Journal of Criminal Law and Criminology

Volume 111
Issue 4 *Fall*

Article 3

Fall 2021

Don't (Tower) Dump on Freedom of Association: Protest Surveillance Under the First and Fourth Amendments

Ana Pajar Blinder

0091-4169/21/11104-0961
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 111, No. 4
 Printed in U.S.A.

COMMENTS

DON'T (TOWER) DUMP ON FREEDOM OF ASSOCIATION: PROTEST SURVEILLANCE UNDER THE FIRST AND FOURTH AMENDMENTS

Ana Pajar Blinder*

Government surveillance is ubiquitous in the United States and can range from the seemingly innocuous to intensely intrusive. Recently, the surveillance of protestors—such as those protesting against George Floyd's murder by a police officer—has received widespread attention in the media and in activist circles, but has yet to be successfully challenged in the courts. Tower dumps, the acquisition of location data of cell phones connected to specific cell towers, are controversial law enforcement tools that can be used to identify demonstrators. This Comment argues that the insufficiency of Fourth Amendment protections for protesters being surveilled by government actors—by tactics such as tower dumps—can be solved by conducting independent First Amendment analyses. A multi-factor balancing test can assist the courts as they consider the scope and pervasiveness of technology such as tower dumps against the potential chilling effects on First Amendment-protected activity, providing a framework to assess the constitutionality of surveillance technology used during mass protests.

* Northwestern University Pritzker School of Law, J.D., expected May 2022. University of Pennsylvania, B.A. 2015. A big thank you to Professor Matthew Kugler for advising and sharing his expertise on several drafts of this Comment. I am additionally grateful to Professor Jason DeSanto and Nate Wessler for their helpful discussions.

INTRODUCTION

Officer Derek Chauvin kneeled on George Floyd's neck for nearly eight minutes,[1] reigniting momentum to protest police brutality and systemic racism.[2] A wave of local, national, and, ultimately, global protests ensued. The moment transformed into a movement, with grassroots action and accompanying social media conversation developing from focus on George Floyd to a broader Black Lives Matter message.[3] Drawing comparisons to the United States civil rights movement of the 1960s, the protests in summer 2020 were responsive to similar violence and systemic racism plaguing Black Americans of the past, but proved to be more intersectional and coalition based.[4]

The Black Lives Matter demonstrations, however, were not immune to governmental efforts to impede, infiltrate, or monitor activism. Instead, they magnified the inextricability of protest and surveillance. Modern innovation

---

[1] *Prosecutors: Derek Chauvin Had Knee on George Floyd for 7:46, Not 8:46*, CBS MINN. (June 17, 2020, 10:42 PM), https://minnesota.cbslocal.com/2020/06/17/prosecutors-derek-chauvin-had-knee-on-george-floyd-for-746-not-846 [https://perma.cc/VQD4-ZKEM].

[2] Eliott C. McLaughlin, *How George Floyd's Death Ignited a Racial Reckoning that Shows No Signs of Slowing Down*, CNN (Aug. 9, 2020, 11:31 AM), https://www.cnn.com/2020/08/09/us/george-floyd-protests-different-why/index.html [https://perma.cc/JC65-RMXH].

[3] Mary Blankenship & Richard V. Reeves, *From the George Floyd Moment to a Black Lives Matter Movement, in Tweets*, BROOKINGS INST. (July 10, 2020), https://www.brookings.edu/blog/up-front/2020/07/10/from-the-george-floyd-moment-to-a-black-lives-matter-movement-in-tweets [https://perma.cc/QM5A-HPPU].

[4] Thomas J. Sugrue, *2020 is Not 1968: To Understand Today's Protests, You Must Look Further Back*, NAT'L GEOGRAPHIC (June 11, 2020), https://www.nationalgeographic.com/history/2020/06/2020-not-1968 [https://perma.cc/P4HL-ABBE].

has made these efforts more sophisticated, but even older forms of technology were also used to stifle dissidence.[5]

Today, government infiltration into perceived dissident groups' activities has been supplanted by advanced surveillance technologies utilizing biometrics, cell phone tracking, and social media monitoring.[6] Americans have dealt with policing perceived threats at the expense of constitutional freedoms for a long time,[7] but technology has changed how aware individuals are of the government's tactics. National security was often invoked to justify surveillance in the past, as it is invoked now.[8] However, today, the tools used by government actors are much further reaching than they were earlier in the 20th century, creating more onerous conditions and greater threats to free speech and association. The inevitable collapse of the distinction between national security and domestic protest—through methods such as designating domestic groups as terrorist organizations—poses graver surveillance concerns and risks of First Amendment infringements.[9] For example, the Department of Justice

---

[5] In the 18th century, fearing insurrectionist enslaved people, New York passed ordinances requiring unaccompanied slaves to carry lanterns in the dark so they could be monitored. *See* Dorothy Roberts & Jeffrey Vagle, *Racial Surveillance Has a Long History*, HILL (Jan. 4, 2016, 5:11 PM), https://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history [https://perma.cc/LC84-DZHP]. In addition, in the 1960s, one of the FBI's most notorious surveillance campaigns, COINTELPRO, was designed to monitor what the Bureau, rather capriciously, considered radical dissident groups. Targets included the Black Panthers and Martin Luther King, Jr. *See* Stanford Univ., *Federal Bureau of Investigation (FBI)*, MARTIN LUTHER KING, JR. ENCYCLOPEDIA https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi [https://perma.cc/DQ4C-43Y2] (last visited Aug. 8, 2021).

[6] Albert Fox Cahn & Zachary Silver, *The Long, Ugly History of How Police Have Tracked Protestors*, FAST CO. (June 2, 2020), https://www.fastcompany.com/90511912/the-long-ugly-history-of-how-police-have-tracked-protesters [https://perma.cc/5MU5-E9TM].

[7] *Id.*

[8] Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1, 3 (2004) (explaining how staving off the threat of terrorism is used to justify FISA's broad permission of warrantless electronic surveillance); L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 6 VAND. L. REV. 1343, 1351–52 (2013) (discussing the role of the Fourth Amendment in national security).

[9] "The First Amendment protects the rights of Americans who like spewing 'hateful speech' and 'assembling with others who share the same hateful views,' so 'unless an organization engages solely in unprotected activity, such as committing crimes of violence, any designation of a (U.S.-based) organization as a terrorist organization . . . would likely run afoul of the First Amendment.'" Mike Levine, *Trump Vows to Designate Antifa a Terrorist Group. Here's Why DOJ Officials Call That 'Highly Problematic,'* ABC NEWS (June 1, 2020, 12:58 PM), https://abcnews.go.com/Politics/trump-vows-designate-antifa-terrorist-group-heres-doj/story?id=70999186 [https://perma.cc/ZWB8-W6QB].

tenuously classified demonstrators as "Antifa" members, which the administration sought to designate as a terrorist organization.[10] Similarly, the Drug Enforcement Administration was reportedly granted authority to "conduct covert surveillance" to "assist to the maximum extent possible in the federal law enforcement response to protests which devolve into violations of federal law."[11]

Technology can be helpful for protesters because it memorializes and exposes instances of police violence, simplifies the mass organization and coordination of demonstrations, and provides rapid communications to fellow protestors on how to stay safe.[12] But technology also facilitates surveillance. The state is able to quickly track the movements of protestors both through monitoring of social media chatter and through more invasive tactics such as facial recognition software, drones, and surveillance towers.[13]

This Comment focuses on tower dumps, which are downloads of cellular data acquired when cell phones connect to cell sites.[14] When cell phones are on, they scan for cell towers for connectivity and register location information with the network about every seven seconds.[15] This enables the

---

[10] *Attorney General William P. Barr's Statement on the Death of George Floyd and Riots*, DEP'T OF JUST. (May 30, 2020), https://www.justice.gov/opa/pr/attorney-general-william-p-barr-s-statement-death-george-floyd-and-riots [https://perma.cc/3BLK-UK6R] ("In many places, it appears the violence is planned, organized, and driven by anarchistic and far left extremists, using Antifa-like tactics, many of whom travel from out of state to promote the violence.").

[11] Jason Leopold & Anthony Cormier, *The DEA Has Been Given Permission to Investigate People Protesting George Floyd's Death*, BUZZFEED NEWS (June 2, 2020, 6:48 PM), https://www.buzzfeednews.com/article/jasonleopold/george-floyd-police-brutality-protests-government [https://perma.cc/5YE3-YDVW] (citing Memorandum from Timothy J. Shea, Acting Adm'r, Drug Enf't Admin., to Deputy Att'y Gen. (May 31, 2020), https://www.documentcloud.org/documents/6935297-LEOPOLD-DEA-Memo-George-Floyd-Protests.html [https://perma.cc/YJR5-VVMV]).

[12] *See* Shira Ovide, *How Social Media Has Changed Civil Rights Protests*, N.Y. TIMES (June 18, 2020), https://www.nytimes.com/2020/06/18/technology/social-media-protests.html [https://perma.cc/4U47-R5R2]; Alex Hudson & Peter Price, *How Is Technology Changing Protests?*, BBC (Apr. 12, 2011), http://news.bbc.co.uk/2/hi/programmes/click_online/9451521.stm [https://perma.cc/4S3P-2RLA].

[13] Aaron Holmes, *How Police Are Using Technology Like Drones and Facial Recognition to Monitor Protests and Track People Across the US*, BUS. INSIDER (June 1, 2020, 9:58 AM), https://www.businessinsider.com/how-police-use-tech-facial-recognition-ai-drones-2019-10 [https://perma.cc/RS4X-6EWU].

[14] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[15] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 228 (2011) (statement of the ACLU), https://www.aclu.org/files/assets/senate_hearing_mobile_tracking_may_2011_-_final.pdf [https://perma.cc/6E3L-KM4E] (citing *In re*

generation of a person's location data through cell site location information (CSLI).[16] Acquisition of information about multiple (or all) devices connected to a cell tower at a certain interval is known as a tower dump.[17] For the proceeding reasons, tower dumps have become an increasingly threatening form of government surveillance.

