MIAC SHADOW REPORT

Reporting on MIAC Auditing Processes Supplemental to the DPS Report

April 1, 2022


Photo: Canva

Written By:

Chris Cushing
Michael LeComte
Brendan McQuade
Mark Sayre
Maxine Secskas

Endorsed By:

Church of Safe Injection
Electronic Privacy Information Center
Maine Association of Criminal Defense Lawyers
Maine Democratic Socialists of America
Maine Youth Justice
Muslim Justice League

Contents

Acronyms

1H	First half (of a year)
2H	Second half (of a year)
DHS	US Department of Homeland Security
DPS	Maine Department of Public Safety
FOAA	Maine's Freedom of Access Act
HIDTA	High Intensity Drug Trafficking Area
JTTF	Joint Terrorism Task Force
LD	Legislative Document
MIAC	Maine Information and Analysis Center
RFI	Request(s) for Information
SAR	Suspicious Activity Report
UFED	Universal Forensics Extraction Device

Executive Summary

The Maine Information and Analysis Center (MIAC) is an interagency intelligence hub and the State of Maine's node in the National Network of Fusion Centers, recognized by the Department of Homeland Security. In May of 2020, George Loder, a Maine State Trooper, accused the Center of violating privacy laws, monitoring environmentalists, and maintaining an illegal database of gun owners. When Loder raised these concerns, the MIAC command retaliated with a demotion and Loder took his case to court. A month later the controversy deepened with the publication of BlueLeaks, a 269-gigabyte hack of police data which included 5 gigabytes of MIAC data that confirmed some of Loder's allegations and raised new ones.

In the summer of 2021, the Maine State Legislature debated a bipartisan bill to close the MIAC, LD 1278: An Act to End the Maine Information and Analysis Center. The bill cleared the house but failed in the senate. A rival bill, LD 12: An Act To Require Annual Information Reporting by the Maine Information and Analysis Center, cleared both houses and was signed into law in June 2021.[1] This bill requires the Department of Public Safety (DPS) to submit a report to the Joint Standing Committee on Criminal Justice and Public Safety that provides a general review of the type of cases, crimes, incidents, and reports the MIAC has reviewed and evaluated on April 1, 2022. The report must also include the two most recent privacy audits performed by the MIAC's Advisory Board.

This *MIAC Shadow Report* is not a point-by-point rebuttal of the DPS report but an alternative, collaborative, grassroots attempt at oversight, released on the same day as the official report and intended to demonstrates the inadequacy of the measures put in place by LD 12. The DPS report is an exercise in self-policing by the MIAC's Advisory Board, a body mostly composed of MIAC personnel. Even if the privacy audit were conducted by an independent body, the scope of the process would be too narrow to address the concerns raised in 2020. It only audits a random selection of MIAC documents. It does not evaluate the privacy implications of the MIAC's information systems or analytic capabilities. It does not ask the basic question: how much information can the MIAC access, and what it can – and does – do with it. It also ignores issues that fall outside of the rubric of privacy protection.

For this reason, the *MIAC Shadow Report* summarizes and synthesizes the findings of the journalism and academic research on the MIAC. It also picks up where the journalism and scholarship left off, identifying new issues using BlueLeaks and documents released under open records laws that raise questions about the extent and scope of the MIAC's surveillance powers and the impact of MIAC operations on vulnerable populations. The report also includes an independent analysis of the MIAC's privacy policy and a recently available privacy audit that identifies and addresses omissions and deficiencies in MIAC's privacy audit process. This work allows us to anticipate the limitations of the DPS report.

This report is a collaborative, grassroots research project. The writing team is small, ad-hoc group: Chris Cushing, a social worker; Michael LeComte, a privacy advocate and public

[1] Maine State Legislature, *An Act to Require Annual Reporting by Maine Information and Analysis Center*, LD 1278, 130th Legislature, 1st sess., Introduced in Committee on Criminal Justice and Public Safety,January 11, 2021, https://mainelegislature.org/legis/bills/display_ps.asp?PID=1456&snum=130&paper=&paperId=l&ld=12

interest technologist; Brendan McQuade, a University of Southern Maine professor and expert on fusion centers; Mark Sayre, a Maine Law student; and Maxine Secskas, a monitoring, evaluation, and learning professional. The Maine Democratic Socialists of America, Maine Association of Criminal Defense Lawyers, the Electronic Privacy Information Center (EPIC), Maine Youth Justice, Muslim Justice League, and The Church of Safe Injection endorse the findings and demands of the *MIAC Shadow Report*.[2]The main findings are as follows:

- The courts have not settled the allegations of the whistleblower complaint. THe courts dismissed counts concerning surveillance and illegal data retention on technicality and without addressing the substance of the allegations.The case may still go to trial, but the only counts still under consideration concern wrongful termination. It is possible the substantive claims could be re-litigated in an appeal, but this is not assured.

- The MIAC's task force organization muddles command hierarchies, creates organizational confusion, and undermines accountability measures.

