Interrogating Information Infrastructure: Policing, Protest, and Structural Racism

Rebecca Slayton and Jason Ludwig

CORNELL UNIVERSITY
REPPY INSTITUTE
OCCASIONAL PAPER #33

ISSN 1075-4857

The Judith Reppy Institute for Peace and Conflict studies was established at Cornell in 1970 as the Peace Studies Program, an interdisciplinary program concerned with problems of peace and war, arms control and disarmament, and more generally, instances of collective violence. Its broad objectives are to support graduate and post-doctoral study, research, teaching, and cross-campus interactions in these fields.

Copies of most Occasional Papers may be ordered from:
Reppy Institute
130 Uris Hall
Cornell University
Ithaca, NY 14853-7601

Table of Contents

Interrogating Information Infrastructure: Policing, Protest, and Structural Racism[1]

Rebecca Slayton and Jason Ludwig

1. Introduction

Facebook, Twitter, cell phones, and digital cameras are part of *information infrastructures*—socio-technical systems for gathering, communicating, and storing information—that have become essential to organizing effective social movements. For example, racial justice activists have used these systems to document and raise awareness about violence against persons of color, to organize large-scale protests, and to stay informed.

Simultaneously, new social media and related infrastructures have become tools for law enforcement and intelligence professionals to assess threats and investigate criminal activity. For example, the Capitol Riot of January 6, 2021—which threatened democratic institutions and killed five police officers, injured 150 more, and traumatized even more, ultimately leading to the suicide of four officers—was largely planned on social media.[2] While many law enforcement and intelligence professionals monitored social media and expressed alarm about activists planning for an insurrection on January 6, these warnings were not taken sufficiently seriously by their organizations—in part because of disagreement about how to interpret and use these infrastructures for intelligence, as we discuss in the conclusion to this report.

This report uses public records to show how law enforcement organizations develop and use information infrastructures for intelligence, and analyzes the impact of those practices on the racial justice movement, law enforcement, and democratic institutions. It is particularly focused on the

[1] Acknowledgments: Hannah Contreras, Zinedine Hoque, Tom Horton, Harmony Lebovic, and Michele Soltsov contributed to this report. This report is based on research supported by National Science Foundation grant number 1553069.

[2] On injuries, see Michael Kaplan and Cassidy McDonald, "At Least 17 Police Officers Remain out of Work with Injuries from the Capitol Attack," *CBS News*, June 4, 2021, https://www.cbsnews.com/news/capitol-police-injuries-riot/. On suicides, see Kevin Mangan and Dan Breuninger, "Two More Police Officers Die by Suicide after Defending Capitol during Riot by Pro-Trump Mob, Tally Now 4," CNBC, August 2, 2021, https://www.cnbc.com/2021/08/02/3rd-police-officer-gunther-hashida-kills-himself-after-capitol-riot-by-trump-mob.html.

relationship between information infrastructures and structural racism, by which we mean institutionalized discrimination against racial and ethnic minorities in a society—something that goes beyond the implicit or explicit biases of individuals, to be embedded in the routinized practices of organizations and the policies they uphold. Structural racism in policing has received growing attention in recent years, and numerous studies have documented that Black and Brown people in the United States are more likely to be stopped, arrested, convicted, and killed by police, despite tremendous evidence that race does not make anyone more prone to criminal behavior.[3] They have also shown that the design and use of criminal records databases and related information infrastructures tend to reinforce this discrimination.[4] However, studies have yet to consider the relationship between structural racism, intelligence gathering practices, and racial justice activism.

We argue that despite the work of many well-intentioned law enforcement professionals, the development and use of information infrastructure for intelligence has reinforced structural racism. This is not because of malfeasance by any individual, but rather because organizations tend to design, maintain, and use technology in ways that continue rather than disrupt existing practices. For example, as many studies have shown, criminal records databases over-represent Black and Brown communities because they reflect a history of racially discriminatory policing; when used to allocate resources for further policing, they exacerbate such discrimination.

Our report further suggests that law enforcement has tended to use information infrastructures to direct more scrutiny towards activists who challenge racist policing practices, than towards White supremacists who ignore or even support such practices.[5] Decisions about whose social media accounts are monitored, where surveillance cameras are deployed, and what protests are disrupted, all reflect a tendency to view critics of law enforcement as threats to public safety. But while anti-racist activists do indeed threaten racist policing practices, this is not the same as threatening public safety. On the contrary, anti-racist critique of government institutions should be understood as an

[3] For example, see Radley Balko, “Opinion: Another ‘Excuse’ for Police Bias Bites the Dust,” *Washington Post*, June 4, 2019, https://www.washingtonpost.com/opinions/2019/06/04/another-excuse-police-bias-bites-dust/.

[4] See, e.g., Matthias Leese and Simon Egbert, *Criminal Futures: Predictive Policing and Everyday Police Work* (London: Routledge, 2021); Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (New York: Oxford University Press, 2020).

[5] We capitalize both Black and White because we recognize the power that both of these categories have in a society that is structured by systemic racism. For further discussion, see Eve Ewing, “I’m a Black Scholar Who Studies Race. Here’s Why I Capitalize ‘White,’” 3 July 2020, https://zora.medium.com/im-a-black-scholar-who-studies-race-here-s-why-i-capitalize-white-f94883aa2dd3.

essential part of reform in a democratic society. Since law enforcement cannot scrutinize all threats, the tendency to dedicate more surveillance towards racial justice groups than towards White supremacist groups tends to neglect real threats. Indeed, as we show, these practices have produced flawed intelligence that endangers not only racial justice activists, but also police and democratic institutions.

Importantly, racial bias in the use and development of information infrastructure is not inevitable or technologically determined. In conclusion, we reflect upon how information infrastructures could be designed and used to advance racial justice. We make recommendations for three overlapping kinds of infrastructure.

- ***Blue data infrastructure***: Our findings support recommendations for developing "blue data," meaning data about police behavior that would enable learning and accountability.[6] But we also emphasize that technology also cannot solve underlying cultural problems. Some police departments have embraced blue data, recognizing that they can use it to redesign procedures and thereby reduce the systemic risks of violent encounters, officer errors, and other negative interactions with citizens. But police unions and many departments have resisted the increased oversight that these systems enable. Because information infrastructure ultimately reflects the goals of its creators and maintainers, the effective development and use of these systems requires more than technology; it also requires a cultural shift in which law enforcement begins to prioritize community trust over and above unbridled autonomy.
- ***Social media and data analytics infrastructure***: Activists have used social media to great effect, but reliance on these infrastructures has also made activists vulnerable to unwarranted surveillance. The public nature of activism has made it "low hanging fruit" for data analytics companies, which portray racial justice activists as threats to public safety as they market their services to law enforcement. Overcoming this bias will require transforming the market through regulation or other measures that raise awareness of the problems intrinsic to the industry.
- ***Camera infrastructure***: While citizens and activists now have ready access to mobile phone cameras that can document racial violence, most public surveillance camera infrastructure

[6] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017).

> remains under the control of law enforcement. Until citizens have more substantial control over the development and use of camera infrastructure—including decisions about where cameras are placed, and how camera data is monitored and used—cameras will do little to establish trust and accountability between police and citizens.

We have written this report for activists, intelligence professionals, and members of the public, all of whom face risks from structural racism in contemporary information infrastructures. Our goals are to improve understanding of problems in these infrastructures, and to stimulate discussion about how to redirect the development and use of information infrastructures towards social justice. We also hope that this report will help racial justice activists better understand and thereby minimize their risks of surveillance and harassment. However, we do not attempt to provide detailed advice because groups such as the Electronic Frontier Foundation have already provided excellent guidelines for this purposes (see, for example, https://ssd.eff.org/en/playlist/activist-or-protester).

The remainder of the report is organized in six major sections. First, we use a recent case in Memphis, Tennessee, to demonstrate how law enforcement can use a wide range of tools—including social media analytics, deceptive social media accounts, undercover phone numbers, surveillance cameras, law enforcement databases, and intelligence briefings—to surveil activists.

Second, we discuss how changes in technology and industry over the past fifty years have tended to reinforce and amplify structural racism, despite the establishment of laws designed to protect civil liberties. We highlight four dynamics: the ability to track increasingly minor interactions with individuals; the growing scale and efficiency of information-sharing among law enforcement; the growth of “data-driven” policing; and the rise of the “surveillance capitalism” industry, which harvests and sells data about the behavior of internet users.

The third, fourth, and fifth sections of the report illustrate how these dynamics work together to reinforce structural racism, respectively focusing on three distinctive kinds of information infrastructures: law enforcement databases, social media, and surveillance camera networks.

A sixth and final section of the report reviews the causes and consequences of structural racism in law enforcement. It contrasts the suspicion shown towards racial justice activists with that shown towards the predominantly male and White activists who planned an assault on the U.S. Capitol for

January 6, 2021. It thus demonstrates that structural racism in intelligence poses a threat not only to racial justice, but also to law enforcement and democratic institutions.

2. Constructing Threats in Memphis

Surveillance of racial justice activists in Memphis dates at least to the 1960s. Federal agencies played a role not only in Memphis, but nationwide, as the U.S. Federal Bureau of Investigation (FBI) monitored and infiltrated the civil rights movement through its now-infamous counter intelligence program (COINTELPRO).[7] The Memphis police department shared the FBI's suspicion of the civil rights movement, and surveilled numerous activists, including Martin Luther King. Jr. shortly before he was assassinated in 1968.[8]

In the 1970s, public backlash against COINTELPRO and similar surveillance efforts led to significant restrictions on the ways that law enforcement uses surveillance. And in Memphis, the American Civil Liberties Union (ACLU) of Tennessee filed a 1976 lawsuit against the city for keeping records that "contained unverified information and gossip which related exclusively to the exercise of lawful and peaceful activities," and "served no lawful or valid law enforcement purpose."[9] The ACLU won the lawsuit, resulting in a 1978 consent decree that prohibited the City of Memphis from conducting "political intelligence"—meaning "the gathering, indexing, filing, maintenance, storage or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations or other exercise of First Amendment rights."[10]

[7] For more on COINTELPro, see Hannah Foster, "COINTELPRO (1956-1976)," at https://www.blackpast.org/african-american-history/cointelpro-1956-1976/, accessed December 10 2021. The FBI today acknowledges the problematic program and provides some files related to its surveillance online at https://vault.fbi.gov/cointel-pro.

[8] Jeffrey Robinson, "Memphis Police Surveillance of Activists Is a Betrayal and a Reminder," American Civil Liberties Union, at https://www.aclu.org/blog/criminal-law-reform/reforming-police/memphis-police-surveillance-activists-betrayal-and, accessed December 10 2021.

[9] Quoted in Wendi C. Thomas, "The Police Have Been Spying on Black Reporters and Activists for Years. I Know Because I'm One of Them," *ProPublica*, June 9, 2020, https://www.propublica.org/article/the-police-have-been-spying-on-black-reporters-and-activists-for-years-i-know-because-im-one-of-them?token=RHsMco8cWQdk817AiL2EafHM1aKlwiQD.

[10] Quoted in the court order for Blanchard et al. v. City of Memphis, No. 2:17-cv-02120-JPM-egb (W.D. Tenn. Oct. 26, 2018), ECF No. 151, p. 16, available at: https://www.aclu-tn.org/wp-content/uploads/2018/10/151-Order-Memphis.pdf.

However, forty years later, following another lawsuit led by the ACLU, a judge once again ruled that the Memphis Police Department (MPD) had engaged in surveillance of the political activities of activists that were protected by their First Amendment rights—in violation of the 1978 decree. The 2018 ruling also found that the MPD had also shared this illegally gathered and privileged information with other law enforcement institutions and private actors, another violation of the 1978 decree.[11]

In what follows, we use evidence from exhibits and depositions associated with the 2018 ruling to demonstrate how law enforcement organizations can transform digital traces of lawful activism—including social media, cell phone data, and surveillance camera images—into intelligence briefings which portray racial justice activists as a threat to public safety. It is worth noting that while the Memphis Police Department is prohibited from such surveillance by the 1978 decree, other police departments are under no such regulations.

2.1 The rise of data-driven policing

The Memphis police department began to embrace "data-driven" policing as early as 1997, when Memphis was one of five cities granted funding under the Department of Justice's Strategic Approaches to Community Safety Initiative.[12] Richard Janikowski, a criminology professor at the University of Memphis, recalls that Memphis had ranked at the top of the nation in forcible rape for twenty years; the rate peaked in at 938 rapes in 1997. Janikowski and other researchers gathered data and concluded that many forcible rapes began after women went to make calls in dark phone booths outside of convenience stores. So the booths were moved inside the stores, where women were not such easy targets, and the rate of forcible rape declined dramatically, to 574 in 2000. In 2001, Janikowski partnered with the Memphis Police Department on a data-driven approach to reducing gun crime, and this was also regarded as successful.[13]

[11] Ibid. The ACLU provides access to many of the case documents at https://www.aclu-tn.org/blanchard-et-al-v-city-of-memphis/.

[12] Jan Roehl et al., "Strategic Approaches to Community Safety Initiative (SACSI) in 10 U.S. Cities: The Building Blocks for Project Safe Neighborhoods" (U.S. Department of Justice, February 2006), available at: https://www.ojp.gov/pdffiles1/nij/grants/212866.pdf.

[13] Erinn Figg, "The Legacy of Blue CRUSH," *High Ground News*, March 19, 2014, available at: https://www.highgroundnews.com/features/BlueCrush031214.aspx.

In 2005 Janikowski helped the Department expand the approach through the Blue CRUSH (Crime Reduction Using Statistical History) program. Police reports on crime data were mapped to identify particular times and places where crime was most likely to occur, and additional officers were sent to monitor those "hot spots." During the first two hours of a pilot program, officers arrested 70 people, the number typically arrested over a weekend. That number grew to 1200 within three days. The Director of the Memphis Police Department, Larry Godwin, was sold. Blue CRUSH was quickly expanded city wide.[14]

The Blue CRUSH program soon entailed the massive expansion of surveillance. In 2008, the Memphis Police Department launched its Real Time Crime Center (RTCC), a 24/7 operation that was modeled after a similar center in New York City. The RTCC boasted "a massive wall of 42 large-screen monitors" which could stream video from surveillance cameras and map the locations of crimes the instant they were reported.[15] But the wall of monitors was only the tip of the iceberg; the RTCC developed or gained access to a vast network of information infrastructures for surveillance, as discussed further below.

2.2 Turning surveillance on activists

Less than a decade after RTCC's establishment, as protests against police brutality against Black people gained momentum nationally and locally, the RTCC began to focus its surveillance on local activists. In August 2014, the police shooting of Michael Brown, an unarmed Black teenager in Ferguson, Missouri, sparked public outrage and helped launch the nascent Black Lives Matter movement nationally, including a chapter in Memphis.[16] Less than one year later, in July 2015, Memphis Police officer Connor Schilling shot and killed Darrius Stewart, an unarmed Black teenager.[17] Memphis activists rallied to protest the shootings and demand that Schilling be held

[14] Figg, "The Legacy of Blue CRUSH," ibid.

[15] Bianca Phillips, "Memphis Police Department Unveils Real Time Crime Center," *Memphis Flyer*, April 16, 2008, https://www.memphisflyer.com/undefined.

[16] On the origins of the Black Lives Matter movement, see https://library.law.howard.edu/civilrightshistory/BLM. For the history of the Memphis chapter of Black Lives Matter, see http://blacklivesmattermemphis.com/.

[17] Stewart was a passenger in a car that Schilling pulled over; when Schilling discovered warrants on Stewart and attempted to arrest him, a struggle ensued. Schilling claims that Stewart assaulted him; the family disagrees. Micaela A. Watts and Daniel Connolly, "Mother of Darrius Stewart, Teen Killed in 2015 Traffic Stop, Sues Former MPD Officer," *Memphis Commercial Appeal*, February 10, 2020,

accountable.[18] And the next summer, they joined nationwide protests that followed police killings of two Black men in less than 24 hours: Alton Sterling in Louisiana on July 5, and Philando Castille in Minnesota on July 6.

Four days later, on July 10, 2016, Black Lives Matter protesters successfully shut down the Interstate 40 Bridge through Memphis for close to four hours. Police showed up in riot gear, though the protest was entirely peaceful and largely ended through a calm negotiation with Memphis Police Department Interim Director Michael Rallings.[19] Keedran Franklin, a Black activist who had first become involved in his community by volunteering with violence interruption programs, felt that he "actually connected" to Rallings on the bridge.[20] Franklin and other activists, such as pastor Earle Fischer, linked arms with Rallings to help lead about half of the demonstrators off the bridge for further discussions.[21]

Memphis activists regarded the bridge shutdown as a major success. Franklin and other activists formed a new group, the Coalition of Concerned Citizens, to continue pressing for change.[22] Meanwhile Rallings—who is Black—won the provisional support of Memphis activists. One day after the shutdown, activists issued four demands, the first of which was to make Rallings permanent director of the police department.[23] In August, the Memphis City Council confirmed Rallings as full director.[24]

https://www.commercialappeal.com/story/news/2020/02/10/darrius-stewart-mother-sues-former-memphis-officer-connor-schilling/4712694002/.

[18] For example, see: Bill Dries, "Crowd Rallies to Protest Darrius Stewart Shooting," *Memphis Daily News*, November 11, 2015, https://www.memphisdailynews.com/news/2015/nov/11/crowd-rallies-to-protest-darrius-stewart-shooting/.

[19] Center for Community Change, "'Take It to the Bridge': Community Change Action," July 7, 2017, available at: https://communitychangeaction.org/changewire/take-it-to-the-bridge/.

[20] On Franklin's involvement with the "guns down" program, see: Alice Speri, "The Fire This Time: In the Face of Rising White Supremacist Violence, Police Continue to Investigate Victims and Activists," *The Intercept*, January 20, 2020, https://theintercept.com/2020/01/20/political-surveillance-police-activists-tennessee/. Franklin now believes the program was surveilling youth under the guise of community outreach.

[21] Jody Callahan, "Marchers Shut down I-40 Bridge at Memphis during Black Lives Matter Rally," *Memphis Commercial Appeal*, July 10, 2016, http://www.commercialappeal.com/news/tennessee-black-caucus-calls-for-calm-amid-racial-unrest--3714d93e-1078-6a7d-e053-0100007f134e-386214081.html.

[22] Center for Community Change, "'Take It to the Bridge'" (footnote 19).

[23] "'Black Lives Matter' Issues 4 Demands of City Leadership," *Action News 5 Memphis*, July 11, 2016, https://www.actionnews5.com/story/32417605/black-lives-matter-to-issue-4-demands-of-city-leadership.

[24] "Memphis City Council Confirms Mike Rallings As Permanent Director Of MPD," ABC 24 Memphis, August 6, 2016, https://www.localmemphis.com/article/news/local/memphis-city-council-confirms-mike-rallings-as-permanent-director-of-mpd/522-77acfc35-e9dc-453b-8269-1404a3564c1b.

Rallings and the many other Black officers on the Memphis police force likely shared a genuine affinity with the Black Lives Matter movement. For that matter, people like Timothy Reynolds, a White detective in the Memphis Police Department's Office of Homeland Security, acknowledged in private briefings to command staff that local activists were part of "legitimate public groups that want to make improvements."[25] But Reynolds was also among those concerned about what he called "radicals" who took "peaceful demonstrations as opportunities to use violence and destruction to promote or advance their own agendas."[26] Eddie Bass, a Black officer whom Rallings had recently promoted to the position of Acting Lieutenant Colonel over special operations, also felt the need to monitor protests. After the bridge shutdown, Bass asked Reynolds to help command staff "get on a page where we can see…where all of the resources in the department are being allocated, because we're having a problem trying to keep up with all of these spontaneous events and to respond adequately and to provide public safety."[27] Bass asked Reynolds to "surf the social media stuff and try to anticipate where some of this stuff would happen."[28]

Memphis police were concerned about more than just disruptive civil disobedience. According to Stephen Chandler, who in 2016 became acting Lieutenant over Homeland Security (a two-person group within the RTCC), the police department had gotten "death threats from unidentified sources" in retaliation for the killing of Darrius Stewart.[29] And police were concerned that violence against police officers in other parts of the nation might spread to Memphis. Just three days before the bridge shutdown, on July 7, 2016, Micah Xavier Johnson killed five White police officers who were monitoring a protest against police brutality in Dallas. Johnson was not affiliated with the protest organizers, who condemned the shooting, but the protest gave him an opportunity for ambush. Ten days later, Gavin Eugene Long killed three Baton Rouge police officers who responded to concerns

[25] Blanchard et al. v. City of Memphis, Exhibit Q, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf.