It is hard to avoid having one's data acquired by a tower dump because cell phones automatically connect to towers.[18] There is no ability to anonymize yourself with a mask or rely on glitches with facial recognition. Options to protect digital privacy at protests include employing technologically savvy safeguards such as turning off biometrics, encrypting devices, turning off location services, using airplane mode, or more extreme solutions like leaving your phone at home altogether.[19] These safeguards pose additional risks, as phones are not only inseparable from everyday behavior,[20] but are also important accountability mechanisms to record police misconduct, summon help, or coordinate movements.[21]

Too much surveillance can seriously impede protests. Fearing the systematization of protestors' identifications, future retaliatory behavior, or the surveillance itself, demonstrators become deterred from participating in protests.[22] The fear of government encroachment on protestor privacy has

---

Application of U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008), *vacated*, 620 F.3d 304).

[16] *See* Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and the Need for Fourth Amendment Protections*, 106 J. CRIM. L. & CRIMINOLOGY 167, 173 (2016).

[17] John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013, 6:02 AM), https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809 [https://perma.cc/3RCP-DQYM] ("A typical dump covers multiple towers, and wireless providers, and can net information from thousands of phones.").

[18] Jess Remington, *Police Use "Tower Dumps" to Collect Cell Phone Data Without a Warrant*, REASON (Dec. 4, 2013, 12:34 PM), https://reason.com/2013/12/04/police-use-tower-dumps-to-collect-your-c [https://perma.cc/GJ6T-LAX5].

[19] Alfred Ng, *How to Maintain Your Digital Privacy at Protests*, CNET (June 15, 2020, 12:56 PM), https://www.cnet.com/news/how-to-maintain-your-digital-privacy-at-protests [https://perma.cc/EDU7-8UJZ].

[20] *See* Lynne Peeples, *Can't Put Down the Phone? How Smartphones Are Changing Our Brains – and Lives*, USA TODAY (Dec. 14, 2018, 3:32 AM), https://www.nbcnews.com/mach/science/surprising-ways-smartphones-affect-our-brains-our-lives-ncna947566 [https://perma.cc/F7B8-YUPD].

[21] Matthew I. Lahana, *Destined to Collide: Modern Protests and Warrantless Cell Phone Search Exceptions*, 1 S. CAL. REV. L. & SOC. JUST. 55, 56 (2012).

[22] *See generally* Complaint for Declaratory and Injunctive Relief, Williams v. San Francisco (Cal. App. Dep't Super. Ct. 2020) (No. CGC-20-587008) https://www.aclunc.org/sites/default/files/2020.10.07-Williams-v.-SF-Complaint-filed_0.pdf [https://perma.cc/ZWE

severe chilling effects on demonstrators.[23] Law enforcement, for example, can request all the CSLI from towers to identify common cell phone numbers when allegedly investigating a crime.[24] Practically speaking, under the auspices of identifying a single suspect of an alleged crime at a protest against police brutality, law enforcement could track the locations of all attendees of a protest.[25] Protestors who have nothing to do with the supposed target or purpose of the surveillance can still be grouped into the surveillance, providing ample reason to fear future attendance.

If protests are seriously impeded, First Amendment infringement follows. The Supreme Court has recognized that state actions which do not facially stifle freedom of association can still have the effect of doing so and thereby abridge First Amendment protections.[26] While certain government action may "appear to be totally unrelated to protected liberties,"[27] a closer look can reveal otherwise, such as when surveillance impedes free speech activity. Protestors who know they are under the relentless watch of the government have rightful fears of participation in demonstrations. State action surveilling protestors via tower dumps certainly "may have the effect of curtailing the freedom to associate."[28]

The topic of surveillance is most often discussed in a Fourth Amendment context, but whether the Fourth Amendment would provide

---

9-6KNV] (Plaintiff protestors allege the San Francisco Police Department defied city ordinance and chilled free speech rights by employing dragnet surveillance of summer protests); Umberto Bacchi & Avi Asher-Schapiro, *Debate on Surveillance and Privacy Heats Up as U.S. Protests Rage*, REUTERS (June 1, 2020, 7:53 PM), https://www.reuters.com/article/uk-minneapolis-police-privacy-trfn/debate-on-surveillance-and-privacy-heats-up-as-u-s-protests-rage-idUSKBN23902V [https://perma.cc/74RG-EC3B].

[23] Bacchi & Asher-Schapiro, *supra* note 22.

[24] Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, ATLANTIC (Sept. 11, 2015), https://www.theatlantic.com/technology/archive/2015/09/how-the-government-surveils-cell-phones-a-primer/404818 [https://perma.cc/ZCS4-3FNN].

[25] As historical records from cell tower dumps "provide a listing of any cell phones that have utilized the cellphone tower for a particular time and date," it is plausible law enforcement would have little difficulty identifying a large number of attendees of a protest while ostensibly searching for a specific individual. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 6 (2013) (quoting Criminal Complaint at 13, United States v. Capito (D. Ariz. 2010) (No. 3:10-CR-8050)).

[26] *See* Am. Commc'ns Ass'n v. Douds, 339 U.S. 382, 393 (1950) ("By exerting pressures on unions to deny office to Communists and others identified therein, § 9(h) undoubtedly lessens the threat to interstate commerce, but it has the further necessary effect of discouraging the exercise of political rights protected by the First Amendment.").

[27] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 461 (1958).

[28] *Id.* at 460 (emphasis added).

protection in the context of tower dumps is disputed.[29] This Comment will take a different approach. Regardless of the answer under a Fourth Amendment analysis, tower dumps during mass protests can chill speech and free association enough to warrant heavy scrutiny under a First Amendment framework.[30]

Part I of this Comment outlines the tangible First Amendment harm posed by government use of tower dumps to surveil protestors and how that injury is conceptualized doctrinally. Despite a body of law established to clarify freedom of association protections, First Amendment jurisprudence has not directly or sufficiently addressed the problem in the context of protest in the modern digital age, in large part due to the courts' reliance on and deference to Fourth Amendment doctrine. Part II argues that the Fourth Amendment is an insufficient framework for courts to utilize when addressing the First Amendment implications of technological surveillance of protests. Finally, Part III illustrates how the doctrinal standard used for freedom of association should be applied when the First Amendment is implicated in novel privacy cases.[31]

---

[29] Owsley, *supra* note 25, at 13 ("[T]he development of Fourth Amendment jurisprudence . . . supports the position that Fourth Amendment protections extend to cell tower dumps."); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 104 (2013) ("When unfettered access to those methods raises the specter of a surveillance state, courts have limited their use by applying the Fourth Amendment's reasonableness standards."); Eric J. Struening, *Checked in: Decreasing Fourth Amendment Protection Against Real-Time Geolocation*, 45 U. MEM. L. REV. 561 (2015) (discussing how the Fourth Amendment applies to real-time geolocation surveillance).

[30] U.S. CONST. amend. I.

[31] This Comment also advances its argument with the contextual awareness that while tower dumps are one of the more dangerous ways of infringing on protestors' rights, other technologies used in combination can drive First Amendment harms. *See* Andy Greenberg & Lily Hay Newman, *How to Protest Safely in the Age of Surveillance*, WIRED (May 31, 2020, 3:27 PM), https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy [https://perma.cc/6RZJ-C9PY]; William Roberts, *US Law Enforcement Surveilled Protests with Drones, Spy Planes*, AL JAZEERA (June 11, 2020), https://www.aljazeera.com/news/2020/6/11/us-law-enforcement-surveilled-protests-with-drones-spy-planes [https://perma.cc/892A-5GUH]; Lulu Garcia-Navarro, *How Authorities Can Use The Internet to Identify Protestors*, NPR (June 28, 2020, 7:59 AM), https://www.npr.org/2020/06/28/884351939/how-authorities-can-use-the-internet-to-identify-protesters [https://perma.cc/RD5D-QWVN]. Tower dumps are a timely and relevant example, but there are more possibilities for freedom of association incursions. Facial recognition software, drone surveillance, iris-scanners, ShotSpotter technology, audio surveillance systems, and surveillance cameras are among the many new technologies and tools used by the government to surveil its citizens. Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 999 (2013).

I. THE FIRST AMENDMENT HARM

This Part explains how certain government surveillance threatens free speech. More specifically, this Part argues that the fear of tower dump surveillance may pose a sufficient chilling effect for First Amendment purposes. This Part then details the governing freedom of association doctrine used by courts when speech is chilled, before clarifying that the courts have neglected to apply this doctrine when government surveillance is the subject of legal challenges.

A. THE BURDEN ON PROTEST

Protests play a valuable role in democratic society. Free speech, assembly, and petition help a free society share ideas, create culture, debate, dissent, disrupt, and even invite dispute.[32] One scholar, Jack Balkin, posits that "[a]lthough freedom of speech is deeply individual, it is at the same time deeply collective because it is deeply cultural."[33] Central to these theories of free speech is the right to protest. Some scholars go so far as to contend that assembly is "at least as central to the process of self-governance as is free speech and that assembly and petition were historically viewed as more fundamental to a politically functioning society than speech."[34] One could argue the very foundation of American ideals is predicated on the right to protest.[35] Protests demanding women's right to vote, the March on Washington and other venerable efforts of the civil rights movement, the Stonewall riots, and anti-Vietnam protests all exist in the annals of history as turning points in the slow turn toward progress.[36]

Further, protests advance self-governance by bolstering civic participation and direct democracy, serving as "one particular public opinion signal" that among other resolutions, "may influence[] elected

---

[32] Terminiello v. Chicago, 337 U.S. 1, 4 (1949).

