. 357 (1927).

93. *Id.* at 359–66.

94. *Id.* at 367–68.

95. *Id.* at 367–71.

96. *See, e.g.*, Konigsberg v. State Bar of Cal., 366 U.S. 36, 51 (1961); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 464 (1958); Yates v. United States, 354 U.S. 298, 318 (1957); Dennis v. United States, 341 U.S. 498, 519–20 (1952) (Frankfurter, J., concurring).

the clear and present danger test when it considered the criminal conviction of a Ku Klux Klan leader charged with advocating for overthrowing the government if it failed to cease its oppression of the white race.[97] The *Brandenburg* Court ruled that criminal restrictions on political speech would only survive if the restricted advocacy expressly called for immediate violence and made such violence likely to occur.[98] In so doing, the Court overruled its previous decision in *Whitney* and tipped the balance further towards protecting the individual's right to advocate for even the most extreme viewpoints.[99]

Absent a finding of clear and present danger under *Brandenburg*'s rigorous standard, political activists enjoy comprehensive protections for expressive advocacy.[100] Alongside these protections, like-minded activists that form groups to promote shared platforms, viewpoints, and ideologies enjoy a right to free association derived from the First Amendment's guarantees of speech, assembly, and petition.[101]

Unlike the First Amendment's enumerated rights, the freedom of association doctrine was originally characterized as a privacy right.[102] The doctrine's modern form developed over a series of cases[103] originating during the Civil Rights Movement.[104] In *NAACP*

---

97. 395 U.S. 444, 448 (1969).

98. *Id.* at 447–49.

99. *Id.* at 449 ("[A] statute [that punishes mere advocacy] falls within the condemnation of the First and Fourteenth Amendments. The contrary teaching of *Whitney v. California* . . . cannot be supported, and that decision is therefore overruled.").

100. *See* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 505–06 (1969) (imposing strict scrutiny for cases of political or symbolic speech). *But cf.* Cox v. Louisiana, 379 U.S. 536, 555 (1965) (imposing rational basis scrutiny for cases involving speech intermingled with expressive conduct such as patrolling, marching, and picketing).

101. *See* Healy v. James, 408 U.S. 169, 181 (1972); United Transp. Union v. State Bar of Mich., 401 U.S. 576, 578–79 (1971); Bates v. City of Little Rock, 361 U.S. 516, 522–23 (1960); *Patterson*, 357 U.S. at 460.

102. *See, e.g.*, *Patterson*, 357 U.S. at 460–66 (describing free association as a privacy right).

103. *See, e.g.*, NAACP v. Button, 371 U.S. 415, 428–29 (1963) (striking as unconstitutional a state law which targeted and restricted the NAACP's ability to identify and provide legal representation for civil rights demonstrators); Shelton v. Tucker, 364 U.S. 479, 485–90 (1960) (rejecting an argument to compel state-employed teachers to disclose membership in progressive professional and sociopolitical organizations); *Bates*, 361 U.S. at 522–23 (rejecting an argument to compel membership list disclosure for state tax identification purposes); *Patterson*, 357 U.S. at 449–66.

104. The Civil Rights Movement produced a number of significant cases dealing with punitive actions against political activists. For example, in *Cox v. Louisiana*,

v. Alabama ex rel. Patterson, the Alabama Attorney General sought a circuit court injunction to prevent the NAACP from organizing in the state.[105] The state issued a subpoena for the NAACP's membership lists, and the NAACP refused to disclose them, resulting in a $100,000 fine for contempt of court.[106] The NAACP's constitutional challenge made its way to the Supreme Court, which unanimously reversed the Alabama Supreme Court and held that members of socio-political organizations maintain a right to privacy in their associations absent a compelling state interest in suppressing the members' First Amendment rights.[107] In *Patterson* and similar subsequent cases, the Court emphasized that compelled disclosure of membership lists runs a high

---

the Court considered whether B. Elton Cox, a civil rights protestor, was rightfully convicted of violating a state statute that criminalized picketing in front of a court house. 379 U.S. 559, 560 (1965). Although the Court upheld the law's constitutionality under rational basis scrutiny and rejected applying the clear and present danger standard to the facts of the arrest, it reversed Cox's conviction because officers of the state had expressly given Cox permission to peacefully protest at the location of his arrest. *Id.* at 569–73 (1965). In so holding, the Court emphasized the need for balancing the state's interest in upholding law and order with due process, free expression, and equal enforcement of constitutional laws regulating speech-related conduct. *Id.* at 574–75.

105. 357 U.S. at 451–52.

106. *Id.* at 452–53.

107. *Id.* at 466–67. In so holding, the Court applied strict scrutiny review of the state laws and practices in question. *Id.* at 460–61, 466. In First Amendment cases, strict scrutiny typically applies where the challenged restriction directly targets the content of free speech or restricts free expression in a public forum. *See, e.g.*, Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989); Bd. of Airport Comm'rs v. Jews for Jesus, Inc., 482 U.S. 569, 572–73 (1987). Although generally couched in due process, freedom of association challenges may also overlap with equal protection scrutiny where a government law or practice classifies people based on race or ethnicity. *See, e.g.*, Loving v. Virginia, 388 U.S. 1, 2 (1967). Under strict scrutiny, the government must show a compelling state interest, and the law must be narrowly tailored to serve that interest. *See generally* Korematsu v. U.S, 323 U.S. 214 (1944). Courts also use intermediate scrutiny—where the government interest must be important and substantially related to the law or practice in question—for analyzing conduct (time, place, and manner) that is intermingled with free speech or commercial speech. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 163 (2002). Finally, rational basis scrutiny may be employed by courts analyzing restrictions to non-speech activities, under which the government must have a legitimate interest that is rationally related to the law or practice in question. *See* Baird v. State Bar of Ariz., 401 U.S. 1, 6–8 (1971) (holding that state bar examiners do not have a legitimate interest in denying an applicant admission based upon views and beliefs).

risk of chilling organizational membership in the first place.[108] These cases tipped the balance further in favor of political activists by creating a strong presumption of freedom from government abridgment.[109]

Another dimension of free association protects individual activists from guilt by association. During the 1960s, the Court considered a number of cases involving the imposition of criminal sanctions or the denial of rights and privileges to individuals affiliated with the Communist Party.[110] In all of these cases, the Court expressed its disapproval that government actors had denied the individuals First Amendment protections solely on the basis of association with an unpopular group.[111]

In 1972, the Court formulated a framework for this issue when it considered the case of *Healy v. James*.[112] *Healy* involved a challenge by Connecticut Central State College students that had sought to form a local chapter of the Students for a Democratic Society, a national left-wing activist group that had developed a reputation for engaging in disruptive on-campus activities.[113] After the college president denied the group's application and prohibited the students from posting bulletins or holding meetings on-campus, the students filed a lawsuit challenging the abridgement of their free expression and association rights.[114] The Court held that the government "has the burden of establishing a knowing affiliation with an organization possessing unlawful aims and goals, and a specific intent to further those illegal aims," and remanded the case for further proceedings.[115] In so holding, the Court reaffirmed that activists enjoy a presumptive right to associate without fearing guilt by association.[116]

---

108. *Patterson*, 357 U.S. at 461–66; *Bates*, 361 U.S. at 522–26; *Shelton*, 364 U.S. at 485–90.

109. The Court has noted, however, that purely social group associations do not enjoy the same constitutional protections as those rooted in sociopolitical causes. *See, e.g.*, City of Dallas v. Stanglin, 490 U.S. 19, 24–25 (1989).

110. *See generally* United States v. Robel, 389 U.S. 258 (1967); Keyishian v. Bd. of Regents, 385 U.S. 589 (1967); Elfbrandt v. Russell, 384 U.S. 11 (1966); Scales v. United States, 367 U.S. 203 (1961).

111. *See Robel*, 389 U.S. at 265; *Keyishian*, 385 U.S. at 606–10; *Elfbrandt*, 384 U.S. at 19; *Scales*, 367 U.S. at 228–30.

112. *See* 408 U.S. 169 (1972).

113. *Id.* at 170–72.

114. *Id.* at 174–77.