[26] Blanchard et al. v. City of Memphis, Exhibit Q, ibid.

[27] Blanchard et al. v. City of Memphis, Exhibit Q, ibid.; Blanchard et al. v. City of Memphis, Timothy Reynolds deposition (April 24, 2018), p. 25, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf.

[28] Reynolds deposition, ibid., p. 25

[29] Blanchard et al. v. City of Memphis, Stephen Chandler deposition (April 25, 2018), p. 35, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf. By mid-2016, the Office of Homeland Security consisted of two officers reporting to Chandler, who in turn reported to Eddie Bass in the Special Operations group. Chandler recalls the office moving into the RTCC sometime in 2016 because it was previously "homeless," but Bass recalls that it fell under his responsibility starting in January 2015 (when Bass started his job). Blanchard et al. v. City of Memphis, Eddie Bass deposition (April 26, 2018) available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf.

that he was carrying a rifle and behaving suspiciously. Both Long and Johnson were Black men who appeared to be partly motivated by anger at police brutality against Black people. They had both been affiliated with Black separatist groups. Johnson was a Facebook follower of the African American Defense League (AADL), whose leader had urged people to kill White cops, and responded to Johnson's shooting by urging more such killings.[30]

Police anxiety about such events and rhetoric is understandable. But intelligence analysts diverted their attention from such threats when they erroneously conflated the Black Lives Matter movement with racist hate groups.[31] Chandler described Johnson as a "radicalized member who claimed association with one group or another" and noted that "we have the same organizations here," meaning "the organizations that arose out of Ferguson," such as Black Lives Matter.[32] But while Johnson had Facebook "liked" organizations associated with the Black Lives Matter movement (which actually predates Ferguson), leaders in that movement quickly condemned Johnson's actions and emphasized a commitment to non-violence.[33] By contrast, three different groups that Johnson liked—the Nation of Islam, the Black Riders Liberation Party, and the New Black Panther Party—long predate the Ferguson protests, and unlike Black Lives Matter, are recognized as racist hate groups.[34] Furthermore, even these groups did not direct Johnson to shoot the police, nor did they claim Johnson's actions after the fact.[35] Similarly, although Long claimed prior affiliation with the Nation of Islam and other Black separatist movements, he insisted that he was acting alone in

[30] The AADL was led by Mauricelm-Lei Millere, but experts understand him to be running a "one man show," and even Millere did not claim that Johnson was acting on his behalf. Other groups, including the New Black Panther Party, explicitly distanced themselves from the AADL. See: Katie Zavadski and Ben Collins, "This Hate Group Called for Killing White Cops. Then Dallas Sniper Micah Xavier Johnson Started Shooting," *The Daily Beast*, July 8, 2016, https://www.thedailybeast.com/articles/2016/07/08/this-hate-group-called-for-killing-white-cops-then-dallas-sniper-micah-xavier-johnson-started-shooting.

[31] BLM was sued for inciting violence in Baton Rouge, but the lawsuit was dismissed. It has more recently resurfaced in the Supreme Court. Michael Kunzelman, "Judge Intends to Dismiss 2nd Suit against Black Lives Matter," *Associated Press*, October 5, 2017, https://apnews.com/article/963f109cfa62475fa25079c356414bfd.

[32] Chandler deposition (footnote 29), p. 23.

[33] Ari Mason, "Black Lives Matter Activists, Civil Rights Leaders Condemn Dallas Ambush," *NBC 4 New York*, July 8, 2016, https://www.nbcnewyork.com/news/local/dallas-police-shooting-sniper-black-lives-matter-naacp/2032867/.

[34] Heidi Beirich and Ryan Lenz, "Dallas Sniper Connected to Black Separatist Hate Groups on Facebook," *Southern Poverty Law Center,* https://www.splcenter.org/hatewatch/2016/07/08/dallas-sniper-connected-black-separatist-hate-groups-facebook.

[35] A leader in the New Black Panther Party noted that Johnson had been asked to leave the Houston chapter of the Party years earlier because of concerns about his mental health, and because he was not respecting their chain of command. Craig Hlavaty, "Quanell X: Dallas Police Shooter Was Excused from Houston Group Years Ago," *Houston Chronicle*, July 11, 2016, https://www.chron.com/news/houston-texas/houston/article/Quanell-X-says-that-Dallas-police-shooter-was-8351761.php.

the killing of police.[36] As this suggests, police confused the individual actions of rare individuals like Johnson and Long with organized violence.

This confusion may partly explain why Chandler and others in the Memphis police department, felt the need to "be aware" of activities by Black Lives Matter activists.[37] The police had begun surveilling local activists long before the events of July 2016, but ramped up surveillance of protesters after the shootings and the bridge shutdown. As the following sections discuss, police drew on a wide range of information infrastructures—including social media, surveillance cameras, and law enforcement information-sharing systems—to construct potential threat profiles of activists and local events.

2.3 Monitoring Activists by Social Media and Phones

One day after the Dallas shootings, an officer in the Real Time Crime Center sent a message to his colleagues asking them to continue monitoring social media for "any details related to protest and in particular MPD."[38] He noted that they had been granted "temporary rights" to NC4 Signal, a software package that allowed users to monitor social media for particular keywords, and identify their location.[39] The RTCC used social media collators like NC4 Signal and Geofeedia to automatically monitor Facebook, Twitter, Instagram, and other social media sites for public "chatter" by activists. Geofeedia was particularly useful, as it allowed analysts to draw a boundary around a particular area on a map, and then examine all social media posts being made by users in that area in real time, filtering for keywords like "riot" or "gun."[40]

In practice, however, the Real Time Crime Center did not just search for keywords suggesting illicit activity. It monitored public information about the Black Lives Matter movement and individuals

[36] He stated: "Don't affiliate me with nothing. ... I'm affiliated with the spirit of justice. Nothing else. Nothing more, nothing less." John Simmerman, "'Intoxicated by His Own Importance': Look inside Mind, Motive of Baton Rouge Officer Shooter Gavin Long," *The Advocate*, July 30, 2016, https://www.theadvocate.com/baton_rouge/news/baton_rouge_officer_shooting/article_24f8502e-5680-11e6-8608-83a6d9d895cd.html.
[37] Chandler deposition (footnote 29), p. 14.
[38] Blanchard et al. v. City of Memphis, Exhibit S, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf
[39] Blanchard et al. v. City of Memphis, Exhibit S, ibid.
[40] Blanchard et al. v. City of Memphis, Exhibit S, ibid. Blanchard et al. v. City of Memphis, Bradley Wilburn deposition (April 26, 2018), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf.

associated with it—even when they were unrelated to public protest. For example, in mid-July Frank Gibson (Facebook name Frank Gottie), posted a Facebook invitation to join him at a church to "watch a Brother get saved," and another invitation to "celebrate history" at a park on Beale Street, noting: "we gone call it Beale & Chill!!!!"[41] Bass forwarded the Facebook post to Memphis Police Department Command Staff, Real Time Crime Center, Shelby County Sheriff's office, and several others, with the subject line "Intel for BLM [Black Lives Matter]," even though the event was not ostensibly related to activism. Bass noted that there was "no adverse information that would suggest the potential for civil disorder," and reiterated that the "social media Intel, a potential gathering involving Mr. Gipson [sic] (Frank Gotti)…DID NOT indicate or suggest the potential social discord."[42] Nonetheless, a station commander stated that they would be "monitoring the situation."[43]

Similarly, on July 16, 2016, a Memphis police officer e-mailed several other officers an announcement of a Black Lives Matter block party that someone else posted on Gibson's Facebook page, noting that she was passing it on "Due to the 'black lives matter' on the flier."[44] Several days later, another officer e-mailed other officers about a social media announcement of a Black Lives Matter vegan soul food cookout; the subject line stated "looks innocent enough, but here it is in case you are asked about it."[45]

Police also used specialized software for analyzing social networks, thereby expanding their surveillance to people associated with activists. They learned about these tools at conferences that discussed predictive policing and social media, as well as from company representatives, who typically use these conferences to market their products. In September 2016, after attending a conference and learning more about how to use i2 Analyst's Notebook (i2AN), a visual analysis software developed by IBM for investigation of criminal networks, Reynolds worked "with the rep

[41] Blanchard et al. v. City of Memphis, Exhibit II, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf.
[42] Blanchard et al. v. City of Memphis, Exhibit JJ, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf. Emphasis in original.
[43] Blanchard et al. v. City of Memphis, Exhibit JJ, ibid.
[44] Blanchard et al. v. City of Memphis, Exhibit V, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf.
[45] Blanchard et al. v. City of Memphis, Exhibit W, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf.

and company representative" to map relationships between Gibson and other individuals and events associated with Black Lives Matter.[46]

Police also used deceptive social media accounts to surveil activists and their associates, beginning at least a year before the Dallas shootings. Reynolds had created a fake Facebook profile named "Bob Smith" in 2009, to help him investigate gang activity.[47] And in July 2015, the same month that officer Schilling killed Darrius Stewart, "Bob Smith" began connecting with activists in the Memphis area on Facebook.[48] Bob Smith's profile picture shows a Guy Fawkes mask, which symbolizes anti-government feelings, but is also suspiciously anonymous. Nonetheless, in the years following Ferguson, many activists were inundated with friend requests while trying to grow the movement, so some took the risk of accepting requests from people they had not met, including Bob Smith.

Memphis activist Paul Garner was one of "Bob's" first Facebook friends. On July 9 2016, Garner posted a recommendation for *Rules for Radicals,* a 1971 book by the late activist Saul Alinsky. Posing as "Bob Smith," Reynolds was able to see this private post, which he forwarded along with a list of 58 people who had "liked" the recommendation to another officer in the RTCC. [49] As this suggests, social media accounts gave the police a way to expand potential targets for surveillance—and activities as minimal as "liking" another post could become a source of suspicion.

Police also set up undercover phone numbers to infiltrate activist circles. For example, in early August 2016, Keedran Franklin posted a Facebook announcement about demonstrations during

[46] Blanchard et al. v. City of Memphis, Exhibit PP, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf. IBM markets i2AN as a tool providing crime analysts with "innovative features such as connected network visualizations, social network analysis, and geospatial or temporal views," intended to help "better identify and disrupt criminal, cyber and fraudulent threats," see: https://www.ibm.com/products/i2-analysts-notebook).

[47] Court Order, Blanchard et al. v. City of Memphis (footnote 10), p. 24. Reynolds was "unmasked" in court hearings following the deposition: "MPD Officer Unmasked as 'Bob Smith' in Federal Hearing," *Memphis Daily News*, August 21, 2018, https://www.memphisdailynews.com/news/2018/aug/21/mpd-officer-unmasked-as-bob-smith-in-federal-hearing/.

[48] Blanchard et al. v. City of Memphis, ACLU of Tennessee, Memo in Support of Motion for Summary Judgement (July 24, 2018), p 12, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/107-01-Memo-in-Support_Redacted.pdf. Exhibit Z shows that "Bob Smith" and Paul Garner were friends starting in July 2015, see: Blanchard et al. v. City of Memphis, Exhibit Z, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/3-Exhibits-Y-HH_Redacted.pdf.

[49] Blanchard et al. v. City of Memphis, ACLU of Tennessee Motion for Summary Judgement (July 24, 2018), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/107-Mtn-for-Summary-Judgment_Redacted.pdf; Blanchard et al. v. City of Memphis, Exhibits Y and Z, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/3-Exhibits-Y-HH_Redacted.pdf.

Elvis Week, and invited people to send him their phone number in order to learn more details. Reynolds and his colleague in the Office of Homeland Security obtained an unidentified caller number, then used it to gather information about the upcoming demonstrations from Franklin and another organizer, Spencer Katz. Texts and phone calls to the number were recorded.[50]

2.4 Surveillance on the ground and in the air

Social media was only a starting point for surveillance. Whenever a planned protest was identified, the Office of Homeland Security checked to see if it had an approved permit, sometimes even when a permit was not required due to the event being held on private property.[51] And police "always had somebody there," either uniformed or in plain clothes, to take photos and monitor activities.[52]

The in-person presence was supplemented by an extensive network of surveillance cameras that the RTCC could access "on demand." Police use cameras on mobile trailers to monitor all large public events in Memphis, and racial justice protests were no exception. The RTCC van with its mounted cameras were also sent to protests.[53] The RTCC also monitored protests from airplanes; on at least one occasion, air support was sent to monitor a protest that was only rumored and never materialized.[54] Finally, the RTCC could access footage from stationary cameras mounted around the city as discussed further in this report's section on surveillance cameras.

By 2020, the RTCC could access almost 2000 camera feeds, but it did not have the personnel or technology to monitor them all simultaneously; instead footage was stored in the camera for about 30 days.[55] In the 1970s, storing photographs would have been a deliberate "investigative" activity; the 1978 consent decree prohibited the city of Memphis from conducting investigative activities

[50] Blanchard et al. v. City of Memphis, Exhibit LL (August 4, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf.

[51] Blanchard et al. v. City of Memphis, Exhibit H (July 16, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf; Blanchard et al. v. City of Memphis, ACLU of Tennessee, Memo in Support of Motion for Summary Judgement (July 24, 2018), p. 7, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/107-01-Memo-in-Support_Redacted.pdf.

[52] Chandler deposition (footnote 29), p. 48-49.

[53] Blanchard et al. v. City of Memphis, Joseph Patty deposition (April 26, 2018), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf.

[54] Blanchard et al. v. City of Memphis, Exhibit EE (July 13, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/3-Exhibits-Y-HH_Redacted.pdf.

[55] See "Frequently asked questions about MPD's Blue Crush Cameras," available at: https://www.memphistn.gov/download/91/crime-prevention-grant/4205/faqs-about-mpds-blue-crush-cameras.pdf

"for the purpose of political intelligence," and thus would have outlawed storing photos on activists.[56] But with contemporary automation, only a specific request for footage would be an obvious investigative activity. These and other technological changes drove the Court for the Western District of Tennessee to update the consent decree in 2020.[57]

While technological changes created some ambiguities about the interpretation of the decree, the Memphis police unambiguously violated the consent decree by sending officers in plain clothes to surreptitiously monitor protests. These officers mostly took "photographs of what was going on to give people an idea of the size of the crowd, what the crowd was doing."[58] In some cases, officers even monitored and photographed events on private property. For example, on July 15, 2016, Mary Stewart, the mother of Darrius, posted a Facebook announcement about a prayer vigil taking place for her son at New Direction Church the same evening. Just three hours later, the Memphis Police Department took note of the post and stationed an officer across the street. The officer surreptitiously monitored the event and sent observations by e-mail to command staff, the Office of Homeland Security, and many others. He began by noting that everyone was on the church property, and that "they do not know that I'm watching them."[59] Although he repeatedly noted that everything was peaceful, and there were "no problems," he took at least one photo and circulated it by e-mail. He also identified "Known individuals in the crowd: Minister Hill…the lady from BLM, also the guy that stormed out of the church…"[60] He finally cleared the scene after the participants planted a tree in memory of Darrius Stewart, and having confirmed that they had permission to plant the tree.

2.5 Law enforcement databases and information sharing

Shortly after the bridge shutdown, the Memphis police Real Time Crime Center began to put together weekly presentations to the command staff that described demonstrations, analyzed tactics,

[56] Blanchard et al. v. City of Memphis, Opinion and Order (October 26, 2018), p. 18, available at: https://www.aclu-tn.org/wp-content/uploads/2018/10/151-Order-Memphis.pdf.
[57] For discussion of this update, with links to the order, see "ACLU-TN Comment on Modification of Court Order Limiting Memphis Police Surveillance," American Civil Liberties Union, https://www.aclu.org/press-releases/aclu-tn-comment-modification-court-order-limiting-memphis-police-surveillance.
[58] Chandler deposition (footnote 29), p. 48.
[59] Blanchard et al. v. City of Memphis, Exhibit KK (July 15, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf.
[60] Blanchard et al. v. City of Memphis, Exhibit KK, ibid.

and highlighted “unlawfuls”—meaning people regarded as having led unlawful protests—as well as their contacts on social media.[61] Additionally, Office of Homeland Security responded to Bass’s request to help the command staff better anticipate events by publishing “Joint Intelligence Briefings” between one and three times a day.[62]

The briefings initially focused on major demonstrations against police brutality, but soon expanded to include less visible demonstrations and events.[63] As concerns about violence grew, the briefings also expanded to include “attacks on officers from across the country.”[64] This meant that violence towards police officers across the United States—most if not all of which had no relation to racial justice protest—came to be a primary context for sharing information about activists in Memphis. For example, an August 5, 2016 Joint Intelligence Briefing begins by describing the detonation of a pipe bomb on the hood of a police cruiser in Thurmont, Maryland, while it was parked in front of the officer’s home. It continues with the heading “social media posts affecting Memphis, TN” and shows photos of Keedran Franklin, Frank Gibson, and Aaron Lewis, noting that they were organizing demonstrations at Graceland during Elvis week. It then lists seven “upcoming events with high LE [law enforcement] presence or large public attendance,” four of which were related to the Black Lives Matter movement.[65] Similarly, a September 2016 Joint Intelligence Briefing lists

[61] Reynolds deposition (footnote 27), p. 104, 97-113.

[62] On frequency of JIBs, see Blanchard et al. v. City of Memphis, ACLU of Tennessee, Memo in Support of Motion for Summary Judgement (July 24, 2018), p. 5-6, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/107-01-Memo-in-Support_Redacted.pdf.

[63] Exhibit H, July 15, 2016 notes that the JIBs had been focused on only “widely published demonstrations,” and that it would henceforth include “lesser mentioned demonstrations.” Interestingly, the sentences announcing this “change” were repeated in subsequent JIBs, suggesting a lack of careful review of the content of JIBs. All events in the July 15, 2016 JIB were about BLM, but subsequent JIBs included events organized by groups unrelated to racial justice. Blanchard et al. v. City of Memphis, Exhibit H (July 16, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf.

[64] In particular, a July 20, 2016 Joint Intelligence Briefing listed several largely unrelated instances of threats or violence towards police officers, describing it as “a national trend” towards individuals or groups “targeting uniformed police officers.” These instances consisted of the Dallas and Baton Rouge shootings of police officers, which arguably were motivated by similar grievances but were not coordinated; four different instances (in Brooklyn, Milwaukee, Kansas City, and Memphis) of guns or bottle rockets fired at police as they responded to calls or conducted patrols, but none clearly motivated by racial grievances; and finally, an instance of discovering firearms stolen from a private citizen around Memphis. The briefing then listed events of interest: specifically an upcoming rally against police brutality (entitled “Stop the Violence Peace Rally”). The briefing promised to cover such threats in the future. Blanchard et al. v. City of Memphis, Exhibit J (July 20, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf. Interestingly, the analyst dated Johnson’s attacks to July 9 (the date of the article cited to describe the attacks) though in fact the killing was on July 7. This is just one example suggesting a lack of careful review of JIBs.

[65] Four of seven appear to be related to BLM, but two of these four are speculative: the second anniversary of Michael Brown’s death in Ferguson, and “some social media chatter” that a protest might occur during Elvis Presley Week.

two "Memphis incidents of interest." These include a small and peaceful protest in response to the announcement that no charges would be filed against Officer Schilling for killing Darrius Stewart, and a totally unrelated case of gunfire at a prowler call.[66]

Information about activists continued to be re-contextualized as it was shared with other law enforcement agencies. Joint Intelligence Briefings were initially sent only to Memphis police department command staff, but dissemination "grew exponentially" over time to include the Shelby County Sheriff's Office and a wide range of other local, state, and federal organizations, as well as some private businesses.[67] This only encouraged further surveillance and misunderstandings of racial justice activists.

The Memphis Police Department also used its special access to government databases to further investigate and amplify surveillance of activists. For example, the Memphis Police Department used the Tennessee Information Enforcement System (TIES), maintained by the Tennessee Bureau of Investigation, to pull driver's license photos and other information about activists.[68] If the activists resided outside of Tennessee, the MPD searched the Regional Organized Crime Information Center (ROCIC), one of six Regional Information Sharing Systems (RISS) centers for similar information.[69] The Memphis Office of Homeland Security used information from such systems to identify activists in weekly presentations and Joint Intelligence Briefings, thereby making it easier for law enforcement to monitor them. For example, on August 5, 2016, a Joint Intelligence Briefing highlighted three Memphis-based activists, including Gibson and Franklin,

[66] Blanchard et al. v. City of Memphis, Exhibit N (September 29, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf. The joint intelligence briefing included photos of the demonstration and identified the two "most notable" demonstrators by name: Frank Gibson (Facebook name Frank Gottie) and Ian Jeffries. The demonstration took place in front of Cecil Humphrey School of Law.