[33] Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 4 (2004).

[34] Ashutosh Bhagwat, *Associational Speech*, 120 YALE L. REV. 978, 981 (2011).

[35] Examples include the Boston Tea Party's demands for representation and the drafters of the First Amendment, borne of the American Revolution, and their understanding of the role of protest in creating popular revolution. SMITHSONIAN INST., PROTEST & PATRIOTISM 5–6, http://smithsonianeducation.org/educators/lesson_plans/protest_and_patriotism/si_protest-and-patriotism.pdf [https://perma.cc/3HGA-AUVE].

[36] Nick Carbone, *Top 10 American Protest Moments*, TIME (Oct. 12, 2011), http://content.time.com/time/specials/packages/article/0,28804,2096654_2096653_2096692,00.html [https://perma.cc/SR4P-WHVC].

representatives."[37] Protests contribute to the marketplace of ideas[38] through the circulation of ideas that critique prevailing policies or respond to minority dissent. Lastly, protests foster self-expression by allowing individuals to form beliefs and then express them.[39] Intrusions on this critical right to protest pose a severe threat to fundamental liberties which form the bedrock of societal participation.

Activist infrastructure has shifted in the digital age, making modern protest ripe for First Amendment infringements. Civic engagement that once relied on face-to-face interactions and traditional organization has been replaced by electronic correspondence and amorphous, but adaptable, networks.[40] Integral to this digital organizing model is the use of cell phones, which protestors use to make organizing more efficient and law enforcement use to track demonstrations.[41] As the Supreme Court has recognized, cell phones are essential accessories in modern life and require greater privacy protection than other physical belongings.[42] The more regularly people use cell phones, the more location data is stored on these omnipresent devices.[43] Further, law enforcement take advantage of this data when tracking individuals.[44]

Thus, technological advancements make way for innovative forms of government surveillance that infringe on protesters' First Amendment rights. One example is tower dumps, a procedure which can "collect all of the historical records that providers maintain from a specific cell tower or towers."[45] Tower dumps, like drone surveillance, facial recognition software, license plate scanners, and social media tracking, are

---

[37] Ruud Wouters & Stefaan Walgrave, *Demonstrating Power: How Protest Persuades Political Representatives*, 82 AM. SOCIO. REV. 361, 362 (2017).

[38] *See* Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821, 821 (2008) (describing the marketplace of ideas as the idea that free speech creates a "competitive environment in which the best ideas will ultimately prevail.").

[39] *See* Thomas I. Emerson, *Towards a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963).

[40] Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 745 (2008).

[41] Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking [https://perma.cc/2BTU-4HQL].

[42] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

[43] Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/E63P-Q2RG].

[44] Zetter, *supra* note 41.

[45] Owsley, *supra* note 25, at 6.

useful surveillance tools for law enforcement,[46] but are uniquely dangerous and increasingly used.[47] They provide an increasingly precise amount of tracking information, including the location and pattern of movements at specific time periods, relative to the location of fixed cell towers.[48] While individual tower dumps are less accurate at location tracking than GPS,[49] cell tower triangulation—tower dumps at multiple cell towers—can help identify individuals across cities and provide bgreatter location accuracy,[50] at times within three-fourths of a mile.[51] As cell towers are in closer proximity to one another in densely populated urban areas, phone location estimations are more accurate in cities than in rural areas.[52] The majority of large protests in summer 2020 took place in cities.[53] Therefore, tower dumps provide law enforcement increasingly accurate information about protesters' locations and have become a very effective surveillance tool.

---

[46] *See* Greenberg & Newman, *supra* note 31; Roberts, *supra* note 31; Garcia-Navarro, *supra* note 31.

[47] The major cellphone providers report thousands of tower dump requests per year. *See* AT&T, TRANSPARENCY REPORT 3 (Aug. 2020), https://about.att.com/ecms/dam/csr/2019/library/transparency/2020-August-Report.pdf [https://perma.cc/LF3B-WU7R] (noting that for the first half of 2020, AT&T reported 1,474 tower dump requests); Verizon Wireless, *United States Report*, VERIZON, https://www.verizon.com/about/portal/transparency-report/us-report [https://perma.cc/7KZC-CPHC] (last visited Aug. 8, 2021) (reporting 1,611 tower dumps for the same time period); T-MOBILE US, INC., TRANSPARENCY REPORT FOR 2019 6 (2020), https://www.t-mobile.com/news/_admin/uploads/2020/07/2019-Transparency-Report-3.pdf [https://perma.cc/44WZ-JESA] (noting that for fiscal year 2019, T-Mobile reported 6,542 tower dump requests).

[48] Amanda Regan, *Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps*, 43 HOFSTRA L. REV. 1189, 1192 (2015).

[49] *See* MINH TRAN, FCC, ACCURATE LOCATION DETECTION 2 (2015), https://transition.fcc.gov/pshs/911/Apps%20Wrkshp%202015/911_Help_SMS_WhitePaper0515.pdf [https://perma.cc/SP6F-U4MU]. In addition, retrospective analyses of individual intervals are coarser, only placing someone within a wider area. Mike Masnick, *Turns Out Cell Phone Location Data Is Not Even Close To Accurate, But Everyone Falls For It*, TECHDIRT (Sept. 9, 2014), https://www.techdirt.com/articles/20140908/04435128452/turns-out-cell-phone-location-data-is-not-even-close-to-accurate-everyone-falls-it.shtml [https://perma.cc/S7BG-YM65].

[50] NAT'L ASSOC. OF CRIM. DEF. LAWS., CELL PHONE LOCATION TRACKING (2016), https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/YR5S-D7CL].

[51] TRAN, *supra* note 49.

[52] *Id.*

[53] Justin McCurry, Josh Taylor, Eleanor Ainge Roy & Michael Safi, *George Floyd: Protests Take Place in Cities Around the World*, GUARDIAN (June 1, 2020, 7:08), https://www.theguardian.com/us-news/2020/jun/01/george-floyd-protests-take-place-in-cities-around-the-world [https://perma.cc/Q6AT-9CXR].

How intrusive or harmful a tower dump is depends on the person experiencing the intrusion. Even a small incursion or seemingly small weight on a scale that limits the size of protests or propensity to protest can be quite powerful for First Amendment purposes.[54] If protestors understand the government is collecting a database of their whereabouts, associations, behaviors, and ideological beliefs, they will fear how this information will be used and become deterred from protesting.[55]

This chilling effect on free speech can have "direct negative implications for democratic governance and social progress."[56] Therefore, even if government use of tower dumps does not physically prevent individuals from protesting, the chilling effect of the surveillance can deter them from demonstrating. Our understanding of technology has changed over time, and in turn made the harm more tangible despite feeling less perceptibly intrusive than a physical halt to a demonstration. As we grow more sophisticated about our understanding of technology, we are able to recognize information gathering is more precise, pervasive, and portable. Surveillance often functions as a chain. What begins as data collection turns into data aggregation, which becomes ripe for misuse without the need for a warrant.[57]

Protestors' speech may be chilled even if their data is not misused immediately following a demonstration. Chilling effects are often predicated on fear. More specifically, "[f]ear or suspicion that one's speech is being

---

[54] Plaintiffs arguing First Amendment claims must "prove only that the officials' actions would have chilled or silenced 'a person of ordinary firmness from future First Amendment activities,' not that their speech and petitioning were 'actually inhibited or suppressed.'" White v. Lee, 227 F.3d 1214, 1241 (9th Cir. 2000) (internal citations omitted).

[55] *See* Letter from H. Comm. on Oversight and Reform to Acting Secretary of Homeland Sec. Chad F. Wolf (June 5, 2020), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-06-05.CBM%20et.%20al%20to%20Wolf-%20DHS%20re%20Peaceful%20Protestors_0.pdf [https://perma.cc/Z5U5-48HG] ("This administration has undermined the First Amendment freedoms of Americans of all races who are rightfully protesting George Floyd's killing."); Lauren Feiner, *We Don't Know How Protests are Being Surveilled. Here's Why That's a Problem*, CNBC (June 13, 2020, 10:15 AM), https://www.cnbc.com/2020/06/13/researchers-politicians-call-for-transparency-in-protest-surveillance.html [https://perma.cc/NAV4-FQDC] ("It's actually scary to imagine how much of our data bodies are kind of within law enforcement systems and how that will be weaponized against us.").

[56] Kelsey Cora Skaggs, *Surveilling Speech and Association: NSA Surveillance Programs and the First Amendment*, 18 U. PA. J. CONST. L. 1479, 1494 (2016).

[57] "Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 320 (1972) [hereinafter *Keith*].

monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas."[58] The fact a portended harm does not occur immediately does not negate that a harm exists. The fear of that harm can be the harm itself.[59] In the context of law enforcement monitoring protests, the concern is not necessarily that acquired data will be misused, but mistrust that it will be misused.[60] The scenario and its burden in question here are distinct from that in *Clapper v. Amnesty International USA*, discussed further in Section B of this Part, in which respondents failed to sufficiently plead that the challenged data collection was happening at all.[61] Here, the debated question is not whether tower dumps are used and systematize location data, but whether fear of how that data will be utilized is sufficient to trigger First Amendment concerns. The number of advice guides provided by civil rights organizations, technology experts, activists, and mainstream media outlets demonstrates evidence of concern of misuse.[62]

---

[58] Bartnicki v. Vopper, 532 U.S. 514, 533 (2001) (quoting PRESIDENT'S COMM'N ON L. ENF'T AND ADMIN. OF JUST., THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967) (internal marks omitted)).

[59] *See* Index Newspapers LLC v. U.S. Marshals Serv., 977 F.3d 817, 826 (9th Cir. 2020) (internal citation omitted) ("A chilling of First Amendment rights can constitute a cognizable injury, so long as the chilling effect is not 'based on a fear of future injury that itself [is] too speculative to confer standing.'"); Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance, and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 647 (2004) ("Many are afraid to speak out when they know, or even suspect, that their speech is being monitored.").