115. *Id.* at 186.

116. *Id.*

While the Court's First Amendment frameworks vary by context,[117] the Court's free expression, free association, and procedural arrest cases produced a set of navigable rules aimed at protecting individual rights from an overextension of law enforcement power. First, socio-political activists enjoy broad free speech protections absent express and immediate calls for violence that make such violence likely to occur.[118] Second, activists enjoy the right to freely associate within groups without fear that the government will compel membership lists or impose liability for unlawful acts based solely upon group affiliation.[119] Finally, when government regulations or actions chill free expression and association rights, the state bears a "heavy burden" of demonstrating its appropriateness.[120] These rules serve the important purpose of checking law enforcement's power to suppress the viewpoints of peaceful socio-political minorities.

B. Development of the Modern Fourth Amendment Framework

Police surveillance practices also implicate Fourth Amendment rights. The Fourth Amendment protects an individual's reasonable expectation of privacy in persons, homes, papers, and effects during searches and seizures by government officers.[121] Inspired by colonial-era experiences and successful common law challenges to the Crown's authority to execute general search warrants,[122] the Framers of the

117. *See id.* 180 ("First Amendment rights must always be applied 'in light of the special characteristics of the . . . environment' in the particular case." (quoting Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 506 (1969)).

118. *See Tinker*, 393 U.S. at 505–06 (1969); Brandenburg v. Ohio, 395 U.S. 444, 447–49 (1969).

119. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958); *Healy*, 408 U.S. at 186; United States v. Robel, 389 U.S. 258, 265 (1967); Keyishian v. Bd. of Regents, 385 U.S. 589, 605–10 (1967); Elfbrandt v. Russell, 384 U.S. 11, 19 (1966); Scales v. United States, 367 U.S. 203, 228–30 (1961).

120. *Healy*, 408 U.S. at 184. It should be noted, however, that free speech intermingled with disruptive conduct may be subject to rational basis review. *See* Cox v. Louisiana, 379 U.S. 536, 555 (1965).

121. *See* U.S. CONST. amend. IV (protecting persons, houses, papers, and effects from unreasonable searches and seizures absent a warrant supported by probable cause); Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring) (recognizing Fourth Amendment protections for an individual's reasonable expectations of privacy).

122. *See, e.g.*, sources cited *supra* notes 50–52.

Fourth Amendment sought to secure the "privacies of life" against arbitrary government power[123] and to "place obstacles in the way of a too permeating police surveillance."[124] As technology has rapidly developed throughout the modern era, the Court has sought to maintain the balance between the government's power to surveil its citizens and the privacy rights of individuals. Two lines of technology cases have thus come to frame the Fourth Amendment issue of covert police surveillance: (1) cases addressing privacy in information captured during communications and (2) cases addressing privacy rights in locations and movements.[125] These cases impose significant restrictions on the government's power to use surveillance technologies without probable cause of criminal activity. Moreover, when these two lines of cases converged in *Carpenter v. United States*, the Court offered a promising glimpse at how it might treat future challenges to invasive surveillance technology.[126]

1. Communications Surveillance Cases

The first line of communication surveillance cases originated as exclusionary challenges to the use of wiretapping and implanted recording devices (also known as "bugging").[127] The Court first addressed the issue in *Olmstead v. United States*, a case concerning the

123. Boyd v. United States, 116 U.S. 616, 630 (1886).

124. United States v. Di Re, 332 U.S. 581, 595 (1948).

125. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214–16 (2018) (discussing the two lines of cases that frame the Supreme Court's Fourth Amendment technology jurisprudence).

126. *See id.* at 2216–23.

127. Wiretapping and bugging, though similar in practical and legal effect, are technically distinct methods of surveillance. Wiretapping involves infiltration through telephone wires, while bugging involves the physical implantation of a listening device. Nicholas M. Horrock, *Electronic Surveillance: Scope of Wiretapping and Bugging an Issue of Rising Concern*, N.Y. TIMES (Feb. 20, 1975), https://www.nytimes.com/1975/02/20/archives/electronic-surveillance-scope-of-wiretapping-and-bugging-an-issue.html. Historically, wiretapping occurred far more frequently than bugging because it could be accomplished from a distance without the need for trespass. *See id.* Wiretapping, however, required agents to diligently standby to capture targeted conversations. *See id.* In the modern era, the nature of cell phone and internet network systems has made it much easier for government agents to intercept communications—even where devices are turned off—without the need for targeting landlines or planting bugs. *See* Ewen MacAskill, *Trump's Wiretap Paranoia and the Reality of Modern Surveillance*, THE GUARDIAN (Mar. 6, 2017, 1:01 PM),

conviction of several defendants for running a bootlegging business during prohibition.[128] Upon suspecting the presence of a criminal conspiracy, federal officers tapped the defendants' phone lines to intercept conversations.[129] The Court considered whether such actions constituted a Fourth Amendment search and held that Fourth Amendment protections did not extend to phone lines, thus affirming the defendants' convictions.[130] Shortly thereafter, the Court considered the constitutionality of bugging in *Goldman v. United States*, a case concerning the use of listening devices in a room adjacent to a defendant's office to allow federal agents to eavesdrop on conversations between conspiring defendants.[131] Under a traditional Fourth Amendment, property-based analysis similar to the one used in *Olmstead*, the Court found that no Fourth Amendment violation occurred because the agents did not physically trespass into any constitutionally protected spaces to gather the evidence needed to convict the defendants.[132]

Forty years later, however, the Court reconsidered the issue in two important Fourth Amendment cases—*Berger v. New York*[133] and *Katz v. United States*[134]—that changed the Court's methods of analyzing Fourth Amendment issues and its overall stance on wiretapping and bugging. *Berger* concerned the constitutionality of a state statute which authorized general wiretapping investigations if a district attorney, attorney general, or high-ranking state police officer provided an affidavit swearing that there was reason to believe the investigations would produce evidence of criminal activity.[135] The *Berger* Court explicitly overruled *Olmstead* insofar that it found that phone conversations between individuals were protected by the Fourth Amendment, and it struck down the statute as an unconstitutional authorization of general warrant search practices in violation of the Fourth Amendment's particularity requirement.[136]

---

https://www.theguardian.com/world/2017/mar/06/trumps-wiretap-paranoia-reality-modern-surveillance.

128. 277 U.S. 438, 455–56 (1928).
129. *Id.* at 456–57.
130. *Id.* at 462–69.
131. 316 U.S. 129, 130–32 (1942).
132. *Id.* at 133–36.
133. Berger v. New York, 388 U.S. 41 (1967).
134. Katz v. United States, 389 U.S. 347 (1967).
135. 388 U.S. at 43, 53–54.
136. *Id.* at 51–64.

That same year, the Court considered the *Katz* case, an exclusionary challenge to evidence used to convict the defendant of violating federal gambling laws that was obtained by federal agents bugging a phone booth.[137] Overruling its previous decisions in both *Olmstead* and *Goldman*, the *Katz* majority emphasized that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" because "the Fourth Amendment protects people, not places."[138] Under this subjective test, the *Katz* majority found that Katz intended for his conversations to be contained to the privacy of the phone booth, and it found that the government violated Katz's Fourth Amendment rights by surveilling him without a warrant.[139] The Court thus affected a final fatal blow to law enforcement's discretion to conduct limitless surveillance under the *Olmstead* standard and strengthened the value of an individual's right to keep his conversations private. Most significantly, *Katz* also produced the modern reasonable expectations of privacy test—which considers both the individual's subjective expectations and the objective reasonableness of these expectations—in Justice Harlan's concurring opinion.[140]

Alongside its early wiretapping and bugging cases, the Court also began developing a framework for considering the admissibility of communications collected without a warrant by wired undercover agents. In *On Lee v. United States*, the Court first addressed the issue of informant-sourced surveillance when it considered a defendant's conviction for selling opium, a conviction that was obtained using evidence collected by an undercover agent wearing a wire.[141] Under the *Olmstead-Goldman* trespass analysis, the Court found that no Fourth Amendment violation had occurred because On Lee had invited the agent onto his property where the recorded inculpatory conversations had occurred.[142]