[67] Chandler deposition (footnote 29), p. 11, 15. Exhibit L, for example, shows an example of an intelligence briefing sent to at least 50 people, including members of local law enforcement agencies such as the Shelby County Sheriff's Department, members of the military, people in the Department of Justice, as well as representatives of private businesses such as FedEx, St. Jude, and AutoZone. Blanchard et al. v. City of Memphis, Exhibit LL (August 4, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/4-Exhibits-II-SS_Redacted.pdf.

[68] Blanchard et al. v. City of Memphis, Albert Bonner deposition (April 24, 2018), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf. p 34, discussing Exhibit C, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf.

[69] Bonner deposition, discussing Exhibit C, ibid. For more on the ROCIC, see https://rocic.com/.

who were planning demonstrations at Graceland during Elvis week, and included driver's license photos.[70]

2.6 From Surveillance to Confrontation

Having monitored plans for demonstrations at Graceland, the police met activists at Graceland's annual candlelight vigil on August 15, 2016 with a heavily-militarized presence, including vans and a special operations vehicle carrying armed officers. The police screened all motorists and pedestrians, attempting to prevent the protesters from getting to the vigil—despite the vigil being a public event. This screening allowed 13 White activists posing as Elvis fans through the police line—where they waited for an hour and then began chanting "Black Lives Matter"—while denying access to at least one Black man who claimed to "love Elvis" and objected to racial profiling.[71] Police arrested three activists—two Black, and one White—for entering or refusing to leave Graceland.[72] Nonetheless, the protest remained peaceful.

In a weekly presentation to command staff, Reynolds presented the police operation at Graceland as successful. He warned of "radical groups" that were using "violence and destruction to promote or advance their own agendas."[73] Reynolds highlighted Garner's Facebook post recommending Alinsky's *Rules for Radicals* and noted that it was posted just one day before the bridge shutdown. Reynolds quoted Alinsky's "rule" 12: "Pick a target, freeze it, personalize it, and polarize it," and claimed that this tactic was being used by Memphis activists. For example, he claimed that a few activists at the Elvis vigil "intended to draw officers into a physical confrontation," and encouraged others "to bring cellphones and video cameras to capture officers arresting or assaulting protesters."[74] A concluding slide shows photos of the two activists who were arrested at the "Save the Greensward" zoo protest (Fergus Nolan and Maureen Spain), along with two activists arrested at the racial justice protest on August 15 (Spencer Kaaz and Dana Ashbury). It describes them as

[70] The briefing notes that the police department phoned each of the organizers to tell them that they would need a permit if more than 25 people were expected. Blanchard et al. v. City of Memphis, Exhibit G (August 5, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf.

[71] Bill Dries, "Elvis Vigil Draws Protest, Heavy Police Presence," *Memphis Daily News*, August 16, 2016, https://www.memphisdailynews.com/news/2016/aug/16/elvis-vigil-draws-protest-heavy-police-presence/.

[72] Blanchard et al. v. City of Memphis, Exhibit Q (n.d.), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf.

[73] Exhibit Q, ibid., p. 3, 21.

[74] Exhibit Q, ibid., p 3.

part of a "group" trying to "embarrass" law enforcement and thereby "undermine the bond between law enforcement and the community."

Even if Reynold's characterization is accurate, it is important to recognize that activists' efforts to embarrass police would not be illegal. Police should be trained to deescalate tensions, and it is an abdication of responsibility to blame members of the public when police respond with disproportionate force. But it is also worth noting that Reynolds' characterization of activists is not well-supported by evidence. Members of the "group" he describes did not all know each other; those associated with the zoo protest were not necessarily involved in racial justice protests, or vice versa. [75] Reynolds claims that Garner is "seldom" seen at demonstrations because his "goal is to be nominated to the CLERB [Civilian Law Enforcement Review Board]" and that he views himself as the CLERB "spokesperson."[76] But simple internet searches do not turn up the evidence one might expect to find of such ambitions.[77]

Reynolds framed the police response to demonstrations as successful because they avoided violent escalation. But activists felt that their concerns were not being taken seriously, and that they were living with threats of violence alongside structural violence. After several months of additional surveillance and tension with the police, the Coalition of Concerned Citizens sent a letter to Memphis mayor Jim Strickland and Elvis Presley Enterprises, accusing them of colluding "in the violation of the First Amendment rights of many citizens by not allowing them passage on a public, Federally funded street" to the Elvis vigil. They also objected to the "military equipment deployed by the MPD in a show of force against citizens, old men and old women, and even children."[78] And they criticized Elvis Presley Enterprises for profiting in the midst of a predominantly Black

[75] Nolan later testified that he did not know Ashbury, only casually knew Kaaz and Spain from the zoo protest, and did not attend the racial justice protests of the summer of 2016. Fergus Nolan, "MPD Documents from the ACLU Lawsuit," *Memphis Truth Commission* (blog), August 28, 2019, https://memphistruth.org/2019/08/28/mpd-documents-from-aclu-lawsuit/. The three activists that Reynolds associates with the Greensward movement are all White, whereas roughly half of the eight people that Reynolds associates with the racial justice protest are Black, suggesting significantly different demographics and causes; Kaaz is the only person described in association with both.

[76] Exhibit Q (footnote 72), p. 22.

[77] While Reynolds may be referencing private conversations with somebody, simple internet searches for "Garner" and "CLERB" do not support these claims; this surfaces several articles with quotes by Garner, or written by Garner, but in none of them is he seeking nomination or claiming to speak for CLERB.

[78] Michael Quander, "Memphis Mayor Woke up to People Playing Dead in His Front Yard," *WREG Memphis*, December 20, 2016, https://www.wreg.com/news/memphis-mayor-woke-up-to-people-playing-dead-in-his-front-yard/.

community but not investing in that community or paying a living wage. It concluded: “Would you rather that we just DIE, and decrease the surplus population?” [79]

The letter was dated December 18, 2016. The next morning, the Mayor of Memphis, Jim Strickland, woke up to find protesters associated with the Concerned Citizens Coalition playing dead on his lawn. Rallings recalls that some of the protesters were beating on Strickland’s windows and doors (at the time, Strickland claimed simply that they looked in his windows).[80] They promised to return every week, calling it “Coffee with the Mayor,” and to stage similar protests at the home of Jack Soden, the CEO of Graceland.[81]

Shortly after the demonstration, the Office of Homeland Security created a database of all protests beginning January 2016, including the “Group” and “key personnel” responsible, as well as any arrests and/or damage to critical infrastructure. Initially they cast a broad net, including things as innocuous as Black Lives Matter chapter meetings, but when several meetings passed with no incidents, they “fell off the list.”[82] Reynolds viewed the list as a means of focusing limited police resources.

Rallings also sought “a way to better protect the mayor’s home.”[83] He instructed Bass to “identify all individuals arrested at any protest in 2016 and all protest leaders” and prepare an “authorization of agency” for the Mayor’s residence, the Zoo, and Graceland, and “malls with any individuals who have been arrested or created a disturbance.”[84] This authorization would forbid individuals on the list from going to the specified locations.

[79] Michael Quander, “Memphis Mayor Woke up to People Playing Dead in His Front Yard,” ibid.
[80] Michael Quander, “Memphis Mayor Woke up to People Playing Dead in His Front Yard,” ibid.
[81] Blanchard et al. v. City of Memphis, Michael Rallings deposition (April 25, 2018), p. 65: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf; According to Reynolds they also said they would visit the director’s (Rallings) house: Reynolds deposition (footnote 27), p. 120.
[82] Reynolds deposition, ibid., p. 27.
[83] Rallings deposition (footnote 81), p. 64
[84] Blanchard et al. v. City of Memphis, Exhibit B (December 29, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf. Rallings later said he couldn’t recall “having much involvement” in the creation of the Authorization of Agency “other than it being presented to me,” and that he didn’t know who instructed Reynolds to create the list (Rallings deposition (footnote 81), p. 64). This is very evasive; he likely did not have a direct role in selecting individuals for the list, but he did ask Bass and his team to identify protest leaders and create an authorization of agency, as shown in Exhibit B.

Ultimately, authorizations of agency were created only for the mayor's and Soden's homes; the latter was quickly rescinded since Soden lived outside of Memphis.[85] However, individuals listed on the authorization were also added to a City Hall "escort list"—people who could not enter without a police escort. The escort list had been created years earlier to track disgruntled employees or people who had been fired by the city, but it suddenly expanded from a couple dozen to over 80 individuals. The authorization list was primarily created by Reynolds, who was tasked with making a list of associates of Keedran Franklin or the Coalition of Concerned Citizens. Reynolds looked for Franklin's social media contacts, anyone he had been arrested with, or who was "often seen" with him at "unlawful assemblies…that kind of thing."[86]

Lieutenant Albert Bonner, who was in charge of protecting the mayor, ordered that the authorization of agency along with detailed information on each person on the list—including driver's license photos, social security numbers, height, weight, and race—be printed and put in a folder, and that "everyone familiarize themselves with people on the list".[87] The resulting authorization came to include many individuals who were uninvolved with the die-in.

In mid-February, when Thomas Nolan attempted to attend a city council meeting, he was surprised to be turned away. He went to a local news agency, which filed a Freedom of Information Act request for the list.[88] Though Nolan and others should have been notified about the restrictions on their movements, many people discovered that they were blacklisted only after city released the list late Friday, February 17, 2017.[89]

The following Monday, Rallings responded to public outcry about the blacklist by acknowledging that names may have been added in error.[90] He initiated a review, but the damage was done; many

[85] Blanchard et al. v. City of Memphis, Exhibit A (January 4, 2017), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf. Reynolds recalls that Graceland and Soden's home were removed because that's a "Germantown problem." Reynolds deposition (footnote 27), p. 121, 123.

[86] Reynolds deposition, ibid. p. 122.

[87] Blanchard et al. v. City of Memphis, Exhibit C (January 17, 2017), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf, p. 23

[88] Sasha Jones, "MPD Releases List of Those on Memphis City Hall's 'Blacklist,'" *Action News 5 Memphis*, February 18, 2017, https://www.actionnews5.com/story/34536181/mpd-releases-list-of-those-on-memphis-city-halls-blacklist.

[89] Ryan Poe, "Memphis City Hall Requires Police Escort for Darrius Stewart's Mother, Protesters," *Memphis Commercial Appeal*, February 17, 2017, https://www.commercialappeal.com/story/news/government/city/2017/02/17/memphis-city-hall-requires-police-escort-darrius-stewarts-mother-protesters/98067844/.

[90] Bill Dries, "City Loses Appeal of City Hall Blacklist Damages," *The Daily Memphian*, July 12, 2021, https://dailymemphian.com/article/22910/memphis-city-hall-blacklist-lawsuit.

citizens felt betrayed. Devante Hill, an activist who had genuinely believed he had a constructive relationship with Mayor Strickland, felt deceived.[91] Similarly, Detric Golden, a former University of Memphis basketball player who was working with troubled youth, objected: "Everybody who knows Detric Golden knows I'm a model citizen. I do great things for this city."[92]

The list included the mother and aunt of Darrius Stewart. Elaine Blanchard, an ordained minister and graduate of the Memphis Police Department's Clergy academy, who had welcomed Rallings to her Presbyterian church for a meal in the fall of 2016, expressing support for the police. She had never been arrested, never visited the mayor's residence, and couldn't recall if she had ever been to city hall. She joked on Facebook: "This grammie is a gangsta!"[93]

On Tuesday after the list was released, over one hundred people protested in front of city hall, facetiously calling it a "weigh-in" because the heights and weights of many people had been listed erroneously.[94] And the next day, Blanchard, Keedran Franklin, Paul Garner, and Bradley Watkins sued the city, arguing that it had violated the 1978 consent decree and their First Amendment rights to free expression—not only by blacklisting them and other activists, but also by video surveilling protests, using social media collators like Geofeedia, and otherwise intimidating activists. By March, many names had been removed from the list but the lawsuit was just getting started.[95] And ironically, the very thing that the Memphis Police Department was trying to prevent activists from doing—undermining the "bond" between police and citizens—is exactly what surveillance accomplished.

[91] Sasha Jones, "MPD Releases List of Those on Memphis City Hall's 'Blacklist,'" (footnote 88).

[92] Sasha Jones, "Rallings Says Names Added to 'blacklist' by Mistake," *Action News 5 Memphis*, February 20, 2017, https://www.actionnews5.com/story/34549551/memphians-were-shocked-to-learn-of-city-hall-escort-list/?_ga=2.213109524.186117098.1628628219-1114997713.1628628219.

[93] David Waters, "Why Did This 'gangsta Grammie' Make the City Hall Escort List?," *Memphis Commercial Appeal,* February 20, 2017, https://www.commercialappeal.com/story/news/columnists/david-waters/2017/02/20/waters-gangsta-grammie-makes-city-hall-escort-list/98147540/.

[94] Annette Peagler, "100 Plus People Attend Protest Outside Of City Hall : They Oppose A-List," *ABC 24 Memphis*, February 10, 2017, https://www.localmemphis.com/article/news/local/100-plus-people-attend-protest-outside-of-city-hall-they-oppose-a-list/522-de14e0a0-8d17-4ead-911d-778c6c354abe.

[95] "City Hall Releases Updated 'Blacklist,'" *Action News 5 Memphis*, March 1, 2017, https://www.actionnews5.com/story/34638607/names-added-to-city-hall-blacklist-in-error-have-been-removed.

2.7 Structural racism and intelligence failure in Memphis

The Memphis case demonstrates how structural racism influences the ways that law enforcement uses information infrastructures to surveil activists. This was not primarily about individual bias—the Director of the Memphis Police Department and other key officers were Black and likely had sincere sympathies with the Black Lives Matter movement—but rather about the common tendency of organizations to treat their critics as suspect. Intelligence analysts conflated a peaceful movement for racial justice with groups that sometimes advocated violent tactics to accomplish racist goals. They also conflated lone individuals who had committed violent acts with the organizations that they "liked" on Facebook, even after those organizations disavowed the individuals. Ironically, the Memphis Police Department could have improved its intelligence simply by reading public webpages about the history, leadership, and actions of groups such as the Nation of Islam and the New Black Panther Party.[96] Instead, they surveilled people who criticized the police.

Structural racism influenced not just who was surveilled, but also how information was focused, framed, and disseminated to others. The Memphis Police Department encouraged further suspicion and surveillance of activists through Joint Intelligence Briefings that framed peaceful demonstrations in the same context as violent attacks on police officers.

The Memphis case illustrates at least three risks of embedding structural racism in intelligence. First, surveillance took a toll on racial justice activists, many of whom were persons of color already living with anxiety about potential harassment by police. Ironically, protesting surveillance and harassment only fueled more of the same. For example, on July 14, 2016, Frank Gibson and another man, Monteiro Batts, entered a police station to complain that a police officer had called Gibson with threats to his family and to charge him with something that would "stick."[97] The next day, a Joint Intelligence Briefing described this encounter with headshots of Gibson and Batts from DMV databases, and noted that Gibson and Batts had exhibited "suspicious behavior" by "circling the precinct after they left."[98] The briefing did not address the question of whether Gibson had in fact been threatened by police.

[96] The Southern Law Poverty Center, for example, provides detailed information about hate groups in the United States: https://www.splcenter.org/issues/hate-and-extremism.
[97] Blanchard et al. v. City of Memphis, Exhibit H (July 15, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf.
[98] Exhibit H, ibid.

Two years later, as Memphis activists' lawsuit against the city got underway, more evidence of harassment emerged. The same day that the hearings opened more than two dozen police cars blocked off the street where activist Antonio Cathey's uncle and grandmother lived, while over fifty officers, many heavily armed, raided their homes. When Cathey's grandmother called him, he rushed to the scene, terrified for her safety. According to Cathey, police wouldn't explain why they were there, except to say "We know all about you" and "We know who you are."[99] Ultimately, the raid produced nothing more than traces of marijuana on an ashtray—not enough to arrest anyone, but police issued a citation.[100]

Activists thus feared for their and their families' safety. Some of Cathey's family members told him that they supported his activism but wished he would stop attending protests. [101] Keedran Franklin began avoiding family members to avoid entangling them in the web of surveillance.[102] Franklin, Cathey, and others also recall being followed by unmarked cars and pulled over for spurious reasons.[103] For Black motorists who are well aware of how traffic stops easily become occasions for police brutality, traffic stops were very stressful.[104] Wendi C. Thomas, a Black reporter covering racial justice issues, was observing the trial of the MPD when she learned that her social media account had been targeted by the Office of Homeland Security. Thomas watched her back and showed anxiety about speaking to other journalists in public spaces, describing Memphis as "one big plantation."[105] Elaine Blanchard, a White activist and reverend, felt that her employment at a non-profit was jeopardized by being blacklisted from City Hall, while Earle Fisher, the only Black pastor to be added to the City Hall escort list, also felt threatened by police for his activities with Black Lives Matter. [106]

[99] Speri, "The Fire This Time," (footnote 20).
[100] Jamiles Lartey, "'It's Definitely Intimidation': Police Accused over Raids on Activist's Family," *The Guardian*, August 26, 2018, https://www.theguardian.com/us-news/2018/aug/26/memphis-police-raids-activists-family-black-lives-matter.
[101] Speri, "The Fire This Time," (footnote 20).
[102] Blanchard et al. v. City of Memphis, Opinion and Order (October 26, 2018), p. 30-31, available at: https://www.aclu-tn.org/wp-content/uploads/2018/10/151-Order-Memphis.pdf. Elaine Blanchard also expressed anxiety over police surveillance.
[103] See for example: Speri, "The Fire This Time," (footnote 20).
[104] Thomas, "The Police Have Been Spying on Black Reporters and Activists for Years," (footnote 9).
[105] Speri, "The Fire This Time," (footnote 20).
[106] "City, ACLU Wrap Surveillance Case; Judge Decision to Come Later This Year," *Action News 5 Memphis*, August 23, 2018, https://www.actionnews5.com/story/38948645/city-aclu-wrap-surveillance-case-judge-decision-to-later-this-year.

Second, structural racism in the use of information infrastructures for intelligence poses risks to the racial justice movement and its goals. The 2018 ruling ultimately found that the "negative subjective reaction" of many activists to surveillance was not sufficient to prove that the police had harassed them or interfered with their First Amendment rights.[107] Nonetheless, law enforcement agencies have long used psychological stress as a means of suppressing dissent. For example, agents working for COINTELPRO, mentioned earlier, worked to break up marriages and alienate people from their professions, recognizing that the resulting stress undermined the effectiveness of activists.[108] For that matter, one explicit purpose of highly visible surveillance cameras and other forms of police presence is precisely to create "subjective" feelings that deter illegal activities. And given the hostility that many police have often shown towards their critics, it can hardly be surprising that such surveillance can also deter activism aimed at reform.[109]

Legitimate concerns about surveillance also limit activists' ability to grow the movement freely on social media, as they must approach new contacts with suspicion. Some Memphis activists correctly suspected Bob Smith of being a cop; at least one stated plainly: "You sound like a cop. Identify yourself or get blocked." When Smith demurred that he was not a cop, the activist replied: "none of our mutuals know you."[110] Garner let Smith into his network, but later reflected that he "always assumed there are cops on my profile, many of whom I've blocked." As this suggests, anxiety about surveillance could lead organizers to shut out legitimate activists online.

Third, when structural racism shapes intelligence, it diverts resources from serious threats and thereby wastes resources and increases risks to law enforcement and the public that it is sworn to protect. For example, the Memphis Police Department sent air support for a demonstration that never materialized and warned officers to be vigilant about "Day of Rage" protests that were entirely fictional.[111] Meanwhile, many racial justice activists felt that the police did not devote

[107] "Court order for Blanchard et al. v. City of Memphis (footnote 10).
[108] Margaret Talbot, "Opened Files*," The New Yorker*, January 12, 2014, https://www.newyorker.com/magazine/2014/01/20/opened-files; "More About FBI Spying," American Civil Liberties Union, accessed December 10, 2021, https://www.aclu.org/other/more-about-fbi-spying.
[109] Kim Barker, Mike Baker, and Ali Watkins, "In City After City, Police Mishandled Black Lives Matter Protests," *The New York Times*, March 20, 2021, https://www.nytimes.com/2021/03/20/us/protests-policing-george-floyd.html.
[110] George Joseph, "Meet 'Bob Smith,' The Fake Facebook Profile Memphis Police Allegedly Used To Spy On Black Activists," *The Appeal,* August 2, 2018, https://theappeal.org/memphis-police-surveillance-black-lives-matter-facebook-profile-exclusive/.
[111] Day of Rage discussion can be found in Blanchard et al. v. City of Memphis, Exhibit H, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/1-Exhibits-A-M_Redacted.pdf. Air support for the

adequate resources to protecting them from White supremacist groups such as the Ku Klux Klan.[112] For example, in mid-July 2016, several Black Lives Matter (BLM) activists used Facebook to discuss concerns that the Ku Klux Klan (KKK) was planning to attend a protest. One activist urged others to "pray for peace saints," while another warned others to "be safe" and "Steer clear of ignorance."[113] One activist stated that she would take "my gun and my blade," "just in case," and another immediately cautioned her: "don't be a hashtag."[114] An officer in the Real Time Crime Center shared these posts with others, but focused on the single comment about self-defense, reporting that "they are going armed with gun/knives."[115] This not only misrepresented a single comment as a collective activity, but also neglected the multiple comments about staying safe and peaceful. Meanwhile, officers made no comment about the activists' original concern: violence from the KKK. While we cannot be certain that they did not monitor the KKK, the discussion gave no indication that they intended to do so.