[60] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1130 (2002) ("Being watched can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities."); Bacchi & Asher-Schapiro, *supra* note 22 ("Privacy activists worry that by making it harder for protesters to remain anonymous, surveillance technology deployed by authorities around the globe could have a chilling effect on demonstrations, dissuading people from participating.").

[61] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411 (2013) ("[I]t is no surprise that respondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory . . . respondents do not even allege that the Government has sought the FISC's approval for surveillance of their communications.").

[62] *See Surveilling Self-Defense*, ELEC. FRONTIER FOUND. (Jun. 2, 2020), https://ssd.eff.org/en/module/attending-protest [https://perma.cc/9TFJ-V7BH]; Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, VERGE (Aug. 25, 2020, 3:04 PM), https://www.theverge.com/21401280/android-101-location-tracking-history-stop-how-to [https://perma.cc/FB8C-LV2Q]; Jamie Friedlander, *How to Turn Off Location Services on Your iPhone and Prevent Apps from Tracking You*, BUS. INSIDER (April 11, 2019, 12:40 PM), https://www.businessinsider.com/how-to-turn-off-location-on-iphone [https://perma.cc/LK5A-HM3A]; Maddy Varner, *How Do I Prepare My Phone for a Protest?*, FAST COMPANY (June 6, 2020), https://www.fas

B. WHAT'S A COURT TO DO?

When a sufficient harm to the First Amendment is demonstrated, as above, certain protections are triggered. An entire body of freedom of association law developed over decades paying homage to the sense of importance of people coming together for a common cause.[63] For example, the Court concluded in *NAACP v. Alabama ex rel. Patterson* that "[i]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."[64] In particular, the NAACP refused to comply with a court order demanding it produce the names and addresses of all its Alabama members and detail their roles within the organization.[65] In acknowledging that "compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association," the Court was satisfied with the NAACP's proffered evidence that its ability to pursue its beliefs would be adversely affected.[66] The past occasions of threats, public hostility, and potential loss of employment were enough for the Court to believe members may have been induced to withdraw from the NAACP and dissuade others from joining "because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."[67] The interplay of government action and private community responses was

tcompany.com/90513609/how-do-i-prepare-my-phone-for-a-protest [https://perma.cc/7J32-EFAC] ("David Huerta, a digital security trainer at the Freedom of the Press Foundation, says protesters should be prepared for surveillance of their cellphone's transmissions—even if they don't make any calls.").

[63] *See* Shelton v. Tucker, 364 U.S. 479, 485–86 (1960) ("[T]o compel a teacher to disclose his every associational tie is to impair that teacher's right of free association, a right closely allied to freedom of speech and a right which, like free speech, lies at the foundation of a free society."); Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos., 515 U.S. 557, 568 (1995) (holding that parades are exercises of the right to expressive association, because of the "inherent expressiveness of marching to make a point . . . ."); Gregory v. City of Chi., 394 U.S. 111, 112 (1969) ("Petitioners' march, if peaceful and orderly, falls well within the sphere of conduct protected by the First Amendment"); Edwards v. South Carolina, 372 U.S. 229, 235 (1963) (holding that expressing grievances to the government by protesting and marching "reflect[ed] an exercise of these basic constitutional rights."); Rumsfeld v. F. for Acad. & Institutional Rts., Inc., 547 U.S. 47, 68 (2006) (noting expressive association includes the right to associate "for the purpose of speaking.").

[64] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958).

[65] *Id.* at 451.

[66] *Id.* at 462.

[67] *Id.* at 463.

crucial in this assessment.[68] The chilling effect was the fear of what forced revelation of associations would bring.[69]

In explaining the standard for government regulation, the majority contended even "[s]tate action which may have the *effect* of curtailing the freedom to associate is subject to the closest scrutiny."[70] The sacredness of associating with whom you want—for purposes of expressing shared beliefs and ideologies—is fundamental to the First Amendment.[71] The chilling effect in *Patterson* focused on forced disclosure of membership lists when the Court had yet to "contend with the seismic shifts in digital technology."[72] The use of triangulation to identify and systematize groups of people protesting against police brutality through cell tower dumps threatens freedom to associate much in the same way forcing disclosure of formal membership lists did. Membership lists helped the government identify and categorize individuals based on trends in political ideologies and associations with the NAACP,[73] while triangulation can help law enforcement identify common groups of people protesting police brutality, ostensibly categorizing them by common cause and ideology as well. Furthermore, with much of organizing conducted on social media and other digital platforms, association with movements is not even confined to formal membership.[74]

In 2000, more than forty years after *Patterson*, the Supreme Court reaffirmed that "implicit in the right to engage in activities protected by the First Amendment is a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends."[75] Such an emphasis placed on the inviolability of free speech, assembly, and association—and their intersections—is an important backdrop in assessing the exceptionality of a protest setting when more conventional Fourth Amendment questions emerge.

---

[68] *Id.* It is worth noting, I similarly posit that even if federal or local government officials conduct tower dumps and administer surveillance programs, revelation of association with Black Lives Matter or other protests can result in retaliatory responses from private communities.

[69] *Id.*

[70] *Id.* at 460–61 (emphasis added).

[71] *Id.* at 460.

[72] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

[73] *Patterson*, 357 U.S. at 464–65.

[74] *See* Brooke Auxier, *Activism on Social Media Varies by Race and Ethnicity, Age, Political Party*, PEW RSCH. CTR. (Jul. 13, 2020), https://www.pewresearch.org/fact-tank/2020/07/13/activism-on-social-media-varies-by-race-and-ethnicity-age-political-party [https://perma.cc/CM6B-CCEE]; Ovide, *supra* note 12.

[75] Boy Scouts of Am. v. Dale, 530 U.S. 640, 647–48 (2000) (internal citations omitted).

First Amendment doctrine has long considered chilling effects to be significant encroachments on personal liberty.[76] In the annals of First Amendment law, the courts have found that "informal censorship" may sufficiently inhibit certain behaviors.[77] In *Bantam Books, Inc. v. Sullivan*, Rhode Island formed a commission to "educate the public" on obscene materials and recommend prosecutions for violations.[78] Although the Commission could only apply informal sanctions, the Court found "the threat of invoking legal sanctions and other means of coercion, persuasion, and intimidation . . . demonstrates that the Commission deliberately set about to achieve the suppression of publications deemed 'objectionable' and succeeded in its aim."[79] Freedom of expressive association, therefore, can only "be overridden by regulations adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."[80] In sum, due to the sacredness of the freedom to associate, government regulations that chill free speech must meet strict judicial standards to pass constitutional muster.

C. AVOID THE QUESTION, APPARENTLY

The courts once took seriously the bounds of permissible incursion on the freedom of association. Of note in this arena is the importance of privacy and the threat of indirect restraints on speech.[81] Since then, courts have vacillated between sidestepping First Amendment questions that intersect with privacy concerns and acknowledging the harm of mass data collection

---

[76] *See Patterson*, 357 U.S. at 460 ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment . . . .").

[77] Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 67 (1963).

[78] *Id.* at 59–60.

[79] *Id.* at 67–68. (The Court further described ways in which the Commission's threats manifested themselves in censorial actions, including that "[t]hese acts and practices directly and designedly stopped the circulation of publications in many parts of Rhode Island.").

[80] *Dale*, 530 U.S. at 640–41.

[81] *See Patterson*, 357 U.S. at 462; *Douds*, 339 U.S. 382, 402 (1950) ("But as we have noted, the fact that no direct restraint or punishment is imposed upon speech or assembly does not determine the free speech question. Under some circumstances, indirect 'discouragements' undoubtedly have the same coercive effect upon the exercise of First Amendment rights as imprisonment, fines, injunctions or taxes. A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature.").

on First Amendment activity.[82] This Section will trace this judicial inconsistency before arguing that the original commitment to freedom of association should reign in the digital age.

In the landmark *Keith* case, the Court balanced concerns regarding internal subversion and citizens' rights to privacy.[83] First, the government argued that the state was excepted from a federal law's warrant requirement for wiretaps because of national security concerns.[84] Recognizing the convergence of the First and Fourth Amendments in national security matters, the Court acknowledged the heightened protections needed when surveillance targets are suspected "of unorthodoxy in their political beliefs" and because "[t]he danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'"[85] While the Court held that a warrant was required on solely Fourth Amendment grounds, it importantly noted that "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[86] Such an acknowledgment shows the Court's concern with domestic surveillance of First Amendment activities and the room to expand *Keith* to account for novel First Amendment problems raised by such surveillance.

The Court long ago flagged this intersecting problem in a string of seminal freedom of association cases.[87] It then spent several decades avoiding the issue, often saying that mass data collection was either not truly at issue or was not that damaging.[88] Some lower court cases were brought on

---

[82] *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 821 n.12 (2d Cir. 2015); Laird v. Tatum, 408 U.S. 1, 2–3 (1972); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[83] United States v. U.S. Dist. Ct. E. Dist. of Mich., S. Div., 407 U.S. 297, 312 (1972) (noting the need for government safeguards "does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens.").

[84] *Id.* at 303.

[85] *Id.* at 314.

[86] *Id.* at 320.

[87] *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (acknowledging the intersection of freedom of association and privacy); Bates v. Little Rock, 361 U.S. 516, 523 (1960) (recognizing the "vital relationship" between freedom to associate and privacy); Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 544 (1963) (recognizing the "vital relationship" between freedom to associate and privacy).