After its decision in *Katz*, the Court reconsidered the wired undercover agent issue under a privacy rights framework in *United States v. White*.[143] A divided majority of the Court reversed the appellate

137. 389 U.S. at 348.
138. *Id.* at 350–53.
139. *Id.* at 352–59.
140. *See id.* at 360–62 (Harlan, J., concurring).
141. 343 U.S. 747, 748–49 (1952).
142. *Id.* at 751–58.
143. United States v. White, 401 U.S. 745 (1971).

court's exclusion of evidence.[144] A plurality held that undercover electronic recordings are constitutionally admissible—even if they frustrate a criminal defendant's subjective expectations of privacy—if ongoing criminal activity and law enforcement's investigative needs render such privacy expectations objectively unreasonable.[145] The Court could not agree, however, on whether *On Lee* could still be considered good law under the Court's post-*Katz* jurisprudence.[146] Furthermore, the *White* Court produced three strong dissents, including that of Justice Douglas, which condemned the chilling effect of electronic surveillance on the propagation of free speech, a protected First Amendment value.[147]

The Court further limited the post-*Katz* expansion of individual privacy rights by developing the Third-Party doctrine. This doctrine originated in *United States v. Miller*, a tax fraud case stemming from the defendant's operation of an illegal bootlegging business which concerned the pre-indictment subpoena of Miller's bank records.[148] The Court reversed the appellate court's order to exclude the bank records, holding that Miller had no reasonable expectation of privacy in information willingly turned over to the bank, a third party.[149] Three years later, in *Smith v. Maryland*, the Court expanded *Miller*'s holding from merely bank records to all information voluntarily turned over to a commercial third party, including numbers typed into a phone that were accessed through a pen register. [150]

In the face of twenty-first century technology, however, the Court has begun limiting the Third-Party doctrine's expansive rule. In *Riley v. California*, a recent case involving the search of a defendant's cellphone incident to the defendant's arrest, the Court rejected the state's argument that *Smith* authorized officers to search the cellphone's call log.[151] The *Riley* Court subsequently held that a cell

144. *Id.* at 754.
145. *Id.* at 750–54.
146. *See id.* at 755 (Brennan, J., concurring).
147. *See id.* at 761–65 (Douglas, J., dissenting).
148. 425 U.S. 436, 436–39 (1976).
149. *Id.* at 440–47.
150. Smith v. Maryland, 442 U.S. 735, 742 (1979).
151. Riley v. California, 573 U.S. 373, 400 (2014).

phone's contents are protected by the Fourth Amendment and are thus generally subject to the warrant requirement.[152]

2. Physical Locations and Movements Cases

The second line of electronic surveillance cases address privacy rights in physical locations and movements. These cases emerged as a series of challenges to law enforcement's use of location-monitoring devices. The Court first considered the issue in *United States v. Knotts* and *United States v. Karo*, two cases where law enforcement officers attached a beeper-like tracking device to chemical containers that were subsequently transported to illegal drug-manufacturing facilities.[153] In *Knotts*, the Court affirmed the defendant's conviction, holding that the use of a beeper to track a defendant's movements along public highways did not violate the Fourth Amendment because it was analogous to an officer visually observing the defendant's voluntary public movements, in which a defendant enjoys no reasonable expectations of privacy.[154] The Court reiterated this principle in *Karo* but further found that the monitoring of such a device became an unconstitutional search once the container left public roadways and was brought into a private residence.[155]

The sophistication of tracking technology during the twenty-first century prompted the Court to reevaluate its *Knotts-Karo* rule in *United States v. Jones*.[156] The *Jones* case concerned the warrantless placement of a GPS tracking device on a defendant's car and its subsequent monitoring by federal agents.[157] In Justice Scalia's majority opinion, the Court held that the device's initial installment on the defendant's vehicle was an unconstitutional trespass and reversed the de-

152. *Id.* at 403; *see also* In re Search of a Residence in Oakland, Cal., 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019) (holding that law enforcement agencies cannot force an individual to use fingerprint or facial recognition software to unlock a phone without a warrant).

153. United States v. Karo, 468 U.S. 705, 708 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).

154. 460 U.S. at 284–85.

155. 468 U.S. at 713–719.

156. United States v. Jones, 565 U.S. 400 (2012).

157. *Id.* at 402–04.

fendant's drug conviction as it had been obtained with the fruits of illegal searches.[158] Justice Alito's concurrence, in which three Justices joined, employed a reasonable expectation of privacy analysis to reach a similar result.[159] Significantly, Justice Alito's concurrence recognized that the ubiquitous presence of sophisticated surveillance technology made it much easier for the government to engage in long-term surveillance operations than was previously possible under *Knotts* and *Karo*, thus causing greater interference with an individual's expectation of privacy.[160]

3. Convergence of the Two Lines of Electronic Surveillance Cases

The two lines of cases concerning electronic surveillance converged in the recent case of *Carpenter v. United States*.[161] In *Carpenter*, the Court considered whether historic cell phone location data obtained through "pinging"[162] falls under the Fourth Amendment's privacy protections.[163] The issue of cell site location information ("CSLI") records required the Court to assess a new area of privacy law at the intersection of its two lines of technology cases as informed by the Third Party doctrine.[164]

158. *Id.* at 404–13 (distinguishing the case from *Knotts* and *Karo*, where the installment of the device took place before the containers entered the defendant's possession).

159. *Id.* at 418–31 (Alito, J., concurring in judgment).

160. *Id.* at 427–31. Justice Alito's concerns for maintaining privacy in the face of ever-expanding technology echo the Court's sentiments in another technology surveillance case, *Kyllo v. United States*, 533 U.S. 27 (2001). While not a tracking device case, *Kyllo* involved the warrantless use of thermal imaging equipment to record heat emissions from the defendant's residence to obtain evidence of a marijuana-growing operation. *Id.* at 29–30. Because—absent the use of the device—such information would not be discoverable without physical intrusion into Kyllo's residence, the Court found that the warrantless use of thermal imaging equipment on a private home was unconstitutionally impermissible. *Id.* at 34–40. In so holding, the Court recognized that its decision imposed an important and necessary limit on the "power of technology to shrink the realm of guaranteed privacy." *Id.* at 34.

161. 138 S. Ct. 2206 (2018).

162. "Pinging" refers to the interfacing between a cell phone and signaling towers owned by the cell phone's service providers. *See id.* at 2211–12. This interfacing creates a record of a cell phone's location, and law enforcement agencies can track a person's movements by analyzing these records. *See id.*

163. *See id.* (describing the process by which wireless providers receive and record location data).

164. *Id.* at 2214–17.

In a landmark decision authored by Chief Justice Roberts, the Court held that officers must obtain a warrant to access historic CSLI records from third-party cell phone service providers.[165] In so finding, the Court recognized a heightened expectation of privacy in an individual's movements because such movements are capable of revealing individual privacies such as "familial, political, professional, religious, and sexual associations."[166] Citing Justice Alito's concurrence in *Jones*, the *Carpenter* Court also recognized the role that technology played in making it relatively easy and inexpensive for the government to surveil an individual over a long period of time, thus gaining access to these privacies.[167] Noting the ubiquitous nature of cell phones in all aspects of modern life, the Court emphasized the immense impact that unfettered government power to obtain cell phone records would have on the privacy rights of all individuals, including those who have not committed criminal offenses.[168] The Court thus found this type of surveillance to be distinguishable from the more targeted GPS tracking approach used in *Jones*.[169]

The Court found that the prevalence and sophistication of cell phone location surveillance technology—and its high probability for unconstitutionally interfering with the privacy rights of ordinary citizens as well as criminals—justified a departure from the Third-Party doctrine.[170] The Court found further justification for departing from the Third-Party doctrine in the fact that such location data could be sourced through any operation—including the receipt of texts, calls, emails, or social media updates—while the phone is turned on.[171] The Court found that this absence of a voluntary, affirmative act in sharing

165. *Id.* at 2221–23.

166. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

167. *Id.* at 2217–18 (citing *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment)).

168. *Id.* at 2218.