In the concluding section of this report, we discuss an even more egregious example of how intelligence professionals failed to identify a threat from White supremacist and related groups. But first, we provide a more general discussion of how structural racism can shape the use of information infrastructures for intelligence gathering and production.

3. Information Infrastructures: Technological Change and Privacy Laws

A large body of research has shown that information infrastructures tend to reflect and reinforce social inequalities, including structural racism.[116] Humans and the algorithms they design construct databases by selecting "raw data" from the complex context of everyday life, and making it

demonstration that didn't materialize is discussed in Blanchard et al. v. City of Memphis, Exhibit DD, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/3-Exhibits-Y-HH_Redacted.pdf.

[112] See, e.g., Jenni DiPrizio, "A Look at Differences in How Memphis Police Handle Different Protests," *ABC 24 Memphis*, May 6, 2020, https://www.localmemphis.com/article/news/local/how-memphis-police-handle-different-protests/522-1a2bcea7-71a3-4aee-a250-d2f1918c8bbf; Speri, "The Fire This Time" (footnote 20).

[113] Blanchard et al. v. City of Memphis, Exhibit U (July 10, 2016), available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/2-Exhibits-N-X_Redacted.pdf.

[114] Exhibit U, ibid.

[115] Exhibit U, ibid.

[116] Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (John Wiley & Sons, 2019); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Publishing Group, 2018); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (NYU Press, 2018).

available for individuals to recontextualize for their own purposes. Sometimes this process deliberately reinforces inequalities, as for example in the case of racial classifications in Apartheid South Africa.[117] But other times the reinforcement is almost accidental. For example, internet search engines automatically rank the most popular websites highly, thereby directing searchers to pages that maintain common derogatory stereotypes of minorities.[118]

This report highlights four ways in which the rise of digital computing and networking has tended to reinforce structural racism in the development and use of information infrastructures for law enforcement. First, dropping costs of information storage and processing have allowed law enforcement and private companies to gather, store, and use growing volumes of information about increasingly minor interactions with individuals. This increases the chances that police enter someone into criminal record-keeping systems simply for acting "suspicious" or committing a minor offense (like turnstile jumping or drinking in public).[119] Since Black and Brown people tend to be subject to more policing than White people for such offenses, this contributes to the overrepresentation of minorities in criminal records systems.[120]

Second, the rise of computer networking and an associated industry has increased the scale and efficiency of information sharing among law enforcement at all levels of government. This was not an inevitable result of technological change, and at times private sector interests in proprietary and non-interoperable systems actually limited information sharing.[121] Myriad law enforcement and intelligence organizations developed unique record-keeping systems which were not interoperable, and while companies marketed systems that promised to facilitate information sharing, they eventually produced dozens if not hundreds of systems which ironically were themselves not interoperable.[122] Nonetheless, as we discuss further below, over the last half of the twentieth century and into the new millennium, law enforcement information-sharing infrastructure has expanded dramatically. Today, this makes it easier for an individual stopped by local police for a petty offense

[117] Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (MIT Press, 2000).
[118] Noble, *Algorithms of Oppression* (footnote 116).
[119] Simon A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press, 2009). See also Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (Oxford University Press, 2020).
[120] Cole, *Suspect Identities*, ibid.
[121] John S. Hollywood and Zev Winkelman, "Improving Information-Sharing Across Law Enforcement: Why Can't We Know?" (RAND Corporation, September 4, 2015), https://www.rand.org/pubs/research_reports/RR645.html.
[122] Hollywood and Winkelman, ibid.

to become subject to suspicion by state or federal law enforcement for more serious crimes. Again, since persons of color are disproportionately stopped for petty offenses, information sharing among different federal agencies increases their risk of being subjected to "mission creep"—wherein data gathered for one purpose are used for another. Furthermore, law enforcement collection can often access data from social services; since minorities are more likely than White people to be reliant on government social safety nets, this can contribute to the criminalization of persons of color and make many reluctant to seek the support they need.[123]

Third, growth in data processing and storage power enabled the growth of data analytics companies and the rise of "predictive" or "data-driven" policing, wherein analyses of crime statistics are used to make decisions about where to allocate resources. Because crime statistics increase not only with crime frequency, but also with the frequency of police patrols, reliance on past crime data tends to create a feedback loop that reinforces a historical tendency to treat minority communities as suspect, while all under a facade of objectivity.[124]

Fourth, the rise of "surveillance capitalism"—wherein companies harvest and sell data about the behavior of internet users—has disproportionately affected activists who rely on social media and other networking infrastructures to mobilize public protest. Activists' behavior, by virtue of its public nature, is "low hanging fruit" for an industry eager to gain customers in law enforcement. As we discuss further below, these companies often market to law enforcement's fears of activists who protest police brutality and mobilize for racial justice.

Importantly, none of the dynamics noted above were inevitable results of technological change; rather they emerged from social structures and priorities. This means that laws and policies may be able to reshape the development and use of information infrastructures for law enforcement. In fact, U.S. laws already do provide some protection against undue surveillance. Although "privacy" is never mentioned in the Constitution, the Fourth Amendment directs that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[125] In other words, law

[123] Brayne, *Predict and Surveil* (footnote 119). Eubanks, *Automating Inequality* (footnote 116).
[124] Brayne, *Predict and Surveil* (footnote 119).
[125] "Fourth Amendment," Cornell University Legal Information Institute, https://www.law.cornell.edu/constitution/fourth_amendment, accessed December 10, 2021.

enforcement cannot search an individual's home and belongings without a court determining that the search is warranted by prior evidence suggesting likely criminal behavior.

Historically, the development of new information and communications technologies has continually raised the question of what constitutes "unreasonable" search and seizure. The 1967 Supreme Court case Katz v. United States established that the Fourth amendment prohibits searches where individuals have a "reasonable expectation of privacy," which is defined as situations in which they demonstrate a "subjective expectation" that their information is private *and* that expectation is recognized as reasonable by broader society.[126] While Katz continues to be treated as a guiding precedent, the question of what society recognizes as a reasonable expectation of privacy is subjective and has been interpreted in ways that many citizens might find surprising, as we discuss further below.

The U.S. Congress and many states have also passed laws designed to protect citizens' privacy. For example, growing concerns about computerization of government databases in the late 1960s led to public debate about risks to privacy and ultimately to the 1974 Privacy Act, which restricts federal agencies from disclosing records about an individual to anyone outside the agency, including other federal agencies, without prior consent of the individual concerned. While the Privacy Act helps to limit "mission creep," it is weakened by exceptions. For example, an agency can disclose information with another agency "for a purpose which is compatible with the purpose for which it was collected."[127] Federal, state, and local law enforcement organizations routinely share information under this vague exception.

In what follows, we discuss how the technological and legal changes outlined above have tended to amplify structural racism as police use three different kinds of information infrastructures: law enforcement databases, surveillance cameras, and new social media.

[126] Charles Katz was convicted of transmitting illegal information about gambling through a public payphone. The FBI used electronic listening devices to acquire information about Katz to convict him. The Supreme Court overturned the rulings of the lower courts, arguing that Katz's Fourth Amendment rights were violated because he had a "reasonable expectation" that his conversation would not be heard outside of the phone booth. Charles Katz, Petitioner, v. United States (Supreme Court December 18, 1967), https://www.law.cornell.edu/supremecourt/text/389/347.

[127] "Overview of the Privacy Act: 2020 Edition," United States Department of Justice, October 14, 2020, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties.

4. Law Enforcement Databases

Racial discrimination was built into law enforcement information systems from the very founding of the United States. Before the Civil War, runaway slave advertisements, branding tools, and networks of watchmen and slave patrols formed a comprehensive information system geared towards dehumanizing the enslaved, as well as managing and tracking their movements.[128] After the Civil War, law enforcement remained intentionally complicit in violence against Black people, particularly in the U.S. South, where some departments originated as slave patrols.[129] Even after the Civil Rights Act was passed, and federal law enforcement agencies began to provide some measure of protection against discrimination, discriminatory patterns of policing continued, resulting in much higher rates of arrest, conviction, and incarceration for Black and Brown communities than for White people. Criminal records systems thus overrepresented Black and Brown communities, further encouraging surveillance and policing.[130]

Criminal records systems also embedded assumptions about racial difference. For example, in the 1920s the New York Police Department divided fingerprint records into separate “black,” “yellow,” and “white” files, on the assumption that fingerprints would look different in these categories. When a suspect was brought in, officers searched only the file corresponding to their skin color, making the work of matching easier—but also biased.[131]

Computerization enabled law enforcement to share and search for information more efficiently, but did not eliminate the racial biases intrinsic in law enforcement databases. The Federal Bureau of Investigation began coordinating record-keeping among state and local law enforcement organizations as early as 1924, when it established its “Identification Division,” which collected fingerprint information from organizations across the nation, and searched for matching prints upon

[128] Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

[129] Connie Hassett-Walker, “How You Start Is How You Finish? The Slave Patrol and Jim Crow Origins of Policing,” *Human Rights*, January 12, 2021, available at: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/civil-rights-reimagining-policing/how-you-start-is-how-you-finish/.

[130] Elizabeth Hinton, *From the War on Poverty to the War on Crime: The Making of Mass Incarceration in America* (Harvard University Press, 2016); Michelle Alexander, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness* (The New Press, 2012).

[131] Simon Cole, *Suspect Identities* (footnote 119), p. 164.

request.[132] It began automating the system with IBM card sorters in the 1930s.[133] In 1992, the FBI's Identification Division became the Criminal Justice Information Services (CJIS) division, which today maintains many databases and tools for use by law enforcement organizations at all levels of government.[134] For example, the National Crime Information Center (NCIC) was launched in 1967 and today includes seven files on property (e.g., separate files for guns, stolen articles, and license plates) and fourteen files on people (e.g., different files for missing persons, sex offenders, suspected terrorists). The FBI describes the NCIC as the "lifeline of law enforcement."[135]

The FBI's CJIS also includes the National Data Exchange (N-DEx), a searchable database containing records from thousands of law enforcement organizations nationwide, and tools for sharing information or visually depicting relationships between people, events, and places.[136] Similarly, the FBI's Law Enforcement Enterprise Portal (LEEP) provides a wide range of web-based tools, such as a virtual command center for real-time incident response (e.g., to active shooter incidents, child abductions, and presidential inaugurations).[137]

Other federal agencies have also developed information-sharing infrastructures for law enforcement. For example, in 1990 the Treasury Department created a Financial Crimes Enforcement Network (FinCEN) to help detect money laundering and other kinds of crimes.[138] FinCEN maintains a database of "Suspicious Activity Reports," (SARs) which financial organizations are required to file within thirty days of observing particular kinds of transactions (e.g., cash transactions in excess of $10,000 in a single day).[139] Law enforcement and regulatory

[132] "Criminal Justice Information Services (CJIS)," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis, accessed December 10, 2021.
[133] Simon Cole, *Suspect Identities* (footnote 119), p. 251.
[134] "Criminal Justice Information Services (CJIS)," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis, accessed December 10, 2021.
[135] "National Crime Information Center," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis/ncic, accessed December 10, 2021.
[136] "National Data Exchange (N-DEx)," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis/ndex, accessed December 10, 2021. See also: Hollywood and Winkelman, "Improving Information-Sharing Across Law Enforcement" (footnote 121).
[137] "Law Enforcement Enterprise Portal (LEEP)," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis/leep, accessed December 10, 2021.
[138] "Law Enforcement Overview," Financial Crimes Enforcement Network, https://www.fincen.gov/resources/law-enforcement-overview, accessed December 10, 2021.
[139] "Suspicious Activity Reports (SAR)," Office of the Comptroller of the Currency, March 4, 2019, https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html.

organizations can search the FinCEN portal for SARs and other financial information that may indicate criminal activity, such as money laundering.[140]

State and local organizations have also developed systems for sharing information.[141] For example, dozens of U.S. state law enforcement organizations (such as highway patrols) established the National Law Enforcement Telecommunications System (NLETS) in the 1960s, and today it is used by all U.S. states and territories, as well as some international organizations.[142] Additionally, in the 1970s and 1980s, several law enforcement organizations formed regional information exchanges, and these were eventually connected through the Regional Information Sharing Systems Program (RISS).[143] Today six regional networks share information through RISS, including databases on gangs, terrorism, and other criminal records.[144] As noted above, the Memphis Police Department used RISS to gather information on racial justice activists who had crossed state lines.

Despite the development of extensive information sharing infrastructures, intelligence agencies have not always used that information effectively. For example, the intelligence failures that allowed the terrorist attacks of September 11, 2001, were not about a lack of information available in databases, or even a lack of analysis, but rather about the FBI's failure to respond effectively to that analysis.[145] Nonetheless, the U.S. federal government responded to the intelligence failure by pushing for better information sharing infrastructure.[146] Most notably, the Homeland Security Act of 2002 integrated 22 disparate federal agencies into a new Department of Homeland Security

[140] "Fact Sheet: The FinCEN Portal," Financial Crimes Enforcement Network, accessed December 10, 2021, https://www.fincen.gov/sites/default/files/shared/Facts_FinCENPortal.pdf.

[141] For an overview of several systems, see Hollywood and Winkelman, "Improving Information-Sharing Across Law Enforcement" (footnote 121).

[142] "About: Who We Are," National Law Enforcement Telecommunications System (NLETS), https://www.nlets.org/about/who-we-are, accessed December 10, 2021. On the history of NLETS see John E. Craft, "Final Report for National Law Enforcement Telecommunication System Upgrade Project, 1973-1977" (National Law Enforcement Telecommunications Systems, Inc., 1977), available at: https://www.ojp.gov/pdffiles1/Digitization/48514NCJRS.pdf.

[143] "RISS Overview," Regional Information Sharing Systems, https://www.riss.net/about-us/, accessed December 10, 2021.

[144] "RISS Overview," ibid.

[145] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton University Press, 2009).

[146] For example, in 2003, motivated by both 9/11 and the U.S.S. Cole bombing, the U.S Navy launched the Law Enforcement Information Exchange (LInX), an information sharing network for law enforcement organizations. While the Navy pays for the service to monitor activity near its bases, law enforcement in other areas can also pay to access the network. "NCIS Law Enforcement Information Exchange (LInX)," Naval Criminal Investigative Service, https://www.ncis.navy.mil/Mission/Partnership-Initiatives/LInX-D-Dex/, accessed December 10, 2021.

(DHS).[147] In April 2005, the Chief Information Officers of DHS and the U.S. Department of Justice launched the National Information Exchange Model, which built on previous efforts to improve information sharing among state and local governments.[148]

The 9/11 Commission Act of 2007 further directed the Department of Homeland Security "to establish a State, Local, and Regional Fusion Center Initiative" to facilitate sharing between and among federal, state, and local law enforcement and intelligence organizations.[149] There are currently 54 fusion centers in all 50 states as well as Washington, D.C. and other U.S. territories. According to a study from the Government Accountability Office (GAO), there were "nearly 300 representatives from agencies—such as the Department of Homeland Security's Office of Intelligence and Analysis, TSA, the FBI, and the DEA, among others" [150] distributed nationwide (although the exact distribution of personnel-to-center was not spelled out).

Although fusion centers were ostensibly established to monitor terrorist threats, they have demonstrated "mission creep" by casting suspicion on civil society groups exercising constitutionally-protected rights, including those concerned with racial justice. For example, in 2009, a fusion center in Virginia issued a terrorism threat assessment that described some historically Black colleges and universities as "radicalization nodes."[151] A 2012 report by the Senate Permanent Subcommittee on Investigations found that fusion centers "forwarded 'intelligence' of uneven quality–oftentimes shoddy, rarely timely, sometimes endangering citizens'

[147] "Creation of the Department of Homeland Security," Department of Homeland Security, February 17, 2011, https://www.dhs.gov/creation-department-homeland-security, accessed December 10, 2021.
[148] "NIEM's History," National Information Exchange Model, https://www.niem.gov/about-niem/history, accessed December 10, 2021. The NIEM includes the Law Enforcement Information Sharing Program Exchange Specification (LEXS), which helps in the translation of information that may be stored in different formats by different law enforcement organizations.
[149] Quoted in Thomas Nolan, *Perilous Policing: Criminal Justice in Marginalized Communities* (Routledge, 2019), p 143.
[150] Jason Barnosky, "Fusion Centers: What's Working and What Isn't," *Brookings Institution* (blog), March 17, 2015, https://www.brookings.edu/blog/fixgov/2015/03/17/fusion-centers-whats-working-and-what-isnt/.
[151] "Fusion Center Declares Nation's Oldest Universities Possible Terrorist Threat," American Civil Liberties Union, available at: https://www.aclu.org/press-releases/fusion-center-declares-nations-oldest-universities-possible-terrorist-threat. See also the Brennan Center's letter to Congress urging investigation of DHS sending the fusion centers data on protests of the Trump administration's immigration policies in 2018, discussed further in the section on social media: https://www.brennancenter.org/our-work/research-reports/brennan-center-urges-congress-hold-hearings-fusion-centers.

civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."[152]

In fact, many law enforcement personnel came to mistrust fusion centers, particularly after they flagged social media posts that sent officers on "wild goose chases."[153] As this suggests, law enforcement organizations have not always agreed upon how to use new social media for intelligence—a topic to which we now turn.

5. Social Media and Mobile Devices

Federal, state, and local law enforcement agencies commonly use mobile devices and social media platforms such as Facebook, Instagram, and Twitter to monitor for illegal activity and threats.[154] While these tools can be legitimately useful for improving public safety, they have often been used in ways that undermine civil liberties. For example, as the police killing of unarmed Black teenager Michael Brown gave momentum to the Black Lives Matter movement in 2014, law enforcement organizations ramped up surveillance of social media accounts held by racial justice activists. The Department of Homeland Security played a leading role, collecting extensive data on racial justice events across the country and sharing it with state and local agencies to provide what DHS described as "situational awareness."[155] This surveillance tended to conflate lawful activism with terrorism; for example, DHS worked with New York City Police Department's SHIELD, a counterterrorism force, to monitor social media activity related to a vigil for Michael Brown.[156]

[152] "Federal Support for and Involvement in State and Local Fusion Centers" (United States Senate Permanent Subcommittee on Investigations, October 3, 2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

[153] Phoebe Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," *Washington Post,* October 31, 2021, https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/.

[154] A 2016 survey conducted by the International Association of Chiefs of Police and the Urban Institute found that 70% of the 539 American law enforcement organizations surveyed used social media to gather intelligence for investigations. In addition, 59% had contacted social media companies to obtain information to use as evidence in criminal investigations. KiDuek Kim, Ashlin Oglesby-Neal, and Edward Mohr, "2016 Law Enforcement Use of Social Media Survey" (International Association of Chiefs of Police and the Urban Institute, March 3, 2017), https://www.urban.org/research/publication/2016-law-enforcement-use-social-media-survey/view/full_report.

[155] George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," *The Intercept*, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

[156] Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," ibid.

Racial justice activists are particularly vulnerable to such surveillance and harassment, both by virtue of the public nature of their work, and because law enforcement is naturally suspicious of its critics. We begin this section by briefly overviewing laws that aim to protect civil liberties online, before turning to three common and somewhat overlapping methods that law enforcement uses: targeted tracking of activists, including the use of deception on social media; mass surveillance of social media activity through data analytic platforms and services; and geofencing technologies.