[88] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 9 (1972) (noting the complaints of surveillance activities were nonspecific and contained no allegations of illegal activity).

exclusive Fourth Amendment grounds but still sparked conversation about the potential First Amendment questions.[89] In *Klayman v. Obama*, a case challenging the NSA's metadata program, Judge Leon presciently warned in his district court opinion of the "Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States."[90]

Other cases in this jurisprudential era asked the courts more explicitly to take on First Amendment questions, only to be sidestepped in favor of procedural or technical grounds.[91] In *Laird v. Tatum*, activists alleged the Army's domestic surveillance program violated First Amendment rights to protest.[92] The Court considered and decided the action on the basis of ripeness. It held 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."[93] The Court's ripeness analysis seemed to overlap with its discussions on the merits. A diffuse fear of a surveillance system or policy, the majority argued, did not pose enough of a chilling effect on First Amendment rights.[94] Though the Court acknowledged that constitutional

---

[89] *See* Obama v. Klayman, 800 F.3d 559, 563 (D.C. Cir. 2015) (addressing a challenge to NSA's metadata program on explicit Fourth Amendment grounds); United States v. Moalin, 973 F.3d 977, 985–87 (9th Cir. 2020) (detailing how defendants accused of providing material support to al-Shabaab, a U.S.-designated terrorist organization, challenged the government's collection of metadata on Fourth Amendment grounds).

[90] Klayman v. Obama, 957 F. Supp. 2d 1, 33 (D.D.C. 2013).

[91] *See* ACLU v. Clapper, 785 F.3d 787, 821 n.12 (2d Cir. 2015) (holding, in a case challenging the NSA's metadata program, that "because we find that the telephone metadata program exceeds the bounds of what is authorized by § 215, we need not reach either constitutional issue, and we see no reason to discuss the First Amendment claims in greater depth"); *Laird*, 408 U.S. at 12–13; Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013); Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, at 35, *In re* Elec. Priv. Info. Ctr., 571 U.S. 1023 (2013) (No. 13-58) (petitioning to the Supreme Court regarding the NSA's metadata collection program, challenging the program in part on First Amendment grounds, and arguing the "NSA does not need the contents of communications to stifle EPIC's advocacy. The metadata alone is sufficient to identify who has been talking to EPIC and to chill those communications and associations.").

[92] *Laird*, 408 U.S. at 2. President Johnson ordered federal troops to assist with "civil disorders" that arose in the wake of Martin Luther King's assassination, and the Army's data-gathering system was purportedly "established in connection with the development of more detailed and specific contingency planning designed to permit the Army when called upon to assist local authorities, to be able to respond effectively with a minimum of force." *Id.* at 5.

[93] *Id.* at 13–14.

[94] *Id.* at 13.

violations may arise from the deterrent effects of governmental action,[95] it declined to conduct a First Amendment analysis because of the factual differences between the matter at hand and past chilling effects cases.[96]

Similarly, in *Clapper v. Amnesty International USA*, the Court did not consider the merits of a First Amendment argument, but rather decided a challenge to Section 702 of the Foreign Intelligence Surveillance Act of 1978 on standing grounds.[97] The Court relied on its previous reasoning in *Laird* when discounting the First Amendment harm posed by subjective fear of government surveillance programs in *Clapper*.[98] Based on its standards for standing, *Clapper*[99] seems entirely incompatible with *Patterson*, where the Court found fear of both government and private community misuse of disclosed membership information sufficient to confer standing and demonstrate a chilling effect on the right to associate.[100] As discussed, the *Clapper* court found the fear of potential government misuse of surveilled data insufficient to confer standing.[101]

Despite the Court's seeming categorization of fear of government surveillance as an unmeritorious First Amendment burden in both *Laird* and *Clapper*, it took pains to formally decide the cases on other grounds.[102] In *Laird*, the position of the petitioners was deemed insufficient because they failed to establish the foreseeability of the military's misuse of their data.[103] No endorsement of the government's policy was offered.[104] Dissenting opinions criticized categorizing the harm as speculative and remote, instead arguing a "present inhibiting effect on their full expression and utilization of their First Amendment rights" is the proper test for justiciability.[105] In *Clapper*, the Court held respondents failed to demonstrate a "certainly impending" harm.[106] *Clapper* can perhaps be narrowly distinguished from

---

[95] *Id.* at 11 ("In none of these cases, however, did the chilling effect arise merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual.").

[96] *Id.*

[97] 568 U.S. 398, 401 (2013).

[98] *Id.* at 418.

[99] *Id.* at 410.

[100] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958).

[101] *Clapper*, 568 U.S. at 401–02.

[102] See cases cited *supra* note 100; *supra* note 88.

[103] Laird v. Tatum, 408 U.S. 1, 9–10 (1972)

[104] *Id.* at 15.

[105] *Id.* at 25 (Douglas, J., dissenting) (internal marks and citation omitted).

[106] *Clapper*, 568 U.S. at 417.

Patterson in that plaintiff's attorneys in the former asserted their own behavior was chilled by government surveillance,[107] while in the latter, plaintiffs argued their *members*' behavior was chilled due to fear of retaliation.[108] However, this distinction is unavailing and *Clapper* was wrongly decided, for chilling effects turn on the practical effects of discouraging constitutionally protected behavior rather than outright prohibitions of them.[109] Thus, the principles espoused in *Patterson* should have carried over to the Court's reasoning in *Clapper*. It is unlikely a protestor will ever be able to perfectly predict the retaliatory behaviors of government officials or private community members as a result of infringements on associational rights; the justified fear of misuse of data is itself sufficiently inhibiting for purposes of a chilling effect analysis.[110]

While decades of decisions showed the Court's reluctance to confront the merits of First Amendment claims in the surveillance context,[111] a renewed willingness is emerging. For example, the Court has shown increased sensitivity to the problems of mass data collection beginning with

---

[107] *Id.* at 406 (discussing how respondents were human rights attorneys and other organizations who feared surveillance of conversations with clients).

[108] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958) ("[W]e think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.").

[109] *Id.* at 461 (citing Am. Commc'ns Ass'n C.I.O. v. Douds, 339 U.S. 382, 393 (1950)).

[110] George Joseph, *Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 1:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson [https://perma.cc/9BHE-U594] (An activist said in an interview that "[s]urveillance is a tool of fear. When the police are videotaping you at a protest or pulling you over because you're a well known activist — all of these techniques are designed to create a chilling effect on people's organizing. This is no different."); Amna Toor, *"Our Identity is Often What's Triggering Surveillance": How Government Surveillance of #BlackLivesMatter Violates the First Amendment Freedom of Association*, 44 RUTGERS COMPUT. & TECH. L.J. 286, 293 (2018) ("[G]overnment surveillance of associations acts as a censor in deterring individuals from freely engaging with one another.").

[111] *See* Laird v. Tatum, 408 U.S. 1, 13–14 (1972) (decided First Amendment challenge to domestic surveillance program on basis of ripeness); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) (decided challenge to Section 702 of the Foreign Intelligence Surveillance Act of 1978 on surveillance grounds rather than considering merits of First Amendment argument).

Justice Sotomayor's concurrence in *U.S. v. Jones*,[112] and moving through Justice Roberts's opinions in *Riley v. California*[113] and *Carpenter v. United States.*[114] While the aforementioned cases were not raised on First Amendment grounds, its themes were discussed. In her 2012 *Jones* concurrence, Justice Sotomayor sounded the alarms on First Amendment themes, pointing out the amenability of government surveillance technology to misuse, because "[a]wareness that the Government may be watching chills associational and expressive freedoms."[115] Her concern that unfettered government discretion to acquire information about citizens could "alter the relationship between citizen and government in a way that is inimical to democratic society"[116] is echoed in other recent privacy cases.[117] As will be shown in Part II, the Court has yet to grapple with the tension between its newfound awareness of the harms of mass data collection in these Fourth Amendment cases and its legacy of dodging First Amendment issues.[118] However, the Court is now at an opportune moment to revisit its brush with First Amendment analyses in the novel privacy context.

Given how dynamically surveillance tools have developed in the modern protest setting,[119] it is not entirely surprising that the courts have yet to apply a consistent doctrinal framework when such issues arise. But with the scope of surveillance[120] and the infrastructure of protest activities scaling

---

[112] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

[113] Riley v. California, 573 U.S. 373, 403 (2014) ("Modern cell phones are not just another technological convenience . . . The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

[114] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.").

[115] *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

[116] *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, Cuevas-Perez v. U.S., 566 U.S. 1189 (2012)) (internal citation omitted).

[117] *See, e.g.*, *Riley*, 573 U.S. at 403; *Carpenter*, 138 S. Ct. at 2219.

[118] *See infra* Part II.

[119] *See* Greenberg & Newman, *supra* note 31; Roberts, *supra* note 31; Garcia-Navarro, *supra* note 31.

[120] Marguerite Rigoglioso, *Civil Liberties and Law in the Era of Surveillance*, STANFORD LAW. (Nov. 13, 2013), https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance [https://perma.cc/B5SD-5V8C].

up since the 1970s,[121] avoiding First Amendment questions will become impracticable. The deleterious purpose and effects of the surveillance tactics as Justice Douglas recognized them are eerily similar to those posed by tower dumps.[122] The *Laird* plaintiffs' fear that "permanent reports of their activities will be maintained in the Army's data bank"[123] reflects current fears shared by nearly two-thirds of Americans who are concerned about how government collects and uses the data of citizens it surveils.[124] Members of Congress concerned with surveillance tactics employed against protestors also pointed to the recent spike in downloads for encrypted messaging apps "during recent demonstrations, showing a broad concern of surveillance among protesters."[125] As will be shown, this growing problem cannot sufficiently be handled with the Fourth Amendment alone.