169. *Id.*

170. *Id.* at 2219 (noting that when the Third Party doctrine originated in *Miller* and *Smith*, the technology involved was much more limited and much less invasive); *see also supra* pp. 260–61 for a discussion of the Third Party Doctrine, *Miller*, and *Smith*.

171. *Id.* at 2219–20.

one's location negated the voluntary assumption of risk that underpinned the Third-Party doctrine.[172]

Carpenter, while perhaps the most significant technology case to date, was not limitless in its scope. The Court declined to overrule *Miller* and *Smith*'s application in other established contexts and emphasized that its decision was narrowed to historic location data, explicitly excluding real-time CSLI[173] or "tower dump" events.[174] The Court further indicated that warrantless acquisitions of the kind at issue in *Carpenter* may be justified by exceptions to the warrant requirement.[175] Nevertheless, Justice Roberts concluded his opinion by recognizing the future necessity of balancing "powerful new tool[s] [afforded to law enforcement] to carry out its important responsibilities" with the "risks [of] [g]overnment encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent."[176]

---

172. *Id.* at 2220.

173. *Id.* While the warrant requirement for historic location data is settled law after *Carpenter*, jurisdictions have split on whether officers must obtain a warrant to track a cell phone's real-time movements using CSLI. *Compare, e.g.*, United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017) (holding that a warrant is not required for police to access real-time CSLI to track an individual), *with* Tracey v. State, 152 So. 3d 504, 525–26 (Fla. 2014) (holding that a warrant is required to access real-time CSLI to track an individual) *and* State v. Earls, 70 A.3d 630, 588 (N.J. 2013) (same). The issue of real-time CSLI also implicates the use of cell site simulators such as "Stingray" devices. *See supra* note 39 and accompanying sources. Because cell site simulators do not require officers to seek records from a third party cell service provider, the use of cell site simulators is not subject to the Third Party doctrine and generally requires a warrant. *See* Jones v. United States, 168 A.3d 703, 716–17 (D.C. 2017) (holding that a warrant is required to use cell site simulators to access CSLI); State v. Andrews, 134 A.3d 324, 395 (Md. Ct. Spec. App. 2016) (same). *But see* United States v. Ellis, 270 F. Supp. 3d 1134, 1149–53 (N.D. Cal. 2017) (illustrating that cell site simulators may be used without a warrant in cases of exigent circumstances).

174. *Carpenter*, 138 S. Ct. at 2220 (defining tower dumps as "a download of information on all the devices that connected to a particular cell site at a particular interval").

175. *Id.* at 2222–23.

176. *Id.* at 2223 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)); *see* sources cited *supra* notes 50–54 for the "lessons" to which Justice Roberts likely refers.

C. Surveillance Cases at the Nexus of the First and Fourth Amendments

First Amendment surveillance cases are not prevalent among the Supreme Court's jurisprudence. However, the cases of the modern era are not completely without relevant analogues. In *United States v. United States District Court* (the "*Keith*" case), the Court considered whether, in the face of a domestic threat to national security, the Attorney General of the United States could order the wiretapping of an anti-war political advocacy group's members without first obtaining a warrant.[177] Noting that this type of case reflected "a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime," the Court held that wiretapping conducted for national security purposes nevertheless required the federal government to first obtain a warrant.[178] In so holding, the Court emphasized the importance of protecting minority political beliefs from government action taken "under so vague a concept as the power to protect 'domestic security.'"[179]

The same year it decided *Keith*, the Court considered *Laird v. Tatum*, a class action brought by activists alleging that the Army's surveillance of their protest-related activities violated their First Amendment rights.[180] The Court considered whether the plaintiff's mere knowledge of the existence of the Army's surveillance program, without further certainty that the Army would take future action against the individuals, created a chilling effect sufficient to provide standing for the plaintiffs to sue.[181] A majority of the Court held that it did not, stating that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[182] Four Justices dissented, disagreeing with the

177. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 299–300 (1972).

178. *Id.* at 313, 320.

179. *Id.* at 314. Following the Court's decision in *Keith*, one of the affected group members sued the Attorney General for damages from the warrantless surveillance. *See* Mitchell v. Forsyth, 472 U.S. 511, 513–15 (1985). Although the Court held that the Attorney General was not entitled to absolutely immunity, he nevertheless was entitled to qualified immunity because the constitutional requirement for a warrant was not clearly established at the time of the violation. *Id.* at 520–24, 530–35.

180. Laird v. Tatum, 408 U.S. 1, 2 (1972).

181. *Id.* at 9–10.

182. *Id.* at 13–14.

majority's view that the controversy presented no objective or future chilling of First Amendment rights.[183]

Other federal surveillance cases have ended at the appellate level. Notably, following the post-9/11 implementation of the National Security Administration's ("NSA") Terrorist Surveillance Program ("TSP"), the Sixth Circuit considered a constitutional challenge to NSA eavesdropping and datamining practices.[184] The ACLU and a coalition of journalists, academics, and lawyers who regularly communicated with individuals being monitored by the NSA brought an injunction suit under 42 U.S.C. § 1983 and the First and Fourth Amendments.[185] A divided court held that the plaintiffs lacked standing to sue because they could not prove that the NSA had actually intercepted any of their communications.[186]

Perhaps the most relevant surveillance case to date is *Hassan v. City of New York*, a First Amendment-Equal Protection challenge brought by Muslim citizens that were allegedly surveilled in the wake of 9/11.[187] In *Hassan*, the Third Circuit considered whether the plaintiffs could state a plausible claim that New York's Muslim surveillance practices violated their First and Fourteenth Amendment rights.[188] The *Hassan* Court held that the Plaintiffs' complaint plausibly alleged financial, religious, reputational, and stigmatizing injuries suffered as a result of NYPD's specific targeting of Muslim individuals, businesses, and mosques for counterterrorism surveillance.[189] Significantly, the Court stated in its concluding remarks:

---

183. *See, e.g.*, *id.* at 26–28 (Douglas, J., dissenting) ("The present controversy is not a remote, imaginary conflict. Respondents were targets of the Army's surveillance . . . [and] Army surveillance . . . is at war with the principles of the First Amendment.").

184. ACLU v. NSA, 493 F.3d 644, 648–50 (6th Cir. 2007).

185. *Id.* at 648–49.

186. *Id.* at 659–74; *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410–11 (2013) (providing the present requirements for a plaintiff to establish standing in order to seek injunctive relief in federal surveillance cases).

187. *See* Hassan v. City of New York, 804 F.3d 277, 284 (3d Cir. 2015); *see also Hassan v. City of New York*, CTR. FOR CONST. RIGHTS, https://ccrjustice.org/home/what-we-do/our-cases/hassan-v-city-new-york (last modified Apr. 5, 2018).

188. *Hassan*, 804 F.3d at 284–85.

189. *Id.* at 289–309. In so doing, the *Hassan* Court distinguished the surveillance practices in *Laird*, which were not discriminatory towards a particular protected group. *Id.* at 292.

> What occurs here in one guise is not new. We have been down similar roads before. Jewish-Americans during the Red Scare, African-Americans during the Civil Rights Movement, and Japanese Americans during World War II are examples that readily spring to mind. We are left to wonder why we cannot see with foresight what we so clearly see in hindsight—that '[l]oyalty is a matter of the heart and mind[,] not race, creed, or color.'"[190]

These surveillance cases, when considered with the Supreme Court's other First Amendment free association and Fourth Amendment technology cases, demonstrate that the court has an important role to play in protecting individual rights from an overreaching law enforcement. Judicial responsibility commands courts to recognize when an imbalance in the power dynamics causes constitutional injuries to ordinary people. Where there is an injury, courts should step in to provide a remedy.

IV. SOLUTIONS

The practices that police use to gather, store, and share information on political activists risk running afoul of the First and Fourth Amendments.[191] In fact patterns resembling the *Blanchard* case,[192] targeted and injured activists may be able to seek judicial remedies to enjoin unconstitutional practices or enforce violations of existing surveillance guidelines.[193] Where guidelines are lacking, policy-makers should provide solutions to protect individual rights and delineate clear protocols for political surveillance.[194]

A. Constitutional Concerns Raised by Electronic Surveillance Practices

Modern surveillance practices run the risk of infringing upon the First and Fourth Amendment rights of political activists. In some cases,

190. *Id.* at 309 (alterations in the original) (quoting *Ex parte* Mitsuye Endo, 323 U.S. 283, 302 (1944)).