- The MIAC has drifted far from its original national security mission. It is preoccupied with traditional concerns of policing: the conventional crimes associated with poverty and powerlessness.

- The MIAC's intelligence bulletins laundered right wing conspiracy theories about paid protesters and pre-staged bricks at the racial justice protests in the summer 2020 as intelligence and cited unconfirmed social media sources as evidence.

- The MIAC's existing oversight mechanisms are flawed. The Advisory Board is made of individuals who are largely unaccountable to the public at large or who lack the necessary expertise to provide meaningful oversight.

- A review of past privacy audits and related BlueLeaks documents identified several documents, which appear to violate the MIAC's privacy policy, including the collection and dissemination of information related to constitutionally protected activities, and the failure to destroy information which no longer meets the necessary standard for use and retention by MIAC. These documents–and others potentially like them–can easily slip through the cracks of the MIAC's flawed privacy audit process. The Advisory Board audits a random selection of documents and, as such, avoids scrutinizing many of the documents that pose the greatest risk to privacy and other civil liberties.

- Records released under open records laws suggest that the MIAC has a subscription to a private databroker, provides information on bankruptcies, liens,

[2] We also thank Fatema Ahmed, Al Cleveland, Sarah T. Hamad, Micheal Kebede, José Martín, Adam Schwartz, Kari Morissette, and Jacob Wiener for their helpful comments and criticism. This report is stronger thanks to their efforts.

properties, corporate affiliations, and other information which is fully redacted and cannot be identified. This raises questions as to whether MIAC's use of commercial databases violates its own privacy policy by allowing it to acquire information that it cannot legally acquire by itself.

- Although the MIAC has made efforts to be more transparent since May 2020, the center is still excessively secretive. The broad exemptions in the Freedom of Access Act make Maine's open records law a limited tool and one that does not provide sufficient transparency.

- The full extent of the MIAC's information systems and analytic capabilities remains unknown. In BlueLeaks, there is a request that a Scarborough police officer sent to the MIAC for help making a timeline from data extracted from cellphones using a phone hacking device sold by Cellebrite, the Israeli digital forensics firm. This incident raises questions about the extent and scope of the MIAC's surveillance powers.

- The MIAC's impact on vulnerable populations is unknown. There are at least 89 MIAC bulletins published in BlueLeaks that report on people with suicidal feelings, mental health issues, disabilities, and/or chronic illness. One of these concerns Joshua Hussey, an individual at risk of "suicide by cop" who was wanted for violation of a protection of abuse order. Despite MIAC intelligence that warned about this risk of "sucide by cop," the Maine State Police sent their tactical team to bring the individual into custody in a 2 AM raid on the home of Hussey's mother. In the subsequent confrontation, Hussey shot himself in the head and eventually died from the wound.

- The MIAC's aggressive focus on substance use may exacerbate the problem and impede harm reduction efforts. BlueLeaks documents show that the Lewiston Police aggressively monitored Jesse Harvey, the founder of the Church Safe Injection. Harvey's friends and colleagues cite this police harassment as the reason for his eventual relapse, overdose, and death. While we cannot confirm that the MIAC did anything with these bulletins other than receiving them from the Lewiston Police Department, the case of Jesse Harvey helps contextualize the MIAC's other intelligence reporting on drug use, some of which are "rogue's galleries" of people arrested for opioid possession that lack any discernible intelligence value and others include inaccurate and easily debunked claims that overstate the harm of illegal substances.

After nearly two years of controversy and debate around the Maine Information Analysis Center, there is a strong case to close the embattled spy center. The allegations of the whistleblower complaint, the abuse complaints against Minkowsky, the hyperfocus on the crimes of powerless and vulnerable populations, the shoddy and biased intelligence shared about the 2020 BLM protests, and the repeated failures of the MIAC to follow its own privacy policy set the

issue in dramatic relief. The MIAC, like all fusion centers, is fundamentally flawed. The MIAC should be closed and any and all databases it has created should be destroyed. These actions would not negatively impact public safety. Indeed, there is reason to believe that the MIAC, as the nerve center of mass criminalization in Maine, is actually exacerbating social problems and negatively impacting public safety. The United States became the global leader in incarceration by treating all social problems as issues for the cops and courts. The MIAC, and other fusion centers, are part of this process. Fusion centers are the nerve system of mass criminalization. Defund the MIAC!

However, the State Legislature did not vote to close the MIAC and, instead, passed a first-in-the-nation bill that requires a fusion center to report to legislative authorities. This measure, while well-intended, is insufficient. Self-policing by the MIAC's Advisory Board is an obvious conflict of interest. Our analysis of the MIAC privacy policy and audits shows that the Maine fusion center regularly violates its own privacy policy. It also exposes the privacy audit as a perfunctory exercise that fails to meet the full scale or scope of the privacy risks posed by the MIAC. The audits only consider MIAC intelligence bulletins; they do not assess its information systems and analytic capabilities.