II. THE FAILURE OF THE FOURTH AMENDMENT

Part II argues that despite the judicial tendency to rely on the Fourth Amendment when assessing the legality of government surveillance tactics, it is an unreliable doctrinal framework. More specifically, Part II posits that First Amendment concerns are not sufficiently addressed by the modern

---

[121] Ronald Brownstein, *The Rage Unifying Boomers and Gen Z*, ATLANTIC (June 18, 2020), https://www.theatlantic.com/politics/archive/2020/06/todays-protest-movements-are-as-big-as-the-1960s/613207 [https://perma.cc/779J-28M8] (noting recent protests are larger than those in the 1960s and more democratized).

[122] Laird v. Tatum, 408 U.S. 1, 25 (1972) (Douglas, J., dissenting) ("[T]he charge is that the purpose and effect of the system of surveillance is to harass and intimidate the respondents and to deter them from exercising their rights of political expression, protest, and dissent 'by invading their privacy, damaging their reputations, adversely affecting their employment and their opportunities for employment, and in other ways.' Their fear is that 'permanent reports of their activities will be maintained in the Army's data bank, and their 'profiles' will appear in the so-called 'Blaklist' [sic] and that all of this information will be released to numerous federal and state agencies upon request.'").

[123] *Id.*

[124] Brooke Auxier, Lee Raine, Monica Anderson, Andrew Perrin & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/727R-8C9M].

[125] Letter from 116th Cong., to Christopher Wray, Director, FBI 2 (June 9, 2020) https://eshoo.house.gov/sites/eshoo.house.gov/files/Eshoo-Rush%20Ltr%20to%20FBI%2C%20NG%2C%20CBP%2C%20DEA%20on%20government%20surveillance%20of%20protesters%20-%206.9.20.pdf [https://perma.cc/2AEH-WEFP] (citing Nicolas Rivero, *Signal App Downloads Spike as US Protesters Seek Message Encryption*, QUARTZ (June 4, 2020), https://qz.com/1864846/signal-app-downloads-spike-as-us-protesters-seek-messageencryption [https://perma.cc/DF7U-TLBQ]).

privacy cases. Alone, the Fourth Amendment cannot be used to determine whether tower dump requests for data gathered during First Amendment-protected activity should proceed without a warrant.

A. THE FOURTH AMENDMENT'S DOCTRINAL INADEQUACY

At the highest level, the Fourth Amendment protects against unreasonable searches and seizures.[126] Trespasses are searches,[127] as are violations of reasonable expectations of privacy.[128] The warrant requirement of the Fourth Amendment[129] can only be bypassed through certain exceptions.[130] The Supreme Court has held that acquiring certain types of cell phone location data constitutes a search,[131] but has not yet ruled on a warrant requirement for tower dumps specifically.[132] The surveillance of protestors necessarily implicates both the First and Fourth Amendments, particularly against marginalized groups.[133] Yet recent jurisprudence is almost entirely focused on novel privacy concerns—more specifically, how privacy is invaded by modern technology—and how certain electronic devices or data should be protected, or not, under only the Fourth Amendment.[134]

However, at best, the Fourth Amendment would provide uncertain protection in this realm. To start, no Supreme Court case has specifically

---

[126] U.S. CONST. amend. IV.

[127] United States v. Jones, 565 U.S. 400, 406 (2012).

[128] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[129] U.S. CONST. amend. IV.

[130] Kentucky v. King, 563 U.S. 452, 460 (2011). Exceptions include, but are not limited to, certain searches incident to arrest, exigent circumstances, administrative searches, stop and frisk, certain automobile searches, and custodial searches. Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473–74 (1985).

[131] *See Jones*, 565 U.S. at 404 (holding that GPS tracking was a search under the Fourth Amendment); Riley v. California, 573 U.S. 373, 393 (2014) (holding that a warrant is required to search digital data on a phone seized during an arrest, which involves greater privacy interests than a traditional inspection of an arrestee's pockets); Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (holding that the government needs a warrant before acquiring CSLI from a cell carrier).

[132] *Carpenter*, 138 S. Ct. at 2220 (declining to rule on tower dumps).

[133] Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L.J. 527, 553 (2017).

[134] *See* Stephen E. Henderson, *Real-Time and Historical Location Surveillance after* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 809 (2013); Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 411 (2018).

addressed tower dumps.[135] The most recent Fourth Amendment cases assuredly began to grapple with what technological innovations could make their way into existing privacy doctrine.[136] In the oft-cited concurring opinion in *Jones*, Justice Sotomayor presaged the dangers of expansiveness of government surveillance, and the futility of a trespassory test in dealing with forms of surveillance that do not require physical invasion.[137] In acknowledging "[a]wareness that the Government may be watching chills associational and expressive freedoms," Justice Sotomayor went on to question "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs . . . ."[138] However, *Jones* dealt with long-term CSLI monitoring.[139] Tower dumps are not long-term monitoring. They are captures of individual intervals, of a moment in time, or with triangulation, many moments in time.[140]

Nor are tower dumps examples of long-term monitoring of individual persons, as addressed in *Carpenter*.[141] The majority took time to distinguish that cell location information is not "shared" in a typical sense because of its ubiquity in everyday life, and deals with an exhaustive amount of location data incomparable to the limited data dealt with in *Smith*.[142] It is a detailed record of physical locations over a prolonged time, rather than discrete uses. The privacy concerns, the Court reasoned, were greater in *Carpenter* than in *Jones*, as individuals compulsively carry cell phones with them, whereas they regularly leave their vehicles.[143] The Court moves incrementally in extending protections to technologies whose "tracking partakes of many of the qualities" of technologies addressed in previous cases.[144] However, they

---

[135] The Court in C*arpenter* specifically declined to rule on "[r]eal-time CSLI or 'tower dumps.'" *Carpenter*, 138 S. Ct. at 2220.

[136] *See Jones*, 565 U.S. at 404 (holding that GPS tracking was a search under the Fourth Amendment); *Riley*, 573 U.S. at 393 (holding that a warrant is required to search digital data on a phone seized during an arrest, which involves greater privacy interests than a traditional inspection of an arrestee's pockets); *Carpenter*, 138 S. Ct. at 2221 (holding that the government needs a warrant before acquiring CSLI from a cell carrier).

[137] *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

[138] *Id.* at 416.

[139] *Id.*

[140] *See* Kelly, *supra* note 17.

[141] *Carpenter*, 138 S. Ct. at 2217.

[142] *Id.* at 2210.

[143] *Id.* at 2218.

[144] *Id.* at 2216.

specifically have reserved the question of tower dumps.[145] And given that tower dumps generally track "a person's movement at a particular time,"[146] it will be more difficult to argue a Fourth Amendment violation under *Carpenter*. Unless used in combination with other surveillance tools, or spanned across a large timeframe and radius, tower dumps are hardly the "detailed chronicle of a person's physical presence compiled every day, every moment, over several years," that troubled the Court.[147] The venture to persuade the Court will be daunting, given the very narrow conditions under which it decided *Carpenter* and its reluctance to make broader determinations on "conventional surveillance techniques and tools."[148] The Court could not convincingly answer why tower dumps are not "the paradigmatic example of 'too permeating police surveillance' and a dangerous tool of 'arbitrary' authority,"[149] demonstrating the existing hurdles to extending *Carpenter*.

B. JUDICIAL MANEUVERING TO FAVOR THE FOURTH AMENDMENT IGNORES THE PROBLEM

The courts have repeatedly sidestepped a First Amendment inquiry when they are able to maneuver judgments on other technical grounds or Fourth Amendment doctrine.[150] While a school of thought exists positing courts should have an extremely limited role in deciding cases and controversies, the judiciary's decision to ignore First Amendment implications is not an example of laudable minimalism.[151] Consistently forcing free speech-adjacent issues into a Fourth Amendment prism is a refusal to address the developing constitutional threats posed by advancing

---

[145] *Id.* at 2220.

[146] *Id.*

[147] *Id.*

[148] *Id.* at 2267 (Gorsuch, J., dissenting).

[149] *Id.*

[150] *See* Farrah Bara, *From Memphis, with Love: A Model to Protect Protestors in the Age of Surveillance*, 69 DUKE L.J. 197, 208 (2019) ("Courts typically analyze surveillance under the Fourth Amendment"); Hannah Fuson, *Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State*, 50 U. MEM. L. REV. 231, 266 (2019) ("First Amendment surveillance cases are not prevalent among the Supreme Court's jurisprudence."); Caitlin Thistle, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1198 (2008) ("Legal commentators have not paid much attention to the additional and independent First Amendment concerns with the NSA program . . . .").

[151] Minimalist judges focus on the specifics before the court and try to avoid venturing too "far beyond the problem at hand." Cass R. Sunstein, *Beyond Judicial Minimalism*, 43 TULSA L. REV. 825, 826 (2008).

technology used by law enforcement, rather than a principled adherence to a judicial preference for case-by-case judgment.[152] Addressing the First Amendment implications of government technology such as tower dumps is not inconsistent with minimalism; in fact, First Amendment doctrine often favors particularized adjudication.[153] As will be shown in Part III, the courts can and should conduct case-by-case analyses utilizing balancing factors under the First Amendment. The problem with the jurisprudential history of cases dealing with government technology is not courts' need to have a limited counter-majoritarian role and rule as narrowly as possible, but rather, that the First Amendment is a better vehicle for these issues.

Irrespective of a specific potential expansion of *Carpenter*, given the sheer breadth of technological tools used by law enforcement—which will only continue to rapidly develop—the surveillance of protest activities should automatically trigger First Amendment protections. Some privacy proponents have argued for the expansion of Supreme Court trends precluding warrantless government acquisition of individuals' locations.[154] Such scholarship argues that First Amendment concerns posed by government tracking require the Court to extend Fourth Amendment privacy protections to freedom of association matters.[155] However, the Fourth Amendment alone is unsuitable for determining the permissibility of warrantless tower dumps in the protest setting. Fourth Amendment doctrine is often narrowly applied, overly permissive, and has yet to convincingly acknowledge the unique importance of the freedom of association.[156] And despite the constant overlap between the First and Fourth Amendments,

---

[152] Cass R. Sunstein, *Problems with Minimalism*, 58 STAN L. REV. 1899, 1902 (2006) (discussing certain judges' preference for case-by-case analyses instead of bright-line rules, which often result in narrow rulings instead of broad clarifications of law).