As noted above, the U.S. Supreme Court has determined that citizens have Constitutional protections against surveillance where they have a "reasonable expectation" of privacy. However, in the late 1970s, the Supreme Court established what has come to be known as "third party doctrine," which states that people who willingly distribute and give their information to a third party have no reasonable expectation that the information will remain private.[157] This freed law enforcement to gather information from employers, businesses, and even individuals' close friends without obtaining a warrant.

In the 1980s, the growth of computerized communications networks raised questions about just how broadly third party doctrine should be interpreted. Since all such communications pass through network service providers—a third party—it would seem that law enforcement could access all internet communications without a warrant. Additionally, as it became increasingly common for computer users to store information on servers managed by other organizations (similar to what we would today call the "cloud"), questions emerged about whether third party doctrine applied to all of that information. In 1986, the U.S. Congress passed the Stored Communications Act to limit law enforcement's access to information that was stored by such organizations. The Act prohibits "public" service providers—companies that provide services to any paying customer—from voluntarily disclosing most kinds of information. But it places no such restrictions on "private" service providers, such as universities, government organizations, and other organizations providing services only to their constituents. Nonetheless, all service providers can disclose some information to law enforcement or other federal agencies, such as information accidentally obtained about a crime, or information indicating an immediate physical threat to another person. And most

[157] Rachel Levinson-Waldman, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media," *Oklahoma Law Review* 71, no. 4 (January 1, 2019), p. 1009. In particular, in United States v. Miller in 1979, the Supreme Court ruled that the Fourth Amendment did not protect Jack Miller's bank account information because he willingly gave his information to a third party (the bank), see: https://www.oyez.org/cases/1975/74-1179.

notably, law enforcement can compel disclosure from either type of organization by obtaining a subpoena, warrant, or similar court order.[158]

The growing prevalence and functionality of cell phones—which are now used not only for voice communications but also social media postings, texting, and much more—has also created new opportunities for surveillance. For example, police can use cell site simulators that connect to mobile communication devices in an area, gathering information about locations, cell phone identifiers, and even voice and text messages. While simulators are typically used to monitor phones known to belong to specific suspects, they also sweep up metadata (such as cell phone identifiers) on all phones connected to them.[159] And while federal agencies are required to obtain a warrant to use a simulator, and must configure it to gather only metadata (such as location and times of calls), restrictions on state and local law enforcement organizations varies by state.[160] Relatively little is known about how these systems are used, but Black Lives Matter protesters have suspected that they have been surveilled using such simulators.[161]

In what follows, we outline three ways in which law enforcement commonly uses information gathered from social media and cell phones: targeted surveillance, including the use of deceptive

[158] See Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review* 72 (2003): 1208–43. Law enforcement can obtain a search warrant only if they persuade a judge or magistrate that there is probable cause of a crime. A warrant allows law enforcement to obtain information from a third party without prior notice to the person whose information is being requested. A subpoena can be obtained from a judge in a legal case; it must be granted by the judge, typically with prior notice to the person whose information is being gathered. A 2703(d) order is something like a mix between a warrant and a subpoena.

[159] "Cell-Site Simulators/IMSI Catchers," Electronic Frontier Foundation, https://www.eff.org/pages/cell-site-simulatorsimsi-catchers, accessed December 10, 2021.

[160] For a primer on cell site simulators, see "Cell Site Simulators: A Primer," National Association of Criminal Defense Lawyers, available at: https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf. Federal guidelines on the use of Cell Site simulators are available here: https://www.justice.gov/opa/file/767321/download.

[161] See, e.g., Fruzsina Eördögh, "Evidence of 'stingray' Phone Surveillance by Police Mounts in Chicago," *Christian Science Monitor*, December 22, 2014, https://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago; Isiah Holmes, "Milwaukee PD's Cell Phone Monitoring Technology," *Wisconsin Examiner*, March 16, 2021, https://wisconsinexaminer.com/2021/03/16/milwaukee-pds-cell-phone-monitoring-technology/; Ali Winston, "Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out," *The New York Times*, January 15, 2019, https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html.
One of the first uses of such simulators was to monitor for potential "criminal activities" at the Miami-Dade Free Trade Area of the Americas Conference in 2003, which almost certainly refers to protesters. See https://cdn.arstechnica.net/wp-content/uploads/2013/09/miami-dade.pdf. Cooper Quintin notes that there is "very little evidence" of the use of cell site simulators to surveil activists, but also acknowledges that it's a legitimate concern and provides guidelines for minimizing the risk: Cooper Quintin, "A Quick and Dirty Guide to Cell Phone Surveillance at Protests," Electronic Frontier Foundation, June 16, 2020, https://www.eff.org/deeplinks/2020/06/quick-and-dirty-guide-cell-phone-surveillance-protests.

social media accounts; mass surveillance through data analytics platforms; and the collection of geolocation data from cell phones. We then discuss the ways in which these intelligence-gathering practices tend to encourage overly aggressive policing of racial justice activists.

5.1 Mass Surveillance of Social Media and the Data Analytics Industry

Law enforcement commonly pays for the services of data analytics companies to help monitor social media.[162] These companies purchase access to data from social media companies such as Twitter, Facebook, and Instagram, and then analyze and market that data for potential customers.[163] They also develop software services that allow their customers to conduct their own searches and analyses of user behavior. Data analytics companies have aggressively marketed their services to police departments across the country, and have scored lucrative contracts to provide surveillance services for organizations at the local, state, and federal levels.

The data analytics industry poses special risks to racial justice activists, not only because their activities are "low hanging fruit" for companies to analyze, but because companies commonly adopt marketing tactics that pander to law enforcement suspicions of racial justice protesters. For example, in 2015, when the Canadian data analytics company MediaSonar began marketing its services to the Fresno Police Department, it included a list of keywords and hashtags that it claimed were associated with "illegal activities and threats to public safety."[164] These included not only keywords related to human trafficking, gang activity, and property crimes, but also "Mike Brown Related" hashtags, such as "blacklivesmatter," "dontshoot," "justiceformike," and "nojusticenopeace," effectively conflating racial justice activism with violent crime. The Fresno

[162] Alexandra Mateescu et al., "Data & Civil Rights: Social Media Surveillance and Law Enforcement," *Data & Society*, October 27, 2015, https://datasociety.net/library/data-civil-rights-social-media-surveillance-and-law-enforcement/.

[163] Some of these companies predate the internet, and grew out of the much older data analytics industry; for example, the company SAS was established in the late 1960s, but began marketing social media monitoring services to law enforcement around 2012. See G.W. Schulz, "Should Police Use Facebook & Twitter To Solve Crimes?" *Huffington Post*, September 4, 2012, https://www.huffpost.com/entry/web-surveillance-social-media_n_1854750.

[164] See: https://www.aclunc.org/docs/201512-social_media_monitoring_softare_pra_response.pdf#page=58, p. 58. The ACLU of California has released additional public records revealing the social media monitoring activities of law enforcement agencies across the state; see https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software.

Police Department seems to have found this approach persuasive, as they went on to do a test run with MediaSonar's online platform.[165]

Similarly, during the April 2015 demonstrations following the police killing of Freddie Gray, the "threat intelligence" firm ZeroFox sent the Baltimore Police Department a promotional "Crisis Management Report" that singled out Black Lives Matter organizers as threats to public safety. ZeroFox labeled DeRay McKesson and Johnetta Elzie, two Black activists who had organized demonstrations in Baltimore, as "high" severity "physical threats."[166] The report provided no evidence that they posed a physical threat to anyone. In fact, after the report went public, ZeroFox founder Evan Blair stated that the labels weren't meant to imply that Elzie and McKesson intended to harm anyone, and that they were likely identified because of the number of followers they have on Twitter.[167] This suggests that ZeroFox's threat intelligence mischaracterizes racial justice "influencers" as "physical threats."

ZeroFox's marketing report encouraged surveillance of McKesson and Elzie—and not just by local police. ZeroFox also reached out to an FBI program for partnering with private providers of critical infrastructure, Infragard. In its outreach to Infragard and the city of Baltimore, company representatives further stated that they had briefed their "classified partners" at Fort Meade, the headquarters of the National Security Agency. This is strange, since NSA is responsible for military rather than domestic intelligence, and suggests that ZeroFox may have been boasting of high-level connections rather than reporting on meaningful intelligence.[168] It is unclear whether ZeroFox's marketing had any influence on surveillance of racial justice activists. The Department of Homeland Security had already monitored McKesson's social media accounts during the Baltimore protest, and in August 2015 DHS agents arrested McKesson and Elzie for obstructing the entrance

[165] Matt Cagle, "This Surveillance Software Is Probably Spying on #BlackLivesMatter," ACLU of Northern California, December 15, 2015, https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.

[166] https://s3.documentcloud.org/documents/2190997/zerofox-crisis-management-report.pdf.

[167] Stephen Babcock, "ZeroFOX under Fire for Social Media 'Threat Actors' Report during Baltimore Riots," *Technical.ly Baltimore*, August 4, 2015, https://technical.ly/baltimore/2015/08/04/zerofox-fire-social-media-threat-actors-report-baltimore-riots/.

[168] Brandon E. Patterson, "Black Lives Matter Organizers Were Labeled as 'Threat Actors' by a Cybersecurity Firm," *Mother Jones*, August 3, 2015, https://www.motherjones.com/politics/2015/08/zerofox-report-baltimore-black-lives-matter/.

to a St. Louis courthouse during a demonstration commemorating the first anniversary of Michael Brown's death.[169]

Nonetheless, it is clear that data analytics companies encourage law enforcement suspicion of activists in their marketing efforts. For example, DataMinr marketed a case study of its ability to track a student protest in South Africa.[170] In e-mail correspondence with the Los Angeles Police Department in 2015, the company Dataminr highlighted its exclusive access to the Twitter "Firehose" data feed, which allows the company to scan every public tweet as soon as it is published. Dataminr also gave some fusion centers direct access to its products.[171]

One particularly troubling example of the ways that marketing can exacerbate surveillance of activists comes from law enforcement's interactions with the data analytics company LookingGlass Cyber Solutions. In 2018, LookingGlass sent the Department of Homeland Security a report on roughly 600 protests against the Trump Administration's harsh treatment of undocumented immigrants, which was based on analysis of public sources such as Facebook. DHS disseminated it through their fusion centers. When the report came to light, DHS stated that the report was "unsolicited" but that they were nonetheless "required to share it [with state law enforcement organizations] consistent with DHS policy to ensure stakeholders have appropriate situational awareness."[172] These interactions suggest that the data analytics industry can exacerbate suspicion of activists by harvesting readily-available information and marketing it as "intelligence" for law enforcement agencies. When law enforcement organizations like DHS forward such reports to others, they amplify not only marketing campaigns, but also the conflation of racial justice protest with criminal activity.

In principle, law enforcement organizations could use social media analysis platforms for legitimate purposes. But in practice, police have used such tools in ways that amplify bias against particular

[169] Jason Leopold, "Emails Show Feds Have Monitored 'Professional Protester' DeRay Mckesson," *Vice News*, August 11, 2015, https://www.vice.com/en/article/qv58n3/emails-show-feds-have-monitored-professional-protester-deray-mckesson; Daniel Victor, "Black Activists Arrested in Ferguson Protests," *The New York Times*, August 10, 2015, https://www.nytimes.com/2015/08/11/us/blacktwitter-leaders-arrested-in-ferguson-protests.html.

[170] Nicole Ozer, "Twitter Cuts Off Fusion Spy Centers' Access to Social Media Surveillance Tool," American Civil Liberties Union, December 15, 2016, https://www.aclu.org/blog/privacy-technology/internet-privacy/twitter-cuts-fusion-spy-centers-access-social-media.

[171] Ozer, "Twitter Cuts Off Fusion Spy Centers' Access to Social Media Surveillance Tool," ibid.

[172] Ryan Devereaux, "Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests," *The Intercept*, April 29, 2019, https://theintercept.com/2019/04/29/family-separation-protests-surveillance/.

minorities and racial justice activists. For example, from 2014-16, the Boston Police Department secretly used Geofeedia to scan and collect posts related to race, religion, and political activity; among other things, they tracked public school students who were protesting budget cuts, and filtered for Arabic words to target Muslims.[173] And as noted in the first section of this report, the Memphis Police Department used Geofeedia and related tools to monitor racial justice activists.

Similar dynamics have been seen in much smaller cities, which can now often afford social media monitoring platforms. For example, in 2017 activists in Clarkstown, New York—a town of around 84,000 people—sued their police department for using social media monitoring in a manner that conflated lawful protest with criminal activity.[174] Clarkstown police searched for “The Black Lives Matter Movement” and “Protests,” along with “Gangs,” Violence,” “Terrorism,” and “Heroin Initiative,” despite the district attorney repeatedly warning them not to target activists.[175]

In 2016, Twitter, Facebook, and Instagram responded to controversy about such incidents by publicly announcing that they would terminate the special access they offer to Geofeedia and companies that engage in surveilling protests.[176] Twitter’s Vice President blogged that “using Twitter’s Public APIs [application programming interfaces] or data products to track or profile protesters and activists is absolutely unacceptable and prohibited.”[177] It continued to allow Dataminr access to its feeds, but emphasized that Dataminr had cut off direct access to federal fusion centers.

[173] In 2016, BPD ended its contract with Geofeedia, but it soon requested $1.4 million for a new social media surveillance system. Iqra Asghar, “Boston Police Used Social Media Surveillance for Years Without Informing City Council,” American Civil Liberties Union, February 8, 2018, https://www.aclu.org/blog/privacy-technology/internet-privacy/boston-police-used-social-media-surveillance-years-without.

[174] “Clarkstown to Pay in Suit Involving Surveillance of Black Lives Matter Members,” *News 12 Westchester*, February 6, 2019, https://westchester.news12.com/clarkstown-to-pay-in-suit-involving-surveillance-of-black-lives-matter-members-39920785.

[175] The department turned these tactics against its political opponents as well, monitoring the social media profiles of the local Town Supervisor in order to gather information to use in order to oppose his proposed review and reform of the department. Brandon E. Patterson, “Exclusive: Internal Documents Show Police Spied on New York Black Lives Matter Group,” *Mother Jones,* October 19, 2017, https://www.motherjones.com/crime-justice/2017/10/police-spied-on-new-york-black-lives-matter-group-internal-police-documents-show/.

[176] Twitter executives also affirmed that the use of data products for surveillance purposes was strictly prohibited and that developers found violating these rules would be suspended from the platform. Lora Kolodny, “Facebook, Twitter Cut off Data Access for Geofeedia, a Social Media Surveillance Startup,” *TechCrunch*, October 11, 2016, https://social.techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/.

[177] “Developer Policies to Protect People’s Voices on Twitter,” Twitter, November 22, 2016, https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.

Yet subsequent reports show that companies have continued to use special access to Twitter's data to provide information on activists to U.S. law enforcement organizations, even if they have limited the means by which they do so.[178] For example, in 2020, Dataminr monitored protests across the country following the killing of George Floyd, and provided police departments across the country with social media content concerning the latest location and activities of demonstrators. On June 9, 2020, the FBI signed an agreement to extend its relationship with Dataminr, which provides the agency with the First Alert platform to deliver "breaking news alerts on emergency events, such as natural disasters, fires, explosions and shootings."[179]

5.2 Individualized Social Media Surveillance: Tracking and Deceiving Activists

While mass surveillance gathers data on public social media communications, law enforcement has resorted to deceptive techniques to monitor the private accounts of activists. In fact, although companies such as Facebook officially prohibit creating fake personas, the U.S. Department of Justice actively encourages law enforcement to use deceptive accounts, recommending that law enforcement organizations draft policies to ensure that such deception is utilized only for valid law enforcement purposes.[180] Unfortunately, such policies are often too ambiguous to be meaningful. For instance, the Georgia Bureau of Investigation's social media policy, cited as a model by the Department of Justice, allows agents to use online aliases to collect information for vaguely-defined purposes such as "the prevention of crime," without discussing what kinds of activities should or should not be considered suspect.[181]

The Supreme Court has long held that law enforcement does not need a warrant to gather evidence through a deceptive persona, and this precedent has typically been upheld in cases where law

[178] Sam Biddle, "Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr," *The Intercept*, July 9, 2020, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

[179] Lee Fang, "FBI Expands Ability to Collect Cell phone Location Data, Monitor Social Media, Recent Contracts Show," *The Intercept*, June 24, 2020, https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/.

[180] "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations," Bureau of Justice Assistance, February 2013, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_inves.pdf.

[181] Bureau of Justice Assistance, "Developing a Policy on the Use of Social Media in Intelligence" ibid., p. 32.

enforcement uses deceptive social media accounts.[182] Unfortunately, this opens the door to law enforcement surveilling individuals on the basis of their race, religion, or political activities.

For example, in 2013 Detective Bradley Landis, of the New Castle County Police Department in Delaware, sent a Facebook friend request to Terrance Everett through a fictitious Facebook account. Everett accepted, and Landis began to monitor him for reasons that are still unclear. Everett was a Black man who had previously been convicted of a felony for distributing cocaine and had faced a number of other charges, resulting in a few years in prison. But by 2013 he had been released from prison, was working legally, and there is little evidence that he was under suspicion of any specific crime. Nonetheless, in 2013 Everett posted a YouTube video entitled "Cop pulls black guy over for nothing and gets dissed," which showed Everett criticizing a police officer who had pulled him over for playing music too loudly.[183] Years later, Everett concluded that he was targeted for this video.

After friending Everett, Landis monitored his Facebook activity between one and three times a week, for more than two years. One morning in 2015, Everett spotted a photo posted by Everett's girlfriend which suggested that he might own a firearm—something illegal because of Everett's felony record. Within 24 hours, officers knocked down the door of Everett's apartment, threw a smoke bomb inside, detained Everett's girlfriend, and charged Everett with illegal possession of a firearm. Everett's girlfriend showed records that she had purchased the weapons, but she was accused of having given it to Everett. In 2018, Everett was sentenced to 15 years in prison.[184] Everett appealed, arguing that the use of his private Facebook post, available only to his friends, was a violation of his reasonable expectation to privacy. However, Delaware's Supreme Court ruled Everett did not have a reasonable expectation of privacy from those who he allowed into his friend network, including Detective Landis. [185]

Everett's case suggests that law enforcement can use deceptive social media accounts to surveil individuals without any probable cause—opening the door to racial, religious, and political

[182] Specifically, See, e.g., United States v. White, 401 U.S. 745, 752 (1971), discussion in Lisa Schmidt, "Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare," *Cornell Journal of Law and Public Policy* 22, no. 2 (January 1, 2012).
[183] The video remains available on YouTube at: https://www.youtube.com/watch?v=Y2FxmiCAPG0&ab_channel=RysheenBowers.
[184] Kashmir Hill, "The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook," *The Root*, October 23, 2018, https://www.theroot.com/the-wildly-unregulated-practice-of-undercover-cops-frie-1828731563.
[185] See Everett v. The State of Delaware, Supreme Court of the State of Delaware May 29, 2018, p. 8, available at: https://courts.delaware.gov/Opinions/Download.aspx?id=273550.

discrimination. Courts have sometimes found that the use of deceptive social media accounts violates reasonable expectations of privacy—particularly when the person being surveilled made substantial efforts to protect their privacy, or when state laws offer stronger privacy protections than federal laws.[186] But for the most part, courts have upheld this precedent by allowing warrantless surveillance through deceptive social media accounts.[187]

Just as private companies have provided software for mass surveillance, they have also helped with deception and targeted social media surveillance. For example, in 2014 an intelligence analyst at the Mall of America's security firm created a fake Facebook profile to befriend local activists. The activists planned a protest at the mall in response to grand jury decisions not to indict the police officers who, in two separate instances, killed Black men Michael Brown and Eric Garner.[188] The analyst compiled dossiers on at least ten activists, which were then sent to city officials. In December 2014, when thousands of activists peacefully protested at the Mall, managers concerned about losing holiday shoppers ordered the activists to leave. Law enforcement ultimately arrested

[186] For example, Detective Dana McNeil of the Bozeman, Montana police department created a fictitious Facebook account of a 16-year-old girl named "Tammy Andrews" to help him investigate crimes against minors. In 2013, while posing as "Tammy," McNeil received a message from William Windham through Facebook Messenger, and established a conversation. Windham went on to request nude photos of Tammy, and McNeil and Windham later began exchanging messages through their cell phones. Eventually McNeil arranged a meeting between "Tammy" and McNeil at the local high school. When Windham appeared for the meeting, he was arrested. However, the Montana Judicial District Court ruled that Windham's conversations with "Tammy" could not be used against him because he had a reasonable expectation of privacy. The court stressed that Windham had adopted the most private possible Facebook settings and tended to only friend people whom he knew well. Thus, the court ruled that Windham had a reasonable expectation of privacy and that his communications with McNeil could not be used against him. See: Larry Bodine, "Montana Judge Rules Warrant Required for Social Media Profiles," *The National Trial Lawyers*, March 6, 2015, https://thenationaltriallawyers.org/2015/03/montana-judge-rules-warrant-required-for-social-media-profiles/.
The contrast between the rulings in Delaware and Montana suggests that courts in different states may adopt different standards of what exactly a "reasonable expectation" of privacy is. In fact, the Montana court also invoked a provision of the Montana Constitution upholding individuals' right to privacy, as well as previous findings by the Montana Supreme Court that "the range of warrantless searches which may be lawfully conducted under the Montana Constitution is narrower than the corresponding range of searches that may be lawfully conducted pursuant to the federal Fourth Amendment," see p. 10 of the ruling, available at: https://www.scribd.com/doc/255331745/Montana-v-Windham-Opinion-and-Order-Hon-John-Brown-District-Court-Gallatin-County.
For critique see Orin S. Kerr, "Undercover Facebook Investigations and the Federal/State Divide — a Response to David Post," *Washington Post*, February 11, 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/02/11/undercover-facebook-investigations-and-the-federalstate-divide-a-response-to-david-post/.