191. *See supra* Section III.C.

192. *See supra* Part I.

193. *See supra* Section IV.B.

194. *See supra* Section IV.B.

targeted surveillance may rise to the level of a First Amendment violation, entitling activists to seek judicial relief.[195] Law enforcement's use of sophisticated technological tools to obtain private information may also violate the Fourth Amendment's protections against searches and seizures where such tools invade protected privacy realms.[196]

1. Surveillance Practices and the First Amendment

Along with free speech, petition, and assembly, the First Amendment guarantees private citizens the right to privacy in their associations. Among other things, freedom of association protects an individual's choice to form groups to engage in political advocacy.[197] When activists bring plausible claims that state practices or actions infringe upon their free association rights,[198] the state's conduct is subject to strict scrutiny review.[199] In other words, a law enforcement agency seeking to restrict free association rights must show a compelling interest in restricting them, and the action sought must be narrowly tailored to serve the purpose of that interest.[200] Where overbroad policy fails to sufficiently cabin government discretion, free association is likely to be chilled in violation of the First Amendment.[201]

---

195. *See, e.g.*, Black Lives Matter v. Town of Clarkstown, 354 F. Supp. 3d 313, 324–25 (S.D.N.Y. 2018) (finding that five individual BLM plaintiffs plausibly alleged present harm of chilling from police intimidation and surveillance tactics employed by police and from the Town's systematic custom, policy, or practice of surveilling based on racial or political reasons).

196. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("Court[s] [are] obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." (third alteration in original) (quoting Olmstead v. United States, 277 U.S. 438, 473–474 (1928)); Katz v. United States, 389 U.S. 347, 351 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citing Rios v. United States, 364 U.S. 253 (1960); *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

197. *See* NAACP v. Button, 371 U.S. 415, 444–45 (1963); Bates v. City of Little Rock, 361 U.S. 516, 525–27 (1960); Shelton v. Tucker, 364 U.S. 479, 487–90 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460–67 (1958).

198. *See Black Lives Matter*, 354 F. Supp. 3d at 323–27.

199. *See* Buckley v. Valeo, 424 U.S. 1, 64 (1976); *Patterson*, 357 U.S. at 460–61.

200. Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226 (2015) (citations omitted).

201. Dombrowski v. Pfister, 380 U.S. 479, 486–87 (1965); Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring).

In cases across the country, police practices have implicated the free association rights of political activists through targeted surveillance.[202] Such practices may violate First Amendment freedoms of association absent a compelling police interest and a narrow tailoring of said practices to achieve this interest.[203] While the police's interest in protecting public safety is certainly important, this justification for compiling and sharing sensitive data may be too overbroad[204] and not compelling enough to pass the high bar for strict scrutiny where individuals have engaged only in lawful advocacy.[205] Furthermore, police practices could not reasonably be described as "narrowly tailored" to serve the interests of public safety where their scope far exceeds the magnitude of any criminal behavior involved, such as surveillance practices that target individuals who lack criminal records on the basis of their participation in local advocacy groups.[206] Where such activities run a high likelihood of chilling First Amendment activities, a professed interest in public safety should not be inadequate to justify any continuance of these operations absent clear evidence of an actual public threat.[207] On balance, protected privacy interests must prevail.[208]

---

202. *See, e.g.*, Winston, *supra* note 38 (describing the still-evolving BLM surveillance case in New York City); Lieberman, *supra* note 81 (describing a particularly troubling surveillance operation in Clarkstown, New York, that targeted BLM activists and elected officials for political purposes); *see also Black Lives Matter*, 354 F. Supp. 3d at 317–25.

203. *See Patterson*, 357 U.S. at 460–61.

204. *Cf. Keith*, 407 U.S. 297, 313–14 (1972) (noting that "domestic security" is far too broad of a purpose to justify warrantless surveillance by the Attorney General).

205. Some activists, such as those in Memphis, may enjoy an even higher interest in engaging in First Amendment activities without the threat of becoming a target for political intelligence if laws are in place to restrict and regulate police surveillance practices.

206. This issue becomes especially problematic when the law-abiding activists engage in advocacy that is critical of police practices, such as BLM. *See* Toor, *supra* note 81, at 327–30.

207. *Cf. Keith*, 407 U.S. at 313–14.

208. However, there may be circumstances where even invasive electronic surveillance practices are justified. A showing of clear and present danger under *Brandenburg* would authorize these activities if an activist group's political advocacy poses an immediate threat of inciting violence and such violence is likely to occur as a result. *See* Brandenburg v. Ohio, 395 U.S. 444, 447–49 (1969) (citations omitted). Under such circumstances, police should be free to compile, maintain, and disseminate information regardless of whether these practices infringe upon the First Amendment rights of individuals. *See id.* Such circumstances necessarily tip the balance in favor of allowing police to adequately do their job.

Standing, however, poses a significant hurdle for targeted activists seeking relief from police surveillance practices. Courts have been reticent to recognize justiciable First Amendment claims to enjoin police surveillance for chilling political activities absent a particularized and concrete injury.[209] However, when targeted activists can identify direct, ongoing, and immediate harm caused by police monitoring practices——such as business losses, loss of employment status, or stigmatizing injuries—they may be able to meet the requirements for First Amendment standing.[210] Likewise, if surveillance practices are accompanied by intimidation tactics that are aimed at suppressing free speech, the resultant chill to the exercise of First Amendment rights may also be sufficient to establish standing under a First Amendment retaliation theory.[211] The Third Circuit's *Hassan* decision offers yet another potential approach to establishing standing when the challenged surveillance practices intentionally discriminate against a protected class of individuals.[212] Members of socio-political groups that receive discriminatory treatment from law enforcement surveillance practices might be able to establish standing under a First Amendment-Equal Protection theory if the discrimination is rooted in race, religion, or nationality.[213]

2. Surveillance Practices and the Fourth Amendment

Several rules and standards synthesized from the Court's technology cases govern the constitutional scope of privacy rights and permissible surveillance. As a starting point, the Fourth Amendment condemns searches that intrude upon reasonable expectations of privacy in persons, homes, papers, and effects.[214] This standard requires an individual to hold subjective expectations that the information targeted by

209. *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 13–15 (1972).

210. *See* Hassan v. City of New York, 804 F.3d 277, 289–309 (3d Cir. 2015).

211. Black Lives Matter v. Town of Clarkstown, 354 F. Supp. 3d 313, 323–25 (S.D.N.Y. 2018); *see also* Lozman v. City of Riveria Beach, 138 S. Ct. 1945, 1953–55 (2018) (recognizing the availability of a First Amendment retaliatory arrest claim against a municipality where the retaliatory animus is a part of municipal policy, custom, or practice).

212. *See* 804 F.3d at 309.

213. *See id.*

214. *See* U.S. CONST. amend. IV (protecting persons, houses, papers, and effects from unreasonable searches and seizures absent a warrant supported by probable

the search is private, and these expectations must be objectively reasonable.[215] Both the content of communications and an individual's location when making them may fall under its protections.[216] In cases involving tangible private property, individuals also enjoy freedom from a trespassing government's physical intrusions.[217] As a general rule, officers must first obtain a warrant supported by probable cause of criminal activity before conducting an invasive search of homes, persons, or effects.[218]

The Fourth Amendment's privacy protections are not limitless. One major limitation is the Third Party doctrine, which removes protections from information that is voluntarily offered to a third party.[219] An affirmative, voluntary publicizing of this information effectively negates the objective reasonableness of any privacy expectations.[220] In addition, the government's interest in protecting public safety may authorize warrantless searches under one of the Supreme Court's common law exceptions to the Fourth Amendment's warrant requirement.[221]

Several surveillance tactics used by police departments implicate Fourth Amendment privacy rights. First is the use of Geofeedia

---

cause); Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring) (recognizing Fourth Amendment protections for an individual's reasonable expectations of privacy).

215. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[The] twofold requirement [for the protections of the Fourth Amendment asks] first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

216. *See, e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) (protecting the content of cell phone communications); Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (protecting cell phone location records).

217. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (protecting vehicles from the warrantless implantation of GPS devices).

218. *See* Illinois v. Gates, 462 U.S. 213, 225–46 (1983).

219. *See* United States v. Miller, 425 U.S. 436, 442–43 (1976).

220. *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." (citations omitted)).

221. *See, e.g.*, Kentucky v. King, 563 U.S. 452, 460 (2011) (recognizing a warrantless search as justified where exigent circumstances make obtaining a warrant objectively unreasonable).

and other social media collators.[222] These tools permit law enforcement to see the location of a social media posting based upon searches that target either the posting's content or the identity of the poster.[223] As of 2019, courts have yet to assess the constitutionality of such tools being employed against individuals engaging in political discourse.

However, general Fourth Amendment principles may inform the analysis. The public nature of the internet strips Fourth Amendment protections from the content of postings that an individual or organization voluntarily releases into the public sphere.[224] Under this application of the Third Party doctrine, it logically follows that any subjective expectations of privacy in the content of public postings are by their very nature unreasonable.[225] However, an individual's location when posting this information presents a different story. Movements, even those made in public, may hold reasonable expectations of privacy.[226] It is reasonable to believe that an individual who opts not to share his location on social media intends to keep his location private. If social media collators are able to track the location of a post through means other than an individual's voluntary, affirmative act in sharing his location, then these tools run the risk of intruding into constitutionally protected privacy realms.[227]

---

222. Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 9–14.

223. Geofeedia also features real-time facial recognition scanning software, which enabled Baltimore police to identify individuals with outstanding warrants that were participating in the protests following the death of Freddie Gray. GEOFEEDIA, BALTIMORE COUNTY POLICE DEPARTMENT AND GEOFEEDIA PARTNER TO PROTECT THE PUBLIC DURING FREDDIE GRAY RIOTS, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf (last visited Sept. 23, 2019).

224. The Third Party doctrine from *Miller*, 425 U.S. at 442–43, can reasonably be expected to apply to this scenario.

225. *See* Levinson-Waldman, *supra* note 81, at 532 ("When it comes to social media, it is something of an uphill battle to argue that there is an expectation of privacy in information that is shared online; for that to change, courts will need to begin to reconsider the dogma that privacy requires secrecy.").

226. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

227. Presently available information does not specify the extent to which social media collators are able to source someone's location when it hasn't been affirmatively shared with the social media site. This Note assumes that, for the sake of argument, current technology is capable of sourcing such information. At any rate, rules

This intrusion is further heightened in situations where location-monitoring tools are used to pick up on the location of social media activities other than posts, such as "commenting," "liking," "following," and similar activities. Modern cell phones constantly track even passive activity, such as social media updates.[228] If social media collators can track an individual's location at the time his social media account receives these updates, these tools may provide new capabilities for law enforcement to surveil an individual's location in contradiction to principles underlying *Carpenter*.[229] Social media collators thus present a great, and largely unchallenged, threat to the personal privacy of ordinary, law-abiding citizens. Where such considerations influenced the *Carpenter* Court's decision to impose the warrant requirement for seizures of cell phone location records, courts should find the application of private social media location-tracking tools unconstitutional in the absence of probable cause of criminal activity.[230] However, if a showing of probable cause or a factual basis for the warrant exception does apply, police can freely and legally interfere with privacy rights by tracking an individual's movements through social media collator software.

Another surveillance tactic subject to Fourth Amendment scrutiny is the use of undercover policing by fake Facebook profiles and

must be adopted that do not leave individuals at "the mercy of advancing technology." Kyllo v. United States, 533 U.S. 27, 35 (2001).

228. *See Carpenter*, 138 S. Ct. at 2220.

229. *See id.* at 2216–23.

230. *See id.* at 2217–20.

cell phone numbers.[231] It is well-established that an individual maintains an expectation of privacy in communications made in private.[232] Communications between activists in private text or social media messages—and perhaps even in Facebook groups that closely guard membership to selected private individuals—appear to reflect *subjective* expectations of privacy among inter-group communications. It has further been established, however, that privacy expectations may not be *objectively* reasonable when the communications are made in furtherance of a criminal conspiracy.[233] Under such circumstances, surveillance through the infiltration of undercover officers is permissible.[234] However, law enforcement agencies generally bear the burden of proving some level of suspicion that First Amendment-protected activities are unlawful.[235] Vague justifications such as "to protect 'domestic security'" are generally insufficient to overcome this burden.[236]

By using online personas and electronic means to present themselves as sympathetic to an activist group's cause, undercover officers

231. *See, e.g.*, Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 9–14 (discussing the use of fake Facebook accounts and cell phone numbers to infiltrate activist groups). A separate but related issue is whether the presence of undercover operatives at private group meetings—often held on private property—poses the possibility of violating Fourth Amendment privacy rights. The law governing this issue has remained unsettled since the Court's decision in *United States v. White*, 401 U.S. 745 (1971). However, one could offer at least two arguments in favor of finding a violation: first, under the reasoning employed in the *White* plurality, an objectively justifiable expectation of privacy does exist because the group's activities were lawful and thus distinguishable from the criminal conspiracy surveilled in *White*; and second, based on Justice Douglas's dissent, judicial permission for such activities poses a high likelihood of chilling First Amendment rights. Because the focus of this Note is addressing privacy concerns stemming from the use of software surveillance and technology, this Note will not elaborate further on the issue of covert informant surveillance but will leave that topic open for future discussion.

232. *See generally* Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

233. United States v. White, 401 U.S. 745, 750–54 (1971).

234. *Id.*

235. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978) (articulating the standard to be "reasonable belief" of criminal activity); Alliance to End Repression v. City of Chicago, 627 F. Supp. 1044, 1056 (N.D. Ill. 1985) (imposing a "reasonable suspicion" standard for the surveillance of political activists); Jabara v. Kelley, 476 F. Supp. 561, 572–73 (E.D. Mich. 1979) (requiring a "good faith" basis for law enforcement to investigate political activists), *vacated by* 691 F.2d 272 (6th Cir. 1982).

236. *Keith*, 407 U.S. 297, 313–14 (1972).

can effectively gain the trust of group members and exploit this trust to receive otherwise undiscoverable information. The Court has never clarified whether *On Lee*'s rule still applies to render undercover electronic surveillance permissible if the agent is voluntarily invited into a group's inner circle. However, recent Supreme Court decisions emphasize the stark contrast between the limited capabilities of 1950s and 1960s recording devices and the sophisticated nature of modern technology.[237]

In the modern era, it is relatively easy for undercover officers to create fake online identities, use unregistered cellphone numbers, and employ other technological tools to infiltrate activist groups.[238] Given the magnitude of private information available to an undercover agent through use of these deceptive techniques, the privacy interests of group members should be balanced against an overextension of police powers. This particularly holds true when there is no ascertainable evidence that the group engages in regular or ongoing criminal activity. When agents continuously and covertly monitor the lawful activities of activists through private social media connections, the facts support finding an unreasonable intrusion of the sort found objectionable in Justice Alito's *Jones* concurrence and Chief Justice Roberts's majority opinion in *Carpenter*.[239]

The final fact to consider is the collection, maintenance, and dissemination of personal information concerning targeted activists.[240] Where this information is classified and kept from public domain, it may fall squarely beneath the Fourth Amendment's protections for an individual's reasonable expectations of privacy.[241] If the individual enjoys an established right to keep this information private and if inter-

237. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); United States v. Jones, 565 U.S. 400, 427–31 (2012) (Alito, J., concurring in judgment).

238. *See, e.g.*, Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 9–14.

239. *See* cases cited *supra* note 237.

240. *See* Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 9–14.