[153] For example, the Supreme Court has held that a First Amendment right of public access hinges on passage of the "experience and logic" test. Press-Enterprise Co. v. Superior Ct. of Calif. for Riverside Cty., 478 U.S. 1, 9 (1986). *See also* W. Robert Gray, *Public and Private Speech: Toward a Practice of Pluralistic Convergence in Free-Speech Values*, 1 TEX. WESLEYAN L. REV. 1, 72 n.398 (1994) ("Defamation law in this sense is ideologically neutral, and therefore is remitted to a [case-by-case] balancing test.") (quoting LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-2, at 789 (2d ed. 1988).

[154] Brief for Ctr. for Competitive Pol. et al. as Amici Curiae Supporting Petitioner at 4, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

[155] *Id.*

[156] *See* Alex Abdo, *Why Rely on the Fourth Amendment to do the Work of the First?*, 127 YALE L.J. FORUM 444, 445 (2017) (discussing the differences between the First and Fourth Amendments, particularly that the latter ignores the "cumulative" effects of privacy invasions and offers weaker protections); Bara, *supra* note 150, at 208 (arguing that First Amendment protections are broader than Fourth Amendment protections).

courts' predilection for Fourth Amendment analyses has only demonstrated the shortfalls of its application. Filling a gap in Fourth Amendment law does not do away with the First Amendment concerns raised by government surveillance of protests; in fact, the "development of a 'First Amendment criminal procedure' might begin to close the gaps in Fourth Amendment coverage by providing for the protection of First Amendment-protected behavior that is likely chilled by targeted police surveillance . . . ."[157]

When protestors' rights hang in the balance, they are not protected by an avoidance of the use of First Amendment doctrine, because the Fourth Amendment does little in its absence. A case-by-case analysis using Fourth Amendment precedent alone is insufficient to address the confluence of chilling effects when surveillance technology is used. Reliance on the Fourth Amendment would have been more appropriate in an era such as the 1970s, because surveillance posing a chilling effect was more difficult to achieve prior to the digital revolution. The courts have dealt with this issue in criminal procedure incrementally, but their decisions are continuously outpaced by the sophistication of digital advancement. As the universe of publicly available information has expanded, much more government activity can pass muster without violating the Fourth Amendment if the potential First Amendment infringements are sidelined. Whatever the Fourth Amendment currently says about tower dumps, or similar surveillance technology, we need to think about First Amendment issues first. Further, the Court's expressed concern about potential infringement on freedom of association demonstrates a conceivable willingness to embark on independent First Amendment inquiries.

III. IT ALL COMES DOWN TO THE FIRST

Part III considers the shortcomings of the Fourth Amendment and the unique First Amendment harms posed by government technologies to suggest a new framework for courts to utilize when protestor speech is chilled by state surveillance.

Under the First Amendment, impairments of the right to associate must withstand exacting scrutiny.[158] In turn, protestors' freedom of association should only be permissibly overridden "by regulations adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational

---

[157] Matthew A. Wasserman, *First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program*, 90 N.Y.U. L. REV. 1786, 1789 (2015).

[158] Clark v. Libr. of Cong., 750 F.2d 89, 94 (D.C. Cir. 1984).

freedoms."[159] This standard holds even "if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct."[160] Whether the use of tower dumps during protests is so tailored is a determination the courts must make while taking into consideration the stark differences in how government actors chill free speech in the pre- and post-digital age where social media platforms and smart devices play a large role in the dissemination of information.

A common thread in recent landmark Fourth Amendment jurisprudence is the consistent reminder that past Fourth Amendment case law cannot be mechanically applied on top of new digital age searches.[161] There is no reason the same pragmatic approach should not apply to First Amendment cases. The insight gleaned from recent Fourth Amendment cases is important in considering new First Amendment concerns as applied against older First Amendment rules. Rather than formulaically applying existing rules to unprecedented facts, courts must be open-minded to crafting new protections for new challenges. Law enforcement's use of tower dumps to surveil alleged suspects of crimes involved in protests, which inexorably results in tracking a large swath of protestors, is one example of a conventional Fourth Amendment issue that implicates the First Amendment.[162] Other surveillance tools such as geofences, stingrays, and drones could trigger First Amendment concerns and require an independent analysis as well.[163] There is no magic formula to decide the permissibility of law enforcement actions when free speech and privacy issues are at the fore. The point is, rather, that when both are implicated, conduct cannot only be assessed under the Fourth Amendment, but must also be assessed under the First Amendment.

---

159 Boy Scouts of Am. v. Dale, 530 U.S. 640, 641 (2000).

160 *Clark*, 750 F.2d at 94 (internal citation omitted).

161 *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.");); Riley v. California, 573 U.S. 373, 394 (2014) ("We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future."); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."); Kyllo v. United States, 533 U.S. 27, 36 (2001) ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

162 *See* Owsley, *supra* note 25, at 6.

163 *See* Meyer, *supra* note 24.

Though there are some differences between the surveillance in prior freedom of association cases and in tower dumps,[164] they do not preclude an application of the doctrinal tests or constitutional thresholds for permissible or impermissible encroachments on First Amendment rights. Otherwise put, courts should be able to apply the test for freedom of association encroachments to tower dumps in a protest setting. Highly sophisticated technological tools that can instantaneously unmask everyone at a First Amendment-protected event, such as a protest against police brutality, were not available when the Court recognized the "vital relationship between freedom to associate and privacy in one's associations" in 1958.[165] However, tower dumps are akin to forced disclosure of digital databases of protest participants like in *Patterson*.[166]

This Comment's proposes a judicial framework that balances various factors of the challenged state conduct to address the chilling effects of government surveillance on protestor speech.[167] These surveillance program factors include: 1) the breadth of the program; 2) the intent of the program; 3) the government's interest in the data to be collected; and 4) the level of aggregation resulting from the program. The judicial scrutiny in freedom of association cases necessarily involves balancing these factors, requiring each surveillance program to be assessed individually.

While it has been argued that balancing tests often have deleterious results for those seeking vindication for alleged constitutional violations,[168]

---

[164] *Patterson* addressed compelled disclosure of membership lists which belonged to the NAACP. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 453 (1958) ("Over petitioner's objections, the court ordered the production of a substantial part of the requested records, including the membership lists, . . . "). In the matter of tower dumps to identify protestors, law enforcement is not demanding disclosure of membership lists directly from Black Lives Matter or another analogous organization, but rather, seeks the data from phone companies. *See* Remington, *supra* note 18 ("The police can then go back to the phone company and ask for identifying information.").

[165] *Patterson*, 357 U.S. at 462.

[166] *Id.* at 451.

[167] Given the complexities of the interrelated issues at hand, such as the varying scopes and targets of the surveillance tools, brightlinebright line rules are best to be avoided, in favor of a dynamic test that considers multiple factors. How the courts would procedurally apply freedom of association doctrine to government surveillance challenges would depend on both factors related to the surveillance program itself, and at what stage of the judicial process the program is being challenged.

[168] Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1266 (1988) (arguing that the Fourth Amendment reasonableness or balancing test "has the effect of eroding the fundamental privacy and liberty rights protected by the fourth amendment.").

a multi-factor analysis is still the superior path for the judiciary to chart given the complexities of government surveillance technology and its uses. The most axiomatic advantage of this factor test is that the presence of a test at all is superior to the absence of one. Secondly, while the use of balancing was historically attacked in the mid-twentieth century for "the illiberal results it produced in free speech cases,"[169] it was indisputably an important tool in the seminal associational rights cases mentioned at length in this Comment, and has been used in First Amendment cases even more in the past decades.[170] Judicial discretion can be used in a balancing assessment to tip the scales in favor of the government—as has been done in Fourth Amendment cases—but bright line rules regarding the permissibility of proffered legitimate law enforcement investigatory tactics are more susceptible to discretionary abuse than a process that takes into consideration the nuances of a program and the impact on the target of surveillance. So long as there is transparency about the "valuation standards"[171] and courts avoid nebulous declarations that appropriate conclusions were reached without clarifying the interests considered, a balancing test is the fairest way to adapt to the technological advancements of both government surveillance and modern protest. These factors will help the court more pragmatically assess the potential chilling effects of government technology, while taking into consideration the nuances of investigatory policies and assessing which tactics cross the line into overly invasive surveillance.

A. SCOPE OF THE PROGRAM

The scope of a government surveillance program is an important factor in this Comment's suggested framework. For example, whether tower dumps are contemplated within a broader surveillance program or operate as individual, non-systemic police requests will result in a different First Amendment burden requirement. Lower courts have noted the lack of consistent guidance in determining when "a surveillance system became so intrusive as to create a reasonable or objective chill in a plaintiff and therefore present a justiciable controversy."[172] To begin, systematic efforts to identify protestors will be viewed with more skepticism than isolated tower dumps. If the Department of Homeland Security has an ambitious program designed to surveil protestors on a broader scale, a First Amendment chill will be easier

---

[169] T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943, 944 (1987).

[170] *Id.* at 967.

[171] *Id.* at 976.

[172] Alliance to End Repression v. City of Chi., 627 F. Supp. 1044, 1048 (N.D. Ill. 1985).

to prove in court. The prospect of a modern agency-wide surveillance program specifically targeting protestors would hardly be comparable to surveillance tactics primarily relying on media reports and agents attending public meetings.[173] Concern in this vein would not turn on the actions of a single sergeant but rather a police commission developing an anti-protest task force and instructing all officers to utilize tower dumps to track individuals.