[187] M. Jackson Jones, "Shady Trick or Legitimate Tactic - Can Law Enforcement Officials Use Fictitious Social Media Accounts to Interact with Suspects," *American Journal of Trial Advocacy* 40, no. 1 (2017 2016): 69–82.

[188] Lee Fang, "Mall of America Security Catfished Black Lives Matter Activists, Documents Show," *The Intercept*, March 18, 2015, https://theintercept.com/2015/03/18/mall-americas-intelligence-analyst-catfished-black-lives-matter-activists-collect-information/.

25 people for trespassing, and the mall and the city charged eleven people for misdemeanors.[189] At the same time, officials with the FBI's Counterterrorism Task Force also passed on information gathered by a "confidential human source" on Facebook to Bloomington police officers about the time and location of the protest.[190]

The Memphis case described above similarly suggests how law enforcement can use deceptive social media accounts to surveil activists. Because political movements today often need to use social media to grow their network and organize public protest, activists are at special risk of targeting by deceptive social media accounts. Public controversy over such cases has led Facebook to remind police that it officially prohibits the use of false accounts.[191] Facebook also tries to root out fake accounts through machine learning algorithms and identification requirements.[192] But it is unclear whether this has had any impact on law enforcement uses of social media.

5.3 Geofencing

As noted previously in the cases of Baltimore and Memphis, law enforcement has used the services of companies such as Geofeedia, which track social media postings from devices in a particular region, to monitor protests and demonstrations. Such tracking was originally developed to target advertising to people near certain businesses, and social media users often grant companies permission to track and share their location without realizing that they are doing so.[193] Because

[189] Libby Nelson, "The Mall of America Wants to Stop a Black Lives Matter Protest with a Restraining Order," *Vox*, December 22, 2015, https://www.vox.com/2015/12/22/10651676/mall-of-america-black-lives-matter. Although the Mall was partly financed with public money, it is private property.

[190] Lee Fang, "Why Was an FBI Joint Terrorism Task Force Tracking a Black Lives Matter Protest?" *The Intercept*, March 12, 2015, https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/.

[191] See, e.g., "Facebook Letter to Memphis Police Department on Fake Accounts," *Electronic Frontier Foundation*, September 19, 2018, https://www.eff.org/document/facebook-letter-memphis-police-department-fake-accounts.

[192] "Facebook Help Center: What Types of ID Does Facebook Accept?" *Facebook*, https://www.facebook.com/help/159096464162185?helpref=faq_content, accessed December 10, 2021.

[193] For a brief history of location-based marketing, see James Ewen, "The Evolution Of Location Based Marketing & Advertising," *Tamoco*, January 23, 2018, https://www.tamoco.com/blog/location-based-marketing-history/. For a discussion of the difficulty of stopping tracking, see Zak Doffman, "Facebook Tracks Your IPhone Location—This Is How To Stop It," *Forbes*, May 22, 2021, https://www.forbes.com/sites/zakdoffman/2021/05/22/apple-user-warning-how-to-stop-facebook-secretly-tracking-your-iphone-ipad/.

such permission is implicitly granted by users, law enforcement does not need a warrant to gather location information from companies (see discussion of third party doctrine above).[194]

In 2018 the Supreme Court ruled that law enforcement must obtain a warrant to obtain geolocation data held by cell phone providers, arguing that such data is not consensually shared with service providers—which track location as part of their normal operations—and cell phones are "indispensable to participation in modern society."[195] However, such warrants are not difficult to obtain. In fact, "geofence warrants" are commonly used to gather information from companies like Google that gather location data for targeted advertising, but might not otherwise analyze and market that information to law enforcement. While traditional warrants permit searches of *known* suspects, geofence warrants are issued specifically in instances where a suspect cannot be identified. Law enforcement organizations specify a region and period of time; with court approval, they then demand that companies provide a list of all phones that passed through that region during that time.[196]

The number of geofence warrants issued to Google has proliferated, increasing by more than 1500% between 2017 and 2018 and another 500% the following year.[197] Geofence warrants are frequently directed at Google because it collects and stores vast troves of geolocation data on its billions of users who have their "location history" turned on. Between January and June of 2020 alone, Google

[194] For a review of law on location tracking, see Lisa Schmidt, "Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare," *Cornell Journal of Law and Public Policy* 22, no. 2 (January 1, 2012), https://scholarship.law.cornell.edu/cjlpp/vol22/iss2/7.

[195] Carpenter vs. the United States (2017) challenged the FBI's use of geolocation data from cell phone data to build a case against people suspected of armed robberies. In 2011, the FBI arrested four suspects in a series of armed robberies of electronics stores. One of them confessed and gave the FBI cell phone numbers of fifteen others that he stated had been involved in the robberies. The FBI requested a court order (known as a 2703(d) order), to gather time-stamped location data from the suspects' the cell phone providers. Under the Stored Communications Act, law enforcement can obtain a 2703(d) order to access electronic records by demonstrating "reasonable grounds" for its belief that the records are "relevant and material to an ongoing investigation." This evidentiary standard is less stringent than the "probable cause" necessary to obtain a warrant. The FBI was granted the 2703(d) order, and obtained cell phone location information that showed that two suspects, Timothy Carpenter and Timothy Sanders, were within half a mile to two miles of each robbery. Carpenter asked to suppress this evidence on the grounds that it had been obtained without a warrant, and therefore violated his Fourth Amendment rights. See p. 3: Carpenter v. The United States (Supreme Court October 2017), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

[196] "Geofence Warrants and the Fourth Amendment," *Harvard Law Review* 134, no. 2508 (May 10, 2021), https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/.

[197] "Geofence Warrants and the Fourth Amendment," *Harvard Law Review,* ibid.

received over 19,000 warrants, 83% of which led to the disclosure of account data to law enforcement organizations.[198]

Google has attempted to preserve user privacy by creating a three-step process for responding to geofence warrants.[199] First, the company searches its entire location history database to produce an anonymous list of accounts that were present in a region, along with a track showing approximate location and time stamps of each account. Second, law enforcement identifies tracks they are interested in investigating further and may request additional information to follow those tracks over a larger area or time. Third, Google provides identifying information for specific accounts, such as the full name and email addresses of the users.[200]

Despite Google's efforts to protect user privacy, geofence warrants can sweep a large number of people into a dragnet of suspicion. In the context of racial justice demonstrations, all protesters may become suspects. For example, after protests against the murder of George Floyd in May 2020, Minneapolis police attempted to identify the person who smashed the windows of an AutoZone shop, who was suspected of belonging to a White supremacist organization. The geofence warrant issued to Google nonetheless returned information for all bystanders, most of whom had no connection to the incident.[201]

The large number of accounts swept up in such warrants increases the risk that individuals are erroneously suspected of crimes—and such suspicion can be very costly. For example, Jorge Molina was jailed for six days after police claimed that his phone proved that he was at the scene of a murder in Arizona.[202] In fact, data placed Molina in multiple locations simultaneously, because he had multiple devices simultaneously logged in to his account, and multiple witnesses confirmed that he was elsewhere at the time of the murder. Suspicion slowly shifted towards Molina's stepfather, Marcos Gaeta, who often used Molina's car and phone; Molina's mother and sister

[198] These figures come from Google's transparency report, available at: https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0.

[199] "Geofence Warrants and the Fourth Amendment," *Harvard Law Review (*footnote 196).

[200] Sean Broderick, "Google Data and Geofence Warrant Process," *nlsblog.org*, January 9, 2021, https://nlsblog.org/2021/01/08/google-data-and-geofence-warrant-process/.

[201] Zach Whittaker, "Minneapolis Police Tapped Google to Identify George Floyd Protesters," *TechCrunch*, February 6, 2021, https://social.techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/.

[202] Jennifer Valentino-DeVries, "Tracking Phones, Google Is a Dragnet for the Police," *The New York Times*, April 13, 2019, https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html, https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

described Gatea as “abusive,” noting that he carried a gun everywhere. Nonetheless, Molina’s time in jail and damage to his reputation caused him to lose his job and drop out of college, while traumatizing him.[203]

Civil liberties groups have objected to the use of geofence warrants, and federal judges have not always granted them.[204] Some policymakers have proposed legislation to limit the use of geofence warrants, arguing that they violate the U.S. Constitution.[205] Nonetheless, warrants are commonly used and raise concerns about surveillance of racial justice and other activists.

5.4 Social Media Surveillance and the Escalation of Violence

The methods described above—including monitoring of social media and gathering data more directly from cell phones—do not necessarily produce more reliable intelligence. In fact, because data analytics companies have a vested interest in amplifying threats, and social media algorithms tend to amplify extreme postings, social media surveillance can readily encourage police to respond to peaceful protests with disproportionate force and escalate violence.

This finding contrasts with the “case studies” that data analytics companies market to law enforcement. For example, Geofeedia claims that it helped Baltimore police reduce violence associated with demonstrations following the death of Freddie Gray in 2015. Specifically, Geofeedia alerted the police to “rioters…targeting police vehicles and posting photos of burning police cruisers on social media,” as well as conversations between high school students planning to leave class and attend protests at Mondawmin Mall on April 17, 2015.[206] This allowed the officers

[203] Meg O’Connor, “Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder,” *Phoenix New Times*, January 16, 2020, https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374.

[204] Jennifer Lynch and Nathaniel Sobel, “New Federal Court Rulings Find Geofence Warrants Unconstitutional,” Electronic Frontier Foundation, August 31, 2020, https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0. Donna Lee Elm, “Geofence Warrants: Challenging Digital Dragnets,” *Criminal Justice* 35, no. 2 (2020): 7–13.

[205] For example, policymakers in the New York State Assembly introduced the Reverse Location Search Prohibition Act in both 2020 and 2021, which would prohibit police departments from issuing warrants based solely on geolocation data or keyword searches on social media. As of October 2021, the Bill has been referred to the Committee on Codes, but does not appear to be advancing. See: https://legiscan.com/NY/text/A00084/2021.

[206] Matt Cagle, “Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color,” ACLU of Northern California, October 11, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target. The ACLU has made the Geofeedia case study available at: http://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

to arrive in a large group and stop the students, "some of whom had already hijacked a bus...and found their backpacks full of rocks, bottles and fence posts."[207] Geofeedia quotes a Baltimore detective who claims its alerts "allowed us to protect our people." [208]

But other sources suggest that the people arriving at the mall were largely peaceful, and that the police contributed to escalating violence through an overly militarized response to unreliable information on social media. On April 17, students at the high school had become anxious about a flyer circulating on social media calling for a "purge"—referring to a 2013 film in which crimes are legal for one night—later that day at the mall.[209] The school notified the city police, which issued a statement about "credible information that members of various gangs…have entered into a partnership to 'take-out' law enforcement officers."[210] Officers soon dispatched in full riot gear to the area around the mall, shutting down the local subway station, stopping buses, and forcing riders to disembark. Police corralled hundreds of students, many of whom were simply traveling home from school. While most protesters were peaceful, eventually some began throwing bottles and rocks. One Baltimore teacher recounted: "The riot police were already at the bus stop on the other side of the mall, turning buses that transport the students away, not allowing students to board.… Those kids were set up, they were treated like criminals before the first brick was thrown."[211] The violence escalated, leading to looting at the mall and unrest in other parts of the city.

Contrary to Geofeedia's marketing case study, even some police officers believed that the situation had been handled poorly, and that police should have coordinated better with the school and students.[212] While the police seem to have learned about the "purge" meme independently of Geofeedia, the company encouraged police to treat it as a credible threat. Yet the originator of the "purge" post was never publicly identified, suggesting that it may have been yet another example

[207] Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product," ibid.
[208] Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product," ibid.
[209] Kevin Rector, "What Happened at Mondawmin? Newly Obtained Documents Shed Light on Start of Baltimore Riot," *Baltimore Sun*, April 20, 2019, https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-new-baltimore-riot-documents-20190416-story.html.
[210] Jenna McLaughlin and Sam Brodey, "Eyewitnesses: The Baltimore Riots Didn't Start the Way You Think," *Mother Jones* (blog), April 28, 2015, https://www.motherjones.com/politics/2015/04/how-baltimore-riots-began-mondawmin-purge/. The documents pertaining to the incident released by the BPD are available at https://www.scribd.com/doc/263262264/Credible-Threat.
[211] McLaughlin and Brodey, "Eyewitnesses: The Baltimore Riots Didn't Start the Way You Think," ibid.
[212] Rector, "What Happened at Mondawmin?" (footnote 209).

of the misinformation that pervades social media. It is also unclear how the police determined that there was a "credible" threat of gang violence; a DHS intelligence analyst assessed this as "non-credible" within hours of the alert.[213]

As this suggests, reliance on social media for threat intelligence can sometimes contribute to an overreaction that escalates tensions. In another example, police planned a major operation against protests planned for the Mott Haven neighborhood of the Bronx on June 4, 2020, largely because they saw a social media call for the protest that included images of police vehicles engulfed in flames and a person punching a police officer.[214] However, activists were demonstrating completely peacefully when—shortly before an 8 PM curfew—they were suddenly surrounded by over 100 police officers who pushed, pepper sprayed, and arrested them. Not only did police make it impossible for activists to leave in compliance with the curfew, but they injured many who had been entirely peaceful.[215] The New York City Department of Investigation later highlighted the Mott Haven action as an example of the police force acting on intelligence without sufficient consideration of context or proportionality.[216]

In short, social media does not necessarily lead to reliable intelligence. Indeed, research shows that false stories spread six times faster than true stories on social media because people are drawn to the surprising nature of falsehoods.[217] Policymakers are increasingly concerned that social media amplifies extremism, but empirical research reveals a more nuanced picture, in which extreme

[213] Jason Leopold, "Fearing a 'Catastrophic Incident,' 400 Federal Officers Descended on the Baltimore Protests," *Vice News*, June 24, 2015, https://www.vice.com/en/article/8x393b/fearing-a-catastrophic-incident-400-federal-officers-descended-on-the-baltimore-protests.

[214] The police rationale for the operation is described in "Investigation into NYPD Response to the George Floyd Protests," New York City Department of Investigation, December 2020, p. 54, available at: https://www1.nyc.gov/assets/doi/reports/pdf/2020/DOIRpt.NYPD%20Reponse.%20GeorgeFloyd%20Protests.12.18.2020.pdf. While the report claims that the police were also responding to arrests of individuals carrying weapons in the hours before the demonstration, reports show that the relationship between them and the protest was tenuous at best: Craig McCarthy, "NYPD Commissioner Dermot Shea Ignores His Own 'Misinformation' Warnings," *New York Post*, June 8, 2020, https://nypost.com/2020/06/08/nypd-commissioner-ignores-his-own-misinformation-warnings/.

[215] Jami Floyd, "24 Minutes In Mott Haven," *Gothamist* (blog), June 4, 2021, https://gothamist.com/news/24-minutes-mott-haven; "'Kettling' Protesters in the Bronx: Systemic Police Brutality and Its Costs in the United States," Human Rights Watch, September 30, 2020, https://www.hrw.org/report/2020/09/30/kettling-protesters-bronx/systemic-police-brutality-and-its-costs-united-states.

[216] "Investigation into NYPD Response to the George Floyd Protests," (footnote 214), p. 49.

[217] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

messages may be amplified without necessarily reshaping user opinions or behavior.[218] As a result, social media may exaggerate the apparent threat of extremism, and thereby encourage overly aggressive policing.

6. Surveillance Cameras

Camera infrastructure has widely been promoted as a means of establishing the ground truth about how law enforcement interacts with minorities and other members of the public. For example, both police and activists have advocated that officers wear cameras to help establish the "facts" when police are accused of using excessive force. Activists have advocated using mobile phone cameras to document their interactions with law enforcement and to raise awareness about instances of abuse. Video footage has played a prominent role not only in raising awareness of and protest against racial violence, but also in prominent trials, such as the convictions of the officer who murdered George Floyd and the three men who murdered Ahmaud Arbery. One sociologist commenting on the Arbery case declared that "Video is an objective observer."[219]

And yet a closer look suggests that the role of camera footage is more complex. Consider, for example, that the video used in the Arbery case was provided by one of the murderers, who believed it would exonerate him. As this suggests, what people see in video footage is shaped by background assumptions which are not "color blind."[220] Furthermore, footage of the same events may be rendered very differently from different physical perspectives. The persuasiveness of videos is shaped not only by the raw footage, but by common beliefs about the apparent objectivity of camera

[218] Pablo Barberá, "Social Media, Echo Chambers, and Political Polarization," in *Social Media and Democracy: The State of the Field, Prospects for Reform*, ed. Joshua A. Tucker and Nathaniel Persily, SSRC Anxieties of Democracy (Cambridge University Press, 2020), 34–55. Available at: http://pablobarbera.com/static/echo-chambers.pdf.

[219] Meryl Kornfield, "How a shaky cellphone video changed the course of the Ahmaud Arbery murder case," *Washington Post*, November 24 2021, https://www.washingtonpost.com/nation/2021/11/24/arbery-video-conviction/.

[220] Charles Goodwin, "Professional Vision," *American Anthropologist* 96, no. 3 (1994), http://www.jstor.org/stable/pdfplus/682303.pdf. For more recent analysis of lay perspectives on video footage, see Michael Lynch, "Vernacular Visions of Viral Videos: Speaking for Evidence that Speaks for Itself," in *Legal Rules in Practice: In the Midst of Law's Life*, ed. J. Colemans B. Dupret, and M. Travers (Abington and New York: Routledge, 2021).

technology, and the ways that images are incorporated into social media and other information infrastructures.[221]

In this section we examine at least three factors that shape the potential for cameras to mitigate or amplify racial inequality. First, decisions about how and where to deploy cameras can encourage suspicion of particular groups. Police departments commonly use multiple types of surveillance cameras, including mobile cameras to monitor special events, license plate readers, and stationary cameras. Police departments combine multiple approaches when choosing where to place stationary cameras, including past reporting on crime ("data-driven" placement), concerns about particular high-risk targets for attack (for example monuments or commerce hubs), and community input and requests.[222] Each of these approaches can potentially amplify structural inequalities, but in different ways.

Data-driven placement strategies allocate more cameras to regions that have been statistically identified as crime "hot-spots." Advocates of data-driven placement argue that it deters crime where it is most likely to occur, while providing a more objective and efficient means of choosing where to focus police resources. However, as noted above, critics highlight that reliance on past data produced by police is likely to amplify patterns of discriminatory policing.

Police departments also place cameras around areas that they regard as being at high risk of terrorist or related attacks. In fact, the federal government encourages such placement through grant programs, such as the Port Security Grant Program offered by the Federal Emergency Management Agency.[223] While the focus on high-profile areas may be a sensible allocation of scarce resources, it can also enable surveillance of constitutionally protected activities that tend to take place near major public venues. For example, as discussed further below, national monuments around Washington, D.C. are significant sites for lawful demonstrations but are also heavily surveilled by both federal and local agencies.

[221] Rune Saugmann, "The security captor, captured. Digital cameras, visual politics and material semiotics," *Critical Studies on Security* 8, no. 2 (2020/05/03 2020), https://doi.org/10.1080/21624887.2020.1815479.

[222] Examples of these approaches are described below, and also in Nancy La Vigne et al., "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," Urban Institute, September 19, 2011, https://www.researchgate.net/publication/280089845_Evaluating_the_Use_of_Public_Surveillance_Cameras_for_Crime_Control_and_Prevention.