241. For example, information concerning one's "familial, political, professional, religious, and sexual associations" is likely to receive Fourth Amendment protections. *See Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

departmental policy supports maintaining and disseminating this information outside of law enforcement, reputations may suffer actual and concrete damage from this publicization.[242] Such stigmatizing injuries may be sufficient to overcome standing hurdles otherwise posed by *Laird* and its progeny.[243]

B. Procedural and Policy Solutions

The problems articulated in Parts II, III, and IV of this Note demonstrate the need to reform modern police practices concerning the surveillance of socio-political activist groups. Ideally, reformative measures should remedy constitutional violations while still allowing law enforcement leeway to investigate actual criminal activity. This reform could be achieved through litigation that establishes binding precedent or a consent decree that can be enforced against the police. However, given the costs of litigation, a more effective solution likely lies in policy-based reforms.

1. Procedural Solutions

Courts may be able to provide relief for activists that have been targeted by municipal police surveillance. The appropriate vehicle for seeking relief depends in part upon the amount of information available to activist plaintiffs, the extent and nature of the plaintiffs' injuries, and the availability of local precedent or law prescribing limits to political surveillance. Three broad categories of procedural vehicles[244] may be available to activists: records requests, constitutional claims, and statutory claims.

First, individuals may seek information about law enforcement's activities and practices under federal or state open records

242. Where false information is disseminated, a plaintiff may be able to state a claim for defamation. *See* RESTATEMENT (SECOND) OF TORTS § 558 (AM. LAW INST. 1977).

243. *See supra* notes 180–90, 209–13.

244. Another potential solution is Department of Justice (DOJ) intervention. The DOJ has statutory authority to intervene where police practices regularly and systematically infringe upon the rights of state citizens. *See* 34 U.S.C. § 12601 (2018).

laws.[245] If law enforcement agencies refuse to turn over records mandated by statute, activists can seek a court order to compel law enforcement to release the records.[246] Although records requests do not provide direct relief for enjoining police conduct, these procedural vehicles may produce critical information needed for drafting pleadings. Furthermore, activists should use the information recovered from records requests to lobby local legislative bodies to enact reformative policies.[247]

Second, if activists can state a facially plausible claim that they were personally injured by targeted police surveillance,[248] plaintiffs may be able to bring civil rights actions under 42 U.S.C. § 1983 against officers[249] or municipalities[250] for violating their constitutional rights.[251] Although qualified immunity generally protects police officers from suit, plaintiffs may be able to overcome a qualified immunity defense if the violated constitutional right—such as First Amendment expressive or association rights or Fourth Amendment privacy rights—was clearly established at the time of the violation.[252]

Finally, where existing consent decrees, state laws, or municipal ordinances already offer standards for constraining police surveillance practices, plaintiffs may be able to seek remedies for the violation of these laws.[253] If the suit concerns the violation of a consent decree, the

245. *See, e.g.*, 5 U.S.C. § 552 (2018) (codifying the Freedom of Information Act); TENN. CODE ANN. § 10-7-503 (2018) (codifying the Tennessee Public Records Act).

246. *See, e.g.*, TENN. CODE ANN. § 10-7-505 (2018) (providing individuals with a cause of action for an official's failure to comply with an authorized public records request). Most states have enacted similar provisions to compel government agencies to release information. *See generally* SOPHIE WINKLER, NAT'L ASS'N OF CTYS., OPEN RECORD LAWS: A STATE BY STATE REPORT (2010), https://www.governmentecmsolutions.com/files/124482256.pdf

247. *See infra* Section IV.B.2.

248. *See* Black Lives Matter v. Town of Clarkstown, 354 F. Supp. 3d 313, 323–24 (S.D.N.Y. 2018).

249. Alternately, if the officers are federal, a claim could be brought under *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).

250. *See* Monell v. Dep't of Soc. Servs., 436 U.S. 658, 691–95 (1978) (recognizing claims against municipalities based on official custom, policy, or practice).

251. *See* 42 U.S.C. § 1983 (2018).

252. *See, e.g.*, *Black Lives Matter*, 354 F. Supp. 3d at 326–27.

253. As discussed in Parts I and II of this Note, two notable examples of existing laws that limit police surveillance activities are Memphis's Consent Decree from *Kendric*k and New York's *Handschu* Guidelines. *See supra* Parts I, II.

plaintiffs bringing suit for contempt must be parties to the original consent decree or an original party's successors-in-interest.[254] Alternatively, if law enforcement surveillance operations violate a state law or municipal ordinance, activists can pursue statutory claims for these violations.[255]

The general availability of these procedural vehicles does not mean that litigation is always the best solution for resolving police surveillance issues. It can take years and prove costly for lawsuits to reach final resolutions. Furthermore, a successful outcome is never guaranteed but depends upon each case's discrete set of facts. For these reasons, non-adversarial methods may provide a more effective solution for reform.

2. Policy Solutions

The best way for cities and states to avoid spending tax-payer money on costly litigation and to deter law enforcement officers from problematic surveillance conduct is to reform existing policies. Effective reform could be achieved in a number of different ways. Whether implemented through municipal ordinance or state statute, policymakers should consider implementing four categories of reformative measures: (1) definitional limits to the scope of permissible police surveillance; (2) training requirements to prevent police from abusing surveillance technologies; (3) oversight provisions to hold law enforcement accountable to the community in which it serves; and (4) enforcement clauses giving private citizens a cause of action against unlawful surveillance conduct.

254. Order Denying the City's Motion for Summary Judgment on the Issue of Standing at 12–13, Blanchard v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. July 30, 2018), ECF No. 117.

255. Statutory actions against private entities that are cooperating with law enforcement may also be available. *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264, 1274–75 (9th Cir. 2019) (recognizing a class action against Facebook for violating Illinois's Biometric Information Privacy Act through use of its facial-recognition software).

i. Definitional Limits

Ordinances and statutes should be enacted to constrain the scope of permissible police surveillance practices. This approach would generally require policymakers to provide police with explicit definitions and standards of what is and what is not appropriate surveillance behaviors. While not legislative in origin, the Consent Decree resolving Memphis's *Kendrick* case[256] offers a useful model.

First, the Decree broadly defines political intelligence as "the gathering, indexing, filing, maintenance, storage[,] or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations[,] or other exercise of First Amendment rights."[257] Second, the Decree strictly prohibits the police from engaging in political surveillance without any consideration of intent; in other words, political intelligence conducted for any purpose—other than active criminal investigations under certain specified circumstances—effectively violates the prohibition.[258] Third, the Decree prohibits several other activities that *do* consider law enforcement's purposes, such as "operat[ing] or maintain[ing] any office, division, bureau[,] or any other unit *for the purpose of engaging in political intelligence*" and "intercept[ing], record[ing], transcrib[ing,] or otherwise interfer[ing] with any communication by means of electronic surveillance *for the purpose of political intelligence*."[259] Fourth, the Decree explicitly prohibits the police from recruiting informants and infiltrating First Amendment-protected groups using undercover agents.[260] Fifth, the Decree defines and prohibits four different types of harassing police behaviors aimed at chilling free speech.[261] Sixth, the Decree prohibits the maintenance and dissemination of information gained through political surveillance.[262]

256. *See supra* notes 4–15 and accompanying text.

257. Order, Judgment & Decree, *supra* note 11, at 2.

258. *See id.* at 3; *see also* Order Granting in Part & Denying in Part the ACLU's Motion for Summary Judgment & Order Denying the City's Motion for Summary Judgment on the Issue of Contempt, *supra* note 4, at 22–29.

259. Order, Judgment & Decree, *supra* note 11, at 3 (emphasis added).

260. *Id.*

261. *Id.* at 3–4.

262. *Id.* at 5.

While the *Kendrick* Decree is useful for these broad definitions and rules, policymakers should also supplement proposed bills with explicit provisions concerning technology. Recently, Seattle passed a comprehensive ordinance that includes, among other things, a transparent definition of surveillance technologies.[263] The definition of surveillance in the Seattle Surveillance Ordinance encompasses technologies "that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equality[,] or social justice."[264] Notably, the ordinance excludes technologies that are essential for police and protective for citizens, such as office equipment and body cameras.[265] The exceptions are to maintain the effectiveness of law enforcement despite reformative measures to technologies policies.

ii. Training Requirements

Policymakers should also implement training requirements to reduce instances of racial or partisan policing,[266] better educate police on actual extremist behaviors,[267] and ensure that police do not infringe upon the constitutional rights of ordinary, law-abiding citizens. For a model of how this might work, policymakers can look to the sanctions the court imposed on MPD in *Blanchard*.