If the program is part of an organized system of multidimensional surveillance, the analysis would also lean more in favor of protestors. A government agency tool combining tower dumps, drone surveillance, and social media monitoring is the exact "unrestrained power to assemble data" warned of that is "susceptible to abuse."[174] Conversely, courts will be less likely to find a chilling effect on freedom of association if law enforcement agents act alone in furtherance of an investigation.

B. INTENT OF THE PROGRAM

Second, the proposed framework assesses the intent of the surveillance program (or individual tower dump request). National security and legitimate law enforcement activities are generally considered legitimate state interests,[175] but the relationship between the professed state interest and invasive burden on protestors depends on what, if any, crime is being investigated. The burden is on the government to prove its compelling state interest, which means it must specify and justify its reason for mounting the program.[176] The program also cannot be overbroad.[177] For example, a policy to arbitrarily monitor protestors will be treated differently than one to investigate serious crimes. The invocation of national security in investigative duties has been recognized as a "greater jeopardy to constitutionally protected speech."[178] If a surveillance program using tower dumps on protestors is justified "under so vague a concept as the power to protect domestic security," courts should consider the chilling effect greater.[179] If an agency has a broad policy to use tower dumps to track Black

---

[173] Laird v. Tatum, 408 U.S. 1, 6 (1972).

[174] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (internal marks omitted).

[175] *Keith*, 407 U.S. at 311 ("Though the Government and respondents debate their seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them.").

[176] Clark v. Libr. of Cong., 750 F.2d 89, 94 (D.C. Cir. 1984).

[177] Skaggs, *supra* note 56, at 1492.

[178] *E.D. Mich.*, 407 U.S. at 313.

[179] *Id.* at 314.

Lives Matter protestors under the guise of prophylactic domestic security, courts should be more skeptical.

If the policy is triggered only when investigating serious crimes unrelated to core First Amendment activity, courts should be more deferential to law enforcement. An example of this would be the investigation of a crime that took place during a demonstration, but whose surveillance prompting was disconnected from the ideological motivations of said demonstration. Even then, what crimes are supposedly being investigated through tower dumps or other surveillance tactics should be considered. The intrusiveness of location tracking should not be outweighed by capricious government tactics, such as seeking information on protestors based on loose accusations of criminal activity. Civil disobedience is an expected part of protests against governments.[180] Reports of tense, but largely non-violent, encounters between protestors and police officers should not warrant widescale data acquisition of copious amounts of people in the vicinity. In a similar vein, while "the Fourth Amendment might permit officers to track the cellphones of protesters to gather evidence of jaywalking" or other lesser crimes, "the First Amendment might prohibit that surveillance as too invasive to be used to investigate an offense so minor."[181] The extant nuances in varying uses of surveillance technology require independent analyses for the reasons presented; the nature of the investigation, coupled with the intent behind the surveillance, come in myriad degrees.

C. GOVERNMENT INTEREST

The government interest in the surveillance program is another important factor. Even if policies to use tower dumps are only activated to aid in criminal investigations, as opposed to specifically and broadly target protestors, the invasiveness of the program's goals can vary greatly. For example, exclusive criminal investigatory interests in using tower dumps can result in divergent objectives, ranging from wanting to identify single suspects to assembling dossiers on everyone in the vicinity. The narrower the reach of the program, the more likely it is to survive constitutional scrutiny.

Relatedly, pretextual intent might weigh a court's analysis in favor of protestors. If law enforcement is investigating a homicide that happened to take place at a protest, the inquiry could be more partial to government interests than the comparatively lesser burden imposed on demonstrators.

---

[180] Harrop A. Freeman, *The Right of Protest and Civil Disobedience*, 41 IND. L.J. 228, 229 (1966).

[181] Abdo, *supra* note 156, at 455.

However, if the crime of investigation is directly related to First Amendment activity, courts should be especially conscious of the justification. For example, courts should be skeptical that investigation of minor crimes closely related to protest activity, such as obstruction of traffic, is worth the imposed burden.

D. AGGREGATION PRACTICES

Lastly, the aggregation practices that occur within a tower dump request or broader surveillance policies are important. Tower dumps that discard data determined irrelevant to the criminal investigation and do not retain relevant data beyond the needs of the investigation will more likely pass constitutional muster. This is because a more carefully circumscribed tower dump is more carefully tailored to the state's interest in an investigation, as opposed to more arbitrary and unending data collection of individuals' information.

Conversely, it will be much more difficult for the government to argue that a policy for retaining data of a broad swath of loosely grouped people serves the state's interest in effective law enforcement investigations, and that the policy is unrelated to the suppression of ideas.[182] Courts may be wary if law enforcement agents routinely seek data from one cell tower or multiple towers in a range concerningly far from the original suspected crime scene. If an alleged crime took place at Chicago's Millennium Park, for example, seeking data from cell towers far outside of that range would be overly broad. Aggregating data of thousands of Black Lives Matter protestors without linking individuals to specific investigations raises similar concerns as gang affiliation databases, criticized for defining affiliation too broadly, and that "carelessly criminalizes people of color, and exposes them to wrongful arrests, convictions, and deportations."[183]

All of these factors are used to determine whether interferences with the right to freely associate are justified by the government's legitimate, compelling interests.[184] We know that "by collective effort individuals can make their views known, when, individually, their voices would be faint or lost."[185] The power in this collective effort can only be justified through the most narrow of means, with the most superseding of interests. Given the historic import conferred on freedom of association, it is clear the courts

---

[182] Boy Scouts of Am. v. Dale, 530 U.S. 640, 640–41 (2000).

[183] Vaidya Gullapalli, *Spotlight: The Dangers of Gang Databases and Gang Policing*, APPEAL (July 3, 2019), https://theappeal.org/spotlight-the-dangers-of-gang-databases-and-gang-policing [https://perma.cc/CS2V-CARN].

[184] Shelton v. Tucker, 364 U.S. 479, 490 (1960).

[185] NAACP v. Claiborne Hardware Co., 458 U.S. 886, 907–08 (1982) (citation omitted).

should adopt a First Amendment framework when government surveillance infringes on that freedom.

CONCLUSION

Government monitoring of perceived dissidents can be traced through nearly all focal points of civil rights history. Surveillance will continue to advance with technology, leading to more intrusive tactics that quell free speech. Despite the advancement of mass data collection in the protest setting, the courts have yet to confront the First Amendment question in surveillance matters. But the salience of the issue compels them to. While the range of surveillance, excessive force, or other First Amendment infringement allegations differ, lawsuits over law enforcement-protestor clashes in Portland,[186] Seattle,[187] Chicago,[188] and other cities, will multiply. At the very least, concerns over government surveillance of protestors will continue to seep the national consciousness.[189]

Tower dumps may appear to be seemingly innocuous and un-intrusive forms of government surveillance on protestors, used in limited intervals to target individual suspects of crimes allegedly committed during protests.[190]

---

[186] Meerah Powell, *ACLU of Oregon Files Lawsuit Against Portland, PPB over Video Livestreams of Protests*, OPB (July 29, 2020, 12:00 PM), https://www.opb.org/article/2020/07/29/portland-police-bureau-oregon-aclu-lawsuit-surveillance [https://perma.cc/P2TT-MMQH].

[187] Heidi Groover, *Lawsuit Alleges City, State Failed to Protect Protestors from Drivers Who Could Hurt or Kill Them*, SEATTLE TIMES (Sept. 25, 2020, 12:36 PM), https://www.seattletimes.com/seattle-news/lawsuit-alleges-city-state-failed-to-protect-protesters-from-drivers-who-could-hurt-or-kill-them [https://perma.cc/MD56-SNWX].

[188] Matt Masterson, *Activists File Suit to Protect Protestors with Federal Agents Coming to Chicago*, WTTW (July 23, 2020, 1:25 PM), https://news.wttw.com/2020/07/23/activists-file-suit-protect-protesters-federal-agents-coming-chicago [https://perma.cc/SB7H-FC5D].

[189] *See* John D. McKinnon & Michelle Hackman, *Drone Surveillance of Protests Comes Under Fire*, WALL ST. J. (June 10, 2020, 3:47 PM), https://www.wsj.com/articles/drone-surveillance-of-protests-comes-under-fire-11591789477 [https://perma.cc/DPJ9-WN8X]; Raphael Satter, *Lawmaker Quizzes Attorney General Barr on Protest Surveillance*, REUTERS (June 11, 2020, 1:08 PM), https://www.reuters.com/article/us-minneapolis-police-protests-surveilla/lawmaker-quizzes-attorney-general-barr-on-protest-surveillance-idUSKBN23I2XM [https://perma.cc/RY3Y-446U]; Sam Biddle, *Police Surveilled George Floyd Protests with Help From Twitter-Affiliated Startup Dataminr*, INTERCEPT (July 9, 2020, 1:00 PM), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests [https://perma.cc/4284-CL3G].

[190] *See* Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014, 11:58 AM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique [https://perma.cc/7PX7-LXZV].

However, the continuously reaffirmed privacy concerns posed by government surveillance, coupled with courts' reluctance to address the First Amendment implications of such surveillance, proves it is time to conduct independent freedom of association inquiries when such matters are implicated. The breadth and precision of technology will only grow. And intrusion is a continuous variable that refines itself when new tools emerge and surveillance programs expand in scope.

Given the threat government data collection poses to the freedom of association, courts should adopt a First Amendment strict scrutiny standard when constitutional challenges to surveillance programs arise. A balancing test involving the scope, intent, government interests, and aggregation methods of the program should guide courts. While tower dumps are a timely and threatening surveillance tool that should trigger a First Amendment analysis, the framework should also apply to similar technologies if they chill free speech. Only then can we ensure that our voices will be protected.[191]

[191] NAACP v. Claiborne Hardware Co., 458 U.S. 886, 908 (1982) (internal marks and citation omitted).