[223] "Port Security Grant Program | FEMA.Gov," Federal Emergency Management Agency, https://www.fema.gov/grants/preparedness/port-security, accessed December 10, 2021.

Finally, camera placement can be shaped by citizens. For example, some city councils are actively involved in authorizing placements, and invite input from local citizens. Additionally, some police departments allow citizens to donate cameras for police monitoring and give grants or rebates to citizens wishing to deploy cameras that will be of service to the police. While such citizen participation must be regarded as positive, some neighborhoods are better able to pay for camera placement and thereby gain more influence than others, as discussed further below in the case of Memphis.

A second major issue concerns how camera footage is monitored, stored, and used. Since police departments can typically deploy far more cameras than they have personnel to actively monitor them, decisions must be made about what to monitor and when—and these decisions can readily amplify structural inequalities. Large amounts of camera footage are typically stored for potential investigations, raising questions about how long data should be retained and the potential for illegitimate appropriations of stored data.[224] Police departments commonly establish regulations designed to prevent discrimination and protect privacy, including prohibitions on racial targeting and restrictions on the length of time that data may be stored. However, as discussed further below, routine enforcement of such regulations typically falls to the police themselves, reducing prospects of accountability and allowing significant abuses. Some scholars have argued that policies restricting how long bodycam footage is retained and how it may be used for discipline pose obstacles to police accountability.[225]

A third issue concerns the potential for cameras to reduce crime, either by police or everyday citizens. Research shows mixed results on the effectiveness of camera surveillance in reducing crime, in part because of measurement difficulties.[226] For example, cameras are typically deployed

[224] Several public interest groups have recommended guidelines to prevent misuse, which include deleting video footage after a specified period of time to prevent potential use, e.g., Nancy La Vigne et al., "Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners" (Urban Institute, September 2011), https://www.urban.org/sites/default/files/publication/27551/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide-for-Law-Enforcement-and-Their-Municipal-Partners.PDF; "CCTV: Developing Privacy Best Practices," Department of Homeland Security Privacy Office Public Workshop, 2006, https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf; "Guidelines for Public Video Surveillance," The Constitution Project, 2006, https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf.

[225] Mary D. Fan, "Body Cameras, Big Data, and Police Accountability," *Law & Social Inquiry* 43, no. 4 (2018), https://doi.org/https://doi.org/10.1111/lsi.12354, https://onlinelibrary.wiley.com/doi/abs/10.1111/lsi.12354.

[226] Gustav Alexandrie, "Surveillance Cameras and Crime: A Review of Randomized and Natural Experiments," *Journal of Scandinavian Studies in Criminology and Crime Prevention* 18, no. 2 (July 3, 2017): 210–22, https://doi.org/10.1080/14043858.2017.1387410.

after a spike in crime; if crime drops after deployment, it is unclear whether the drop was caused by cameras or simply a return to "normal" levels of crime. A review of seven high-quality studies that attempted to account for such difficulties finds that cameras reduced crime up to 28% on city streets but had no effect on parking facilities or subways.[227] However, it is difficult to generalize from such a limited number of studies; the cases discussed below show mixed results, with apparent reductions in some cities but not others.

In principle, surveillance cameras can also increase police accountability, as independent citizens have done with cell phone cameras and other recording devices. While these tools have been used effectively in a few high-profile cases, accountability has often proven difficult because police have tremendous control over surveillance networks. Statistical studies of the effects of police body-worn cameras show little, no, or uncertain effects on police accountability.[228] This is partly because such cameras show officers' perspectives and are easily aimed away from views of police brutality or evidence of civilians' innocence.

In what follows, we illustrate the potential for surveillance camera networks to alternately reinforce or challenge structural racism using evidence from three cities: Memphis, Baltimore, and Washington, D.C. these cases demonstrate that reducing crime and holding police accountable requires more than deploying new technology; it also requires giving everyday citizens meaningful control over how those technologies are used.

6.1 Surveillance cameras in Memphis, Tennessee

As noted in the opening case study, the Memphis Police Department turned to data-driven policing in the late 1990s, and this shaped its camera deployment strategy. For example, precinct colonels commonly assigned mobile camera units to high-traffic areas or places that had been identified as crime "hot spots."[229] The police department also deployed cameras based on perceptions of high-risk targets, for example by placing cameras along the Mississippi River, with funding from a Port

[227] Alexandrie, "Surveillance Cameras and Crime: A Review of Randomized and Natural Experiments," ibid.

[228] Jennifer Lee, "Will Body Cameras Help End Police Violence?," ACLU of Washington, June 7, 2021, https://www.aclu-wa.org/story/%C2%A0will-body-cameras-help-end-police-violence%C2%A0.

[229] James Helms, Angela Madden, and Maura Joyner, "Assessment of Data-Driven Deployment by the Memphis Police Department," University of Memphis Public Safety Institute, 2018, p. 7, available at: https://www.memphis.edu/psi/pdfs/2018assessment.pdf.

Security Grant.[230] But perhaps the most interesting feature of surveillance camera placement in Memphis is the private donation program: between 2016 and 2020, neighborhoods, citizens, and businesses were invited to make private donations to the police department for purchasing and installing cameras that were integrated with the Real Time Crime Center.[231]

The private donation program started after the affluent Belle Meade neighborhood grew concerned about a rash of burglaries in 2015.[232] The neighborhood raised $131,970 to purchase cameras and license plate readers; these were donated to the Memphis Police Department for continual surveillance at nine entrance points to the neighborhood.[233] Two additional affluent neighborhoods soon followed suit.[234]

City Council members were immediately concerned that lower-income areas might not be able to raise the funds to place the cameras in their chosen areas. So not long after approving the deployment around Belle Meade, they also approved $400,000 for a new "Neighborhood Sentinel Program," which gave each of seven city council districts ten cameras for placement in their areas. The Memphis Police Department sent the councils data on crime "hot spots" in their areas, and the councils then chose where to place cameras.[235] While this program was intended to level the playing field, the use of crime statistics provided directly by the police department effectively encouraged a "data-driven" model of deployment in less wealthy neighborhoods.

As of 2018, camera placements in Memphis were heavily concentrated in downtown and tourist areas, with additional cameras distributed around the perimeters of wealthy neighborhoods like Belle Meade.[236] It might seem that the concentration of cameras around wealthy neighborhoods

[230] Blanchard et al. v. City of Memphis, Joseph Patty deposition (April 26, 2018), p. 11-12, available at: https://www.aclu-tn.org/wp-content/uploads/2018/07/5-Depositions_Redacted.pdf.

[231] Bianca Phillips, "Residents Can Get 'SkyCop'-Style Cameras for Their Neighborhoods," *MemphisFlyer*, July 7, 2016, https://www.memphisflyer.com/residents-can-get-skycop-style-cameras-for-their-neighborhoods.

[232] Brad Broders, "Neighborhood To Pay For Own SkyCop Cameras," *ABC 24 Memphis*, February 5, 2016, https://www.localmemphis.com/article/news/neighborhood-to-pay-for-own-skycop-cameras/522-9396707c-8b7e-447f-9ced-cd78d6d6bcb6.

[233] Ryan Poe, "Memphis Eyeing 70 More SkyCop Cameras in City," *Memphis Commercial Appeal*, April 4, 2016, http://www.commercialappeal.com/news/government/city/memphis-eyeing-70-more-skycop-cameras-in-city-2fab4eab-6e13-49f6-e053-0100007fed84-374511371.html.

[234] Michelle Corbett, "East Memphis Neighborhoods Raise Money for Memphis Police Department Surveillance," *Memphis Business Journal*, February 26, 2016, https://www.bizjournals.com/memphis/news/2016/02/26/two-more-east-memphis-neighborhoods-write-checks.html.

[235] Helms, Madden, and Joyner, "Assessment of Data-Driven Deployment by the Memphis Police Department," (footnote 229).

[236] Compare Google Maps with images on p. 184 of Simone Tulumello, "Neoliberalisation of Security, Austerity and the 'End of Public Policy': Governing Crime in Memphis (TN, USA) Through Predictive Policing, Community,

runs counter to the dominant concern about data-driven surveillance: that it exacerbates over-policing of poor and minority communities. However, it is significant that Belle Meade chose to site cameras at nine entry points to the neighborhood—not within the community. This placement presumes that criminal activity originates outside of the neighborhood and encourages police to focus surveillance on individuals who do not fit the typical profile of a Belle Meade resident—a relatively affluent White person.

It is worth noting that even wealthy neighborhoods do not have complete discretion about how and where cameras are operated. In 2016, a Memphis Police Department spokesperson noted that once donated, "cameras could be moved at the discretion of the director of Police Services; however, that has never happened in the past."[237] Law enforcement thus continues to have almost total control over the development and use of surveillance camera networks.

6.2 Surveillance cameras in Washington, D.C.

As the U.S. Capitol, Washington, D.C. has long been surveilled not only by city authorities, but also by federal agencies such as the National Park Police, which deploys surveillance cameras around national monuments. Even before the terrorist attacks of September 11, 2001, the city began deploying closed circuit television (CCTV) camera networks under the control of at least two distinct agencies—the Metropolitan Police Department, and the Washington, D.C. Homeland Security and Emergency Management Agency. These networks expanded dramatically after the attacks.[238] Between 2001 and the fall of 2008 the Homeland Security and Emergency Management Agency tripled the number of cameras to a total of roughly 5,600.[239] Some cameras were monitored by security guards within buildings associated with the cameras, while others were monitored by agency staff in centralized locations; in 2008 the agency was working to integrate these various

Grants and Police 'Mission Creep,'" *ACME: An International Journal for Critical Geographies* 17, no. 1 (February 28, 2018): 171–200. https://www.acme-journal.org/index.php/acme/article/view/1537.

[237] Corbett, "East Memphis Neighborhoods Raise Money for Memphis Police Department Surveillance," (footnote 234).

[238] "MPDC's Closed Circuit Television (CCTV) System," Metropolitan Police Department, https://mpdc.dc.gov/page/mpdcs-closed-circuit-television-cctv-system, accessed December 10, 2021.

[239] Mary Beth Sheridan, "D.C. Forging Surveillance Network," *NBC*, May 1, 2008, https://www.nbcnews.com/id/wbna24400482.

elements into a unified camera network, but met resistance from civil libertarians concerned about expanding surveillance.[240]

The Metropolitan Police Department developed a much smaller network of cameras that was integrated into a Joint Operations Command Center launched in September 2001. While the launch was planned for the World Bank Annual Meetings of late September 2001, the system saw early use during the September 11 terrorist attacks and continued to quickly expand—from just two cameras in April 2000, to fourteen by 2003. Cameras were mounted around national monuments and other strategic locations for monitoring during demonstrations or terrorism alerts. Cameras were turned off when not used for these purposes. While relatively small in number, the cameras were sophisticated, with the ability to pan, tilt, and zoom.[241]

The police department was eager to deploy a more substantial camera network to fight crime in neighborhoods, but initially failed to gain funding from the City Council. That changed after fourteen homicides in the first eleven days of July 2006 prompted the Police Chief and Mayor to declare a "crime emergency" that gave the police wide latitude to adopt new crime reduction strategies, including the deployment of surveillance cameras. By June 2007, the police department had deployed a network of seventy-three surveillance cameras, and active monitoring began in the fall.

While perceptions of "emergency" increased public support for surveillance cameras, the rushed deployment of cameras also raised concerns about accountability and potential misuse. In 2002, the Washington, D.C. city council required the police department to create regulations subject to approval by the city council. Initial approval was granted in November 2002; efforts to revise these guidelines in 2006 were rejected.[242]

[240] La Vigne et al., "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," (footnote 222); also Sheridan, "D.C. Forging Surveillance Network" (footnote 239).

[241] For discussion of the origins and early capabilities of the Park Police network, see "Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C." (United States Government Accountability Office, 2003), https://www.gao.gov/products/gao-03-748.

[242] "Regulations for Use of Video Surveillance by Metropolitan Police Department," Code of the District of Columbia, https://code.dccouncil.us/us/dc/council/code/sections/5-133.19, accessed December 10, 2021. It appears that additional guidelines were passed in 2008 to govern the Homeland Security and Emergency Preparedness Agency's surveillance cameras; see "Rules for Use of Surveillance Cameras," Code of the District of Columbia, https://code.dccouncil.us/us/dc/council/code/sections/7-2231.10, accessed December 10, 2021. These rules did not

Unlike cameras deployed by the Park Police, many of which were deliberately hidden and which were relatively unregulated, the Metropolitan Police Department cameras in the initial installation were highly visible, with flashing blue lights. The police department also lists locations on its website.[243] At any given time, the Metropolitan Police Department are only able to monitor a fraction of the cameras; as of 2011, only 23 cameras were connected to the joint operations center through live feeds, and the department could only display 16 at a time.[244]

Monitoring practices by the Metropolitan Police Department are also regulated. Only public spaces may be surveilled, and camera monitors are not permitted to focus the cameras on posters publicizing protests or other constitutionally-protected activities. Cameras may not be trained on individuals on the basis of their race, gender, sexual orientation, disability, or other distinguishing characteristics. All active monitors must be sworn police officers, and sign a statement acknowledging the privacy rights of citizens. Footage from surveillance cameras can only be accessed if a sworn officer is present, and recordings from cameras are stored for 90 days unless requested for use as evidence or a training material.[245] However, since most of these regulations are managed internally rather than by a body external to the police department, it is unclear if camera monitors are actually held to the standards outlined.

While initial camera placements focused on what were considered to be high-risk targets for terrorist attacks, subsequent installations followed a more “data-driven” approach, using past police reports to identify crime “hot spots”; after gathering additional input from district commanders, neighborhood councils, and citizens, the department makes recommendations for camera placements to the city council. The city council approves certain areas for camera installation, but the Chief of Police ultimately decides where all cameras should be placed within those areas.[246]

allow the agency to use the police department’s cameras, but granted the police department right of access to the agency’s cameras.

[243] These different strategies for visibility are discussed in United States Government Accountability Office, “Video Surveillance,” (footnote 241), p 4; on the police department making their cameras highly visible, see La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 74.

[244] See discussion in La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 73-75.

[245] For discussion of regulations on the police department surveillance, see La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 76.

[246] La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 75.

The resulting pattern of surveillance camera placement has come to be heavily focused on predominantly non-White neighborhoods. As of October 2020, the police department operated a total 264 cameras across the District of Columbia; the average majority White area was allocated fewer than three surveillance cameras, while the average majority non-White area was allocated more than seven.[247] Additionally, the areas with the highest camera densities—Washington's Congress Heights, Bellevue, and Washington Highlands—includes neighborhoods that are over 95% Black and that house some of the most impoverished populations in Washington, D.C.[248]

Finally, the Metropolitan Police Department's surveillance capabilities extend beyond the cameras it owns. Washington, D.C. also launched a video rebate program in 2016, wherein individuals or organizations could receive rebates for video cameras that they purchased, installed outside a building, and registered with the police.[249] By 2019, roughly 17,000 such cameras had been deployed; while the police do not have live access to the footage, they can request it for investigative purposes.[250]

6.3 Surveillance cameras in Baltimore

Baltimore's camera surveillance network was initiated by 1996, when rising crime rates spurred the city to install sixteen cameras outside the downtown Lexington Market, which were then monitored by police officers at street kiosks.[251] In 2005, the city launched the CitiWatch camera network with funding from the Department of Homeland Security, and within two years the network expanded to include 400 closed circuit television cameras (CCTVs) deployed throughout the downtown area as well as local neighborhoods that were regarded as crime "hot spots."[252] By 2011, the network

[247] These numbers were published in Gracie Todd, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore, CNS Finds," *Capital News Service Maryland*, November 19, 2020, https://cnsmaryland.org/2020/11/19/police-cameras-disproportionately-surveil-nonwhite-areas-of-dc-and-baltimore-cns-finds/.

[248] Todd, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore, CNS Finds," ibid.

[249] Christina Sturdivant, "New Program Gives Rebates To People Who Install Private Cameras," *DCist*, February 18, 2016, https://dcist.com/story/16/02/18/post-70/.

[250] Sheridan, "D.C. Forging Surveillance Network," (footnote 239).

[251] La Vigne et al., "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," (footnote 222). See also: J. Cavanaugh Simpson and Ron Cassie, "Underwatch: The Police Spy Plane Experiment Is Over, but the Growing Surveillance of Baltimore Continues," *Baltimore Magazine*, March 23, 2021, https://www.baltimoremagazine.com/section/historypolitics/under-watch-police-spy-plane-experiment-over-but-growing-surveillance-baltimore-continues/.

[252] Simpson and Cassie, "Spy Plane Experiment Is Over, But Growing Surveillance of Baltimore Continues," ibid.

included over five hundred cameras and a centralized control room to enable 24/7 live monitoring.[253] By 2013, CitiWatch had expanded to include over 1,000 cameras operated by more than fifty city, state, federal, and non-governmental organizations, as well as private citizens.[254] Personnel in different agencies could each access footage from the others, but did not control the cameras owned by other organizations.[255] By 2020, the Baltimore Police Department alone controlled almost 780 cameras.[256]

This vast camera network was too large to actively monitor every moment of the day. Police department monitoring followed two different strategies: each district set its own monitoring schedule for cameras within its region (typically 20 hours of active monitoring and four hours in which footage is merely recorded); and a centralized control room enables 24/7 monitoring of cameras in the downtown Baltimore area. By 2013, only three police officers and two information technology personnel were assigned to the system full-time, with another 29 retired officers helping out as monitors.[257]

A 2011 review of surveillance cameras, which includes discussion of Baltimore, argues that police officers with past patrol experience are ideal monitors because they know “where the major crime locations are, who are the persistent offenders, and how to identify subtle movements such as those associated with a drug transaction.”[258] It notes that there is little formal training for monitors, who are typically given a manual outlining allowable and prohibited forms of monitoring, and then trained by veterans. Unfortunately, this also means that officers’ past biases and subjective judgments can also play a strong role in the kinds of activities they decide are worthy of further investigation. Initially, the city also established a Virtual Citizens on Patrol program where community volunteers could be trained as camera monitors, but this was subsequently disbanded, reportedly due to a lack of citizen interest.[259]

[253] La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 23.

[254] William Jackson, “Tech, Tactics behind CitiWatch’s Large-Scale Video Surveillance System,” *GCN*, August 26, 2013, https://gcn.com/articles/2013/08/26/baltimore-psim-tech.aspx.

[255] Jackson, “Tech, Tactics behind CitiWatch’s Large-Scale Video Surveillance System,” ibid.

[256] Todd, “Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore (footnote 247).

[257] Jackson, “Tech, Tactics behind CitiWatch’s Large-Scale Video Surveillance System,” (footnote 254).

[258] La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 25-26.

[259] La Vigne et al., “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,” (footnote 222), p. 24.

At the project's inception, residents expressed concerns about the cameras' potential to violate their privacy and reduce property values. The city held open community meetings to alleviate citizen's fears and persuade them that property values would increase. The police department made all cameras clearly visible to the public, with signs advertising their presence, and also issued a General Order on Electronic Surveillance Procedures to staff to regulate camera use.[260]

Nonetheless, the Baltimore Police Department (BPD) maintains almost complete control over camera placement and use, which is determined based on crime data and input from district commanders. The result has been a network of surveillance cameras that is concentrated in non-White neighborhoods.[261] As of 2020, majority non-White areas of Baltimore have more than 16 cameras, compared with only six in majority White areas.[262] Baltimore's public-housing complexes—98% of which are minority households—are especially targeted by police surveillance cameras. In fact, more than 22% of all cameras in Baltimore are installed on brick apartment buildings that are relatively poor and house less than 2.5% of the city's total population.[263]

Public oversight of the Baltimore Police Department's surveillance network is weak, and the department has previously hidden their activities from the public. In January 2016, BPD launched an aerial "spy plane" surveillance program in conjunction with the for-profit company Persistent Surveillance Systems (PSS), without the knowledge of either the public or elected officials.[264] This program used three daytime planes equipped with cameras to track movement of individuals and send this footage back to a control room staffed with company analysts and police officers. After journalists revealed the program in August 2016, the ACLU and another advocacy group, Leaders of a Beautiful Struggle, sued BPD and the police commissioner for using the aerial surveillance program to surveil activists, thereby violating their constitutional rights. Although two courts denied the plaintiffs' request for a preliminary injunction to stop the program, in June 2021 it was

[260] La Vigne et al., "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," (footnote 222), p. 24.
[261] La Vigne et al., "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," (footnote 222), p. 25.
[262] Todd, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore (footnote 247).
[263] Todd, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore (footnote 247).
[264] Monte Reel, "Secret Cameras Record Baltimore's Every Move From Above," *Bloomberg*, August 23, 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

found to be unconstitutional by the 4th U.S. Circuit Court of Appeals.[265] However, city officials had already ended the program in February, two months after the independent audit that they commissioned revealed that the police department lied about certain aspects of the program, such as how long footage was stored.[266] During the program's six-month run, 99% of plane flights were found to focus on majority Black areas in East and West Baltimore.[267]

As this suggests, a lack of transparency can undermine the potential for surveillance cameras to provide accountability. For example, during the 2015 arrest of Freddie Gray in Baltimore which led to his death, three cameras in the area were inoperative, while two other cameras recorded incomplete footage, entirely failing to capture the first twenty-one minutes of the encounter. Other cameras captured footage but failed to properly train on the scene during the arrest, while others froze during automatic rotations. The police department reported technical glitches when attempting to upload video footage. Some relevant footage of the arrest was entered as evidence into the trials of the six police officers charged in Gray's death, but not all of this footage was released to the public. The glitches, omissions, and low quality of the surveillance footage raised questions about whether BPD was technically incompetent, using opaque and manipulative practices to protect their own officers, or both.[268]

7. Conclusion: Structural Racism, Information Infrastructures, and Intelligence

Most scholars view government intelligence agencies as necessary for protecting institutions of democratic governance, even as they acknowledge that these agencies have often abused their power and undermined democratic aspirations.[269] Recommendations for reform tend to emphasize the need for intelligence to be directed not just towards identifying and prosecuting illegal activities,

[265] "Leaders of a Beautiful Struggle, et al. v. Baltimore Police Department, et al. | Brennan Center for Justice," Brennan Center, December 7, 2020, https://www.brennancenter.org/our-work/court-cases/leaders-beautiful-struggle-et-al-v-baltimore-police-department-et-al.