The sanctions in *Blanchard* first required officers to undergo training to understand how even well-intended investigations can violate the First Amendment rights of law-abiding citizens.[268] Thus, the court directed police leadership to explain that every investigation into

263. *Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, ACLU WASH. (Aug. 8, 2017), https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology.

264. SEATTLE, WASH., MUN. CODE § 14.18.010 (2017).

265. *See* Saad Bashir, *About the Surveillance Ordinance*, SEATTLE INFO. TECH., https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance (last visited Nov. 21, 2019); *see also* SEATTLE, WASH., MUN. CODE §§ 14.18.010 –.080 (2017).

266. *See supra* note 81 and accompanying text.

267. *See supra* note 82 and accompanying text.

268. Opinion & Order, *supra* note 36, at 33.

the lawful exercise of First Amendment constitutes political surveillance, regardless of the underlying motive for the investigation.[269] The training requirements also sought to correct officers' misperceptions about their investigative duties by emphasizing that political intelligence is not permissible as either a "means or an ends of an otherwise lawful investigation."[270] Furthermore, the court required police leadership to train officers on the proper protocols for authorizing criminal investigations that interfere with First Amendment rights.[271] Finally, the court required police leadership to establish written guidelines for electronic surveillance and train officers on the appropriate protocols.[272] Policymakers should strive to implement training programs such as these. Familiarizing officers with the practical and constitutional issues implicated by political surveillance practices will help reduce instances of technological surveillance abuse.

iii. Oversight Provisions

Legislators should also enact laws that provide comprehensive oversight of police surveillance operations.[273] The authority to oversee surveillance operations could be placed with elected officials, an independent government regulatory board, or a civilian regulatory board. Likewise, cities could employ a hybrid model containing multiple levels of oversight.[274]

The Seattle Surveillance Ordinance offers a model for a hybrid oversight approach.[275] This ordinance contains multiple provisions giving different individuals or groups a role in technology surveillance decisions: for example, the Surveillance Ordinance requires law enforcement to present new surveillance technologies at community

269. *Id.*

270. *Id.*

271. *Id.* at 33–34.

272. *Id.* at 34–35.

273. *See, e.g.*, *Community Control Over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (offering model ordinances for cities seeking to reform police surveillance practices) (last visited Nov. 21, 2019).

274. Policymakers could also place greater oversight responsibilities upon internal affairs departments within law enforcement agencies. However, oversight outside of law enforcement provides a more comprehensive check against surveillance abuse.

275. *See* SEATTLE, WASH., MUN. CODE §§ 14.18.010 –.080 (2017).

meetings prior to approval; it requires monthly surveillance usage and impact assessments to be reported to the public; it provides the City Council with approval and oversight authority; and it authorizes a newly-formed surveillance advisory board to directly oversee surveillance practices.[276] Seattle's ordinance is the most comprehensive surveillance oversight bill to date, giving the community, elected officials, and a regulatory board an oversight role over police surveillance operations. [277]

A proposed bill in California takes a somewhat similar approach but leaves oversight responsibility to elected officials.[278] This bill would require law enforcement to propose operation rules and obtain approval from local officials prior to acquiring or using any new surveillance technology system.[279] Although less comprehensive than Seattle's Surveillance Ordinance, this bill still promises a much-needed level of oversight.[280]

Another way cities could increase oversight is by authorizing civilian review boards to review police practices, offer recommendations, and investigate civilian complaints.[281] Civilian review boards are composed of ordinary citizens that are appointed to oversee law enforcement practices, make findings, and propose recommendations to the City Council or police agencies.[282] If given subpoena authority,

276. *Seattle Adopts the Nation's Strongest Regulations for Surveillance Technology*, *supra* note 263; *see also* §§ 14.18.010 –.080 (2017).

277. *Seattle Adopts the Nation's Strongest Regulations for Surveillance Technology*, *supra* note 263; *see also* §§ 14.18.010 –.080 (2017).

278. *See* Jerry Hill, *Stop Secretive Surveillance (SB 1186)*, ACLU N. CAL., https://www.aclunc.org/our-work/legislation/stop-secretive-surveillance-sb-1186 (discussing proposed California Senate Bill 1186) (last visited Nov. 21, 2019).

279. Chloe Triplett, *Police Are Acquiring Surveillance Tech in Secret. A California Bill Would Give the Public a Say.*, ACLU N. CAL. (Aug. 7, 2018), https://www.aclunc.org/blog/police-are-acquiring-surveillance-tech-secret-california-bill-would-give-public-say.

280. *See id.*

281. *See* Olugbenga Ajilore, *How Civilian Review Boards Can Further Police Accountability and Improve Community Relations*, SCHOLARS STRATEGY NETWORK (June 25, 2018), https://scholars.org/brief/how-civilian-review-boards-can-further-police-accountability-and-improve-community-relations.

282. *See id.* Memphis has a civilian review board known as the Civilian Law Enforcement Review Board ("CLERB"). *About*, CIVILIAN L. ENFORCEMENT REV. BOARD, https://clerbmemphis.org/about/ (last visited Nov. 21, 2019). However, CLERB's lack of authority to effectively change police practices has been a point of controversy since its founding, and the board has been criticized by its own members.

such commissions may prove to be an effective and powerful force in constraining law enforcement. [283]

iv. Enforcement Clauses

With any reformative ordinance or statute, policymakers should include an enforcement provision with two important functions. First, the provision should authorize an administrative official to enforce noncompliance with existing regulations. Second, the provisions should create a private cause of action in the event that police violate other reformative provisions.

Seattle's Surveillance Ordinance contains a model provision.[284] Section 14.18.070 of the Seattle Municipal Code authorizes the City's Chief Technology Officer to direct noncompliant departments to cease acquiring or using surveillance technology.[285] Furthermore, it creates a private cause of action for individuals that have been surveilled and injured by a material violation of the Surveillance Ordinance.[286]

An enforcement provision is necessary within any reformative scheme. Such a provision serves the important purpose of holding law enforcement agencies accountable for unlawful surveillance actions. While this proposed provision opens the door to possible litigation, the threat of liability may act as a powerful deterrent against police misconduct. Furthermore, the provision will give injured parties a chance to seek judicial relief where they would not otherwise have standing to do so.

Brandon Richard, *Civilian Review Board Feels it has "No Power" When Overseeing MPD*, WMC ACTION NEWS 5 (Aug. 14, 2018, 10:27 AM), http://www.wmcactionnews5.com/story/38233702/civilian-review-board-feels-it-has-no-power-when-overseeing-mpd/.

283. The establishment of Newark's civilian review board model, which vests the review board with investigative subpoena power, has been lauded by scholars and citizens alike. *See, e.g.*, Alecia McGregor, *Politics, Police Accountability, and Public Health: Civilian Review in Newark, New Jersey*, 93 J. URB. HEALTH 141, 146 (Supp. I 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4824694/pdf/11524_2015_Article_9998.pdf.

284. *See* SEATTLE, WASH., MUN. CODE § 14.18.070 (2017).

285. *Id.* § 14.18.070(A).

286. *Id.* § 14.18.070(B).

V. CONCLUSION

When the Framers of the Constitution drafted the First and Fourth Amendments, they sought to protect the rights of private citizens to freely speak, petition, and peacefully assemble against those in power without the fear of government retaliation. Modern technology has enabled law enforcement to contravene these core constitutional principles at the expense of individual privacies. *Blanchard* thus illustrates a pervasive national issue: the domestic surveillance of political activists by municipal police armed with advanced technological tools. These invasive spying practices violate the privacy rights of ordinary citizens and lack grounds for justification where no criminal activity is present. Balance should be restored to the relationship between political activists and government by judicial means and policy solutions.