Given the strict facial recognition regulations recently implemented in Maine, there is little doubt many Mainers would be equally concerned about private data brokers and software that can decrypt phones, analyze telephony metadata, and automatically monitor social media. This report proves that the MIAC uses some of the surveillance and intelligence systems or has used them in the past. What will we do in this present moment? Should this police surveillance and intelligence gathering continue in the future?

Even if the privacy audit was more rigorous, privacy protection is not the only issue posed by the MIAC's operation. The MIAC's monitoring of constitutionally protected speech and assembly needs to be thoroughly investigated, as do related questions regarding how the MIAC reviews the intelligence it disseminates and vets (or fails to vet) the claims made in those bulletins. Finally, the MIAC's impact on vulnerable populations needs to be investigated and questioned. Does the MIAC have a measurable impact, positive or negative, on public safety issues related to mental illness, substance abuse, and homelessness? Should a secretive police intelligence center originally set up for counterterrorism really be part of the public response to these social problems?

The State Legislature needs to rise to the occasion and exercise oversight powers over the executive branch. Once again: Defund the MIAC! If the political will to revisit closing the fusion center is lacking, then the situation demands a thorough, open, and independent investigation. The allegations of the whistleblower complaint have not been settled by the courts or by journalists and scholars working from the outside. We need an independent investigation. Investigate and defund the MIAC!

Introduction: Why This Shadow Report is Necessary

Spying on peace and environmental activists. An illegal database of gun owners. Violations of privacy laws. Punishing a whistleblower. These are the allegations about the Maine Information and Analysis Center (MIAC) from the May 2020 whistleblower complaint filed by Maine State Trooper George Loder.[3] The MIAC is the State of Maine's node in the National Network of Fusion Centers, recognized by the Department of Homeland Security.

A month later, the controversy deepened. Distributed Denial of Secrets, a WikiLeaks-like transparency collective, published BlueLeaks, a 269-gigabyte archive of hacked police data, which included 5 gigabytes from the MIAC.[4] The disclosures immediately confirmed some of the whistleblower's allegations and raised new ones. The documents showed that the MIAC not only monitored the Black Lives Matter protests, but drawing on FBI documents that reference an obviously satirical website and questionable and unreliable social media posts, the MIAC told law enforcement in Maine to be on the watch for paid protesters and pre-staged bricks.[5] These shocking claims and their dubious sourcing were just the tip of the iceberg, however. BlueLeaks revealed that the substantive focus of the MIAC was not terrorism but, rather, property crime, people that use drugs, people with mental illness, and unhoused people.[6] BlueLeaks drew back the curtain of official secrecy and revealed how mass criminalization operates in Maine.

The controversy culminated in a legislative effort to shut down the MIAC, LD 1278: An Act to End the Maine Information and Analysis Center.[7] The bipartisan bill was co-sponsored by Democrats, Republicans, Libertarians, and Independents. It passed the Maine House but failed to clear the Senate. However, another bill, LD 12: An Act To Require Annual Information Reporting by the Maine Information and Analysis Center, cleared both houses and was signed into law in June 2021.[8] This bill requires the Department of Public Safety (DPS) to submit a report to the Joint Standing Committee on Criminal Justice and Public Safety that provides a general review of the type of cases, crimes, incidents, and reports the MIAC has reviewed and evaluated. The report must also include the two most recent privacy audits performed by the MIAC's Advisory Board.

---

[3] Complaint and Demand for Jury Trial, *Loder v. Me. Intel. Analysis Ctr.*, 2:20-cv-00157, 2021 WL 816470 (D. Me. 2021)

[4] Megan Gray, "Hack included documents from secretive Maine police unit," *The Portland Press Herald,* June 27, 2020, https://www.pressherald.com/2020/06/26/hack-included-documents-from-secretive-maine-police-unit/

[5] Nathan Bernard and Caleb Horton, "Teenager or Terrorist?" *The Mainer,* July 29, 2020, https://mainernews.com/teenager-or-terrorist

[6] Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021).

[7] Maine State Legislature, *An Act to End the Maine Information and Analysis Center*, LD 1278, 130th Legislature, 1st sess., Introduced in Committee on Criminal Justice and Public Safety, March 25, 2021, https://mainelegislature.org/legis/bills/display_ps.asp?ld=1278&PID=1456&snum=130

[8] Maine State Legislature, *An Act to Require Annual Reporting by Maine Information and Analysis Center*, LD 1278, 130th Legislature, 1st sess., Introduced in Committee on Criminal Justice and Public Safety,January 11, 2021, https://mainelegislature.org/legis/bills/display_ps.asp?PID=1456&snum=130&paper=&paperId=l&ld=12

The *MIAC Shadow Repor*t is an unofficial supplement and counter to the DPS report. A "shadow report" is a common tactic used by non-government and civil society organizations to present alternative information to contextualize and challenge reports that governments and government entities are required to submit to meet legislative or treaty obligations. This shadow report identifies what the public knows about the MIAC and what we still do not know. It summarizes and synthesizes the findings of the journalism and academic research on the MIAC. It also picks up where the journalism and scholarship left off, identifying two incidents in BlueLeaks that raise questions about the extent and scope of the