[266] Mitchell Clark, "Baltimore's Spy Planes Will Fly No More," *The Verge* (blog), February 5, 2021, https://www.theverge.com/2021/2/5/22267303/baltimore-maryland-shut-down-spy-plane-surveillance-program-vote.

[267] Simpson and Cassie, "Spy Plane Experiment Is Over, But Growing Surveillance of Baltimore Continues," (footnote 252).

[268] Catherine Rentz, "Gaps Found in CitiWatch Surveillance Footage of Freddie Gray's Arrest, Transport," *Baltimore Sun*, May 14, 2016, https://www.baltimoresun.com/news/crime/bs-md-graysurveillance-20160513-story.html.

[269] Jean-Paul Brodeur, "High and Low Policing in Post-9/11 Times," *Policing: A Journal of Policy and Practice* 1, no. 1 (2007): 25–37, https://doi.org/10.1093/police/pam002.

but also to address the root causes of those activities, such as poverty and a lack of educational and career opportunities.[270] Some have proposed that community intelligence, in which citizens use open sources to direct law enforcement towards their concerns, can make government intelligence more democratic and accountable, while also helping to counter the "blind spots" of the professional intelligence community.[271] Nonetheless, even critics and reformers tend to view governmental intelligence agencies, with specialized expertise and technology for both open-source and covert operations, as the "dirty work" of maintaining democratic institutions.[272]

Unfortunately, so long as intelligence organizations aim to uphold existing institutions, their analysis tends to reinforce the failings of those institutions, including structural racism within law enforcement. Intelligence analysts have tended to be overly suspicious of all individuals and groups that criticize law enforcement—including the racially diverse groups that protest racist policing—while being under-suspicious of groups that claim to support police—including White supremacists who undermine the human rights that officers are sworn to protect. While explicit racism is no longer officially condoned, some police officers do maintain ties to White supremacist groups.[273] Additionally, while police departments sometimes fire officers over overtly racist behavior, other times they merely discipline officers internally; like all organizations, police departments seek to avoid external scrutiny and maintain their autonomy.[274]

To be sure, federal law enforcement agencies such as the FBI have played a significant role in surveilling and disrupting White supremacist groups such as the Ku Klux Klan. But these efforts have often been driven primarily by concerns about national security and the "rule of law," neglecting the ways that laws have systemically discriminated against minorities.[275] In the 1960s,

[270] James Sheptycki, "Policing, Intelligence Theory and the New Human Security Paradigm: Some Lessons from the Field," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Stephen Marrin, and Mark Pythiam (Routledge, 2008), 166–85.

[271] Martin Innes, "Policing Uncertainty: Countering Terror through Community Intelligence and Democratic Policing," *The ANNALS of the American Academy of Political and Social Science* 605, no. 1 (May 1, 2006), https://doi.org/10.1177/0002716206287118, p. 230.

[272] Innes, "Policing Uncertainty," ibid., p. 299

[273] Michael German, "Hidden in Plain Sight: Racism, White Supremacy, and Far-Right Militancy in Law Enforcement" (Brennan Center for Justice, 2020), https://www.brennancenter.org/our-work/research-reports/hidden-plain-sight-racism-white-supremacy-and-far-right-militancy-law.

[274] Michael German, "Hidden in Plain Sight," ibid.

[275] The FBI has produced a history of its work against the KKK, which emphasizes the agency's efforts to restore "law and order" and the "rule of law." FBI, "KKK Series," https://www.fbi.gov/history/famous-cases/kkk-series (last accessed May 6, 2022). The FBI claims that it aimed "to protect the American people—especially minorities—from the evils of the modern-day Klan," but virtually all of the early examples of such protection are focused on Klan

U.S. policymakers grew concerned that widely publicized racial discrimination and violence undermined the international standing of the United States, and they spurred the FBI to launch an invasive and aggressive surveillance and disruption campaign against White supremacist groups.[276] Since the 1990s, the FBI has increasingly recognized White supremacists as a terrorist threat, but concerns have often focused more on the threat to government institutions than the threat to persons of color.[277] And because racial justice activists challenge the structural racism in these institutions, intelligence organizations have tended to treat racial justice movements with greater suspicion than the White supremacists who are content with the status quo.

This report has highlighted four ways in which contemporary information infrastructures have tended to amplify these suspicions. First, the development of increasingly powerful computer systems has enabled police to keep more detailed records of their interactions with anyone stopped for "suspicious" behavior, amplifying long-standing discrimination against persons of color. Second, the growing efficiency of information sharing among law enforcement tends to spread information about such minor offenses, further encouraging suspicion. Third, the rise of predictive policing tends to amplify suspicion and criminalization of communities of color. Finally, the rise of a private industry that can easily harvest data on activists and then market it to law enforcement tends to pander to and encourage suspicion of racial justice protesters.

activities against White government officials and FBI agents. For example, in the early 1920s the FBI responded to the Louisiana governor's concerns about the murder of "two white men" and interference with the governor's office. Although the KKK was much more likely to murder Black people than White people, the FBI provides only one example of direct efforts to protect Black people: protecting a draft dodger from lynching by escorting him to a military camp to be "quickly inducted." The FBI's account discusses prosecuting violence against Black people only after the passage of the 1964 Civil Rights Act. Even this is focused on "law and order," neglecting the systemic racism that was so often built into law and order. It is striking that the FBI's own account of its work against White supremacists does not provide stronger evidence of the protection of Black people. This suggests that such evidence may not exist.

[276] John Drabble, "To Ensure Domestic Tranquility: The FBI, Cointelpro-White Hate and Political Discourse, 1964-1971," *Journal of American Studies* 38, no. 2 (2004): 297–328; Mary L. Dudziak, *Cold War Civil Rights: Race and the Image of American Democracy* (Princeton University Press, 2011).

[277] Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America* (Harvard University Press, 2018). Belew argues that this shift happened dramatically in the early 1990s, when White supremacists began to adopt anti-government positions, and federal law enforcement responded with force in places like Ruby Ridge and Waco, Texas. As of 2020, the U.S. Department of Homeland Security (DHS) describes White supremacists as "the most persistent and lethal threat" in the United States: "Homeland Threat Assessment" (Department of Homeland Security, October 2020), https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf, p 18.

7.1 Risks to Law Enforcement and Democratic Institutions: The Example of January 6, 2021

While this report has highlighted risks to racial justice activists, it is important to recognize that structural racism in intelligence also puts law enforcement and democratic institutions at risk. Because police cannot possibly be vigilant about all threats, misdirected attention entails neglecting real threats. For example, despite the fact that plans to storm the Capitol on January 6, 2021, were discussed openly online, the FBI and Department of Homeland Security both declined to issue a formal assessment of the threat of insurrection. As investigation of this intelligence failure has continued, intelligence analysts from these agencies have suggested that it was partly a result of a technological transition: the FBI switched from DataMinr to ZeroFox starting January 1, 2021, and many analysts were not fully trained in the new system.[278] They also expressed frustration with ZeroFox, which some analysts pronounced with an expletive (ZeroF*&^).

Nonetheless, neither the transition nor the quality of social media analysis platforms can fully account for the intelligence failure. Even before the transition, in December 2020 multiple individuals and organizations warned the FBI of threats of violence online; while the FBI sent agents to investigate a handful of people, it dismissed other tips.[279] Eventually, on the evening on January 5, the FBI's Norfolk, Virginia field office did issue a "Situation Information Report" about online threats of violence related to the Capitol demonstrations. However, it was disseminated electronically, where it was easily lost in the shuffle, and too late to allow a robust response.[280] This report was accompanied by the caveat that the people who issued these threats were engaging in constitutionally-protected activities, and that it did not intend "to associate the protected activity with criminality or a threat to national security."[281]

Federal officials later claimed that it was difficult to distinguish credible threats from rhetoric, and that they were legally restricted from investigating activities protected by the First Amendment.[282] Yet the U.S. Attorney General's Guidelines clearly authorize the FBI to "proactively" search for "publicly accessible websites and services through which recruitment by terrorist organizations and

[278] For a detailed analysis of the intelligence failings leading to the insurrection, see Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).
[279] Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).
[280] "Examining the U.S. Capitol Attack: A Review of the Security, Planning, and Response Failures on January 6" (Senate Committee on Homeland Security and Governmental Affairs and Committee on Rules and Administration, 2021), https://www.rules.senate.gov/imo/media/doc/Jan%206%20HSGAC%20Rules%20Report.pdf.
[281] Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).
[282] "Examining the U.S. Capitol Attack," (footnote 280).

promotion of terrorist crimes is openly taking place."[283] Furthermore, the FBI searched social media for potential threats related to the protests of George Floyd's murder in 2020, and even charged four people under anti-riot laws based solely on social media postings; some charges were so weak that they were quickly dropped.[284] While the FBI gave the benefit of the doubt to those protesting the election of Joe Biden, it showed great suspicion to racial justice activists.

Other law enforcement agencies issued more urgent warnings. The head of intelligence at the Washington, D.C. fusion center, Donell Harvin, had tasked a member of his team with monitoring online plans for January 6. Harvin, who is Black, was sufficiently alarmed by the findings that he called a major planning meeting on December 30. Before sunrise on January 2, Harvin went further by calling his counterpart at the San Francisco fusion center, Mike Sena. Together, they organized a conference call that drew nearly 300 people from 80 regions, much larger than expected, and unlike any conference call they'd experienced.

Harvin also arranged a briefing with his boss, the Director of Washington, D.C.'s Homeland Security and Emergency Management Agency, who in turn worked with the acting D.C. police chief to brief D.C. Mayor Muriel Bowser. Since Bowser did not want a repeat of the militarized response to the George Floyd protests of June 2020, and military leaders wanted to minimize their involvement, they arranged for the limited deployment of National Guards troops, to conduct a narrow mission of traffic control.[285]

The Capitol Police Intelligence and Interagency Coordination Division (IICD) also issued a series of "special event assessments," as is standard before any major event. Such assessments begin with a "Bottom Line Up Front" and end with an "overall analysis."[286] In its first assessment for the planned January 6 protests, issued on December 16, the "Bottom Line Up Front" failed to indicate any significant threat of violence. The "overall analysis" acknowledged that "the threat of disruptive actions or violence cannot be ruled out," but concluded that "there are no specific known threats

[283] Ken Dilanian, "Why Did the FBI Miss the Threats about Jan. 6 on Social Media?" *NBC News*, March 8, 2021, https://www.nbcnews.com/politics/justice-department/fbi-official-told-congress-bureau-can-t-monitor-americans-social-n1259769.

[284] Cyrus Farivar and Olivia Solon, "FBI Arrests of Protestors Based on Social Media Posts Worry Legal Experts," *NBC News*, June 19, 2020, https://www.nbcnews.com/tech/social-media/federal-agents-monitored-facebook-arrest-protesters-inciting-riots-court-records-n1231531.

[285] Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).

[286] "Examining the U.S. Capitol Attack," (footnote 280), p. 38.

related to the Joint Session of Congress - Electoral College Vote Certification."[287] Over the next three weeks, the IICD gathered increasing evidence of the potential for a violent attack—including that protesters were studying tunnels used by legislators, and discussing confronting them with guns. Nonetheless, the "Bottom Line Up Front" and "overall analysis" did not change substantially in the December 23 or December 30 iterations.[288]

On December 31, Harvin's team briefed the Capitol Police intelligence division with their concerns.[289] Nonetheless, the intelligence division's final assessment issued January 3 did not significantly change the "Bottom Line Up Front" to highlight the potential for a large-scale attack. It was only the "overall analysis" at the *end* of the January 3 assessment, that issued serious warnings: thousands of participants might arrive with a "sense of desperation"; lawmakers rather than counter-protesters would be targeted by violence; and "Stop the Steal's propensity to attract White supremacists, militia members, and others who actively promote violence, may lead to a significantly dangerous situation for law enforcement and the general public alike."[290]

In addition to burying the lຈ, the January 3 assessment was only provided to higher-ranking officers, who were expected to brief those in their chain of command. But rank-and-file officers reported having received no warning about the potential threat; they expected a repeat of previous MAGA rallies.[291] By the time the Capitol Police were calling for emergency help on January 6, it was too late. Police officers defending the Capitol were bewildered to find themselves being attacked by people carrying the "thin blue line" flag, symbolizing support for police.[292]

Intelligence assessments are the product of a complex and bureaucratic process, and failures cannot typically be attributed to any single cause. Investigation of the intelligence failure is ongoing at the time of this writing and has highlighted many problems. Nonetheless, structural racism appears to have played a role. Organizationally, the FBI had focused its resources on terrorism inspired by

[287] "Examining the U.S. Capitol Attack," (footnote 280), p. 40.

[288] See "Examining the U.S. Capitol Attack," (footnote 280). The December 30 version did note evidence of unusually full hotels, but nonetheless continued to project that the demonstrations would be relatively small, and similar to past MAGA rallies.

[289] Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).

[290] "Examining the U.S. Capitol Attack," (footnote 280), p. 45.

[291] "Examining the U.S. Capitol Attack," (footnote 280), p. 51-52.

[292] John Wagner et al., "Police Officers Deliver Emotional Testimony about Violent Day at Capitol," *Washington Post*, July 27, 2021, https://www.washingtonpost.com/politics/2021/07/27/jan-6-commission-hearing-live-updates/.

foreign actors rather than home-grown terrorism.[293] This reflects a longstanding tendency to treat threats as coming from foreigners rather than the prototypical American citizen—a White person.[294] Additionally, evidence suggests that in the face of ambiguity about how to interpret social media, structural racism led to flawed judgments of what constituted a credible threat. At least two interrelated factors likely contributed. First, law enforcement is naturally more suspicious of its critics than of its purported supporters; those protesting Floyd's murder were criticizing police, while many of the people and groups planning the January 6 events claimed pro-police positions—even as they attacked law enforcement. Second, and not coincidentally, the groups protesting Floyd's murder included many people of color, whereas the mob that assaulted the Capitol Building was overwhelmingly White and male, with many overt White supremacists leading the charge. The tendency for law enforcement to cast greater suspicion on persons of color likely contributed to the greater suspicion shown towards racial justice protesters. In short, evidence strongly suggests that structural racism led to flawed intelligence.

7.2 Repurposing Information Infrastructures

Ultimately, structural racism in intelligence endangers not only police officers, but also the human rights that they are sworn to protect. The dynamics described in this report have had real consequences for the racial justice movement, as police suspicion of activists has tended to endanger protestors exercising constitutionally-protected free speech. Several reports have found that law enforcement organizations across the country were by and large unprepared and over-militarized to handle the situation, responding aggressively to the protests, and often appearing to target lawful demonstrators while making little effort to de-escalate tensions.[295] A review of the New York Police Department's response to the George Floyd protests, conducted by the New York City Department of Investigations, found that the department's use of excessive force—including batons and pepper spray, as well as the encirclement and mass arrest of protesters—heightened

[293] Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," (footnote 153).
[294] Jason Ludwig and Rebecca Slayton, "Policy Series 2012-3: Rethinking Vulnerability: Structural Inequality as National Insecurity," *H-Diplo: International Security Studies Forum*, January 21, 2021, https://issforum.org/roundtables/policy/ps2021-3.
[295] Kim Barker, Mike Baker, and Ali Watkins, "In City After City, Police Mishandled Black Lives Matter Protests," (footnote 109).

tensions.[296] While police brutality towards minorities and activists is not solely a result of new information infrastructures, the evidence presented in this report suggests that intelligence gathered through social media has encouraged overly aggressive responses to racial justice activists.

Importantly, structural racism is not technologically determined by information infrastructures, but rather an outcome of the ways that they are designed, maintained, and used. Each of the systems discussed in this report could be repurposed to advance social and racial justice. For example, in his work on predictive policing, legal scholar Andrew Ferguson has proposed the notion of "bright data" to suggest that the same kinds of mapping techniques that identify crime "hot spots" could instead be used to identify communities that have long suffered from a lack of resources and opportunity. [297] These tools could then be used to target resources and policies that empower those communities. Ferguson also proposes "blue data," wherein the same techniques used to predict criminal behavior could be turned around to predict police abuses of power.[298] Some such data analytics are already under development, such as location tracking, algorithms to identify officers at risk of disproportionate use of force, and data on unwarranted stops. However, as Sarah Brayne and others have noted, police and their unions often resist such monitoring.[299] The practical development and use of such systems thus requires more than technology; it also requires a cultural shift in which law enforcement begins to prioritize the community trust that such systems might support, over and above unbridled autonomy.

Transforming the use of social media and the data analytics industry may be even more challenging, particularly in a nation that prioritizes free markets. Activists have used social media to great effect, but reliance on these infrastructures has also made activists vulnerable to unwarranted surveillance. The public nature of activism has made it "low hanging fruit" for data analytics companies, which portray racial justice activists as threats to public safety as they market their services to law enforcement. While the data analytics industry may sometimes produce legitimately useful threat intelligence, the evidence provided in this report suggests that its marketing materials often produce a kind of confirmation bias as they appeal to suspicions already held by law enforcement.

[296] "Investigation into NYPD Response to the George Floyd Protests" (New York City Department of Investigation, December 2020) (footnote 214).
[297] Ferguson, *The Rise of Big Data Policing* (footnote 6).
[298] Ferguson, *The Rise of Big Data Policing,* ibid.
[299] Brayne, *Predict and Surveil* (footnote 119). Leese and Egbert, *Criminal Futures: Predictive Policing and Everyday Police Work* (footnote 4).

Overcoming this bias will require transforming the market through regulation or other measures that raise awareness of the problems intrinsic to the industry. We might envision, for example, mandatory reporting on how companies and law enforcement use social media to assess threats. Annual reviews could include statistics on how often different kinds of threats were flagged, which would differentiate between protests associated with Black Lives Matter, protests organized by the Proud Boys or other White supremacist groups, and more obvious criminal threats such as lone shooters. Such reporting could also include information about whether purported threats actually materialized, whether police responded proportionately, and what other threats may have been missed. Since reporting on threats is inevitably subjective, citizen groups or independent government investigatory bodies would be given a significant role in assessment, along with law enforcement and other professionals that use such data. Reviewing the reliability of threat assessments based on social media would not be a cure-all, but could provide a measure of transparency and accountability, enabling both citizens and law enforcement to better discern the advantages and limitations of intelligence gathered from social media and related platforms.

Cameras are also part of information infrastructures that can either maintain or challenge structural racism. While citizens and activists now have ready access to mobile phone cameras that can document racial violence, most camera infrastructure remains under the control of law enforcement. Until citizens have more substantial control over the development and use of camera infrastructure—including decisions about where cameras are placed, and how camera data is monitored and used—cameras will do little to establish trust and accountability between police and citizens.

Ultimately, there can be no technological fix for structural racism. Nonetheless, the ways that law enforcement design, maintain, and use information infrastructures can either advance or suppress efforts to achieve social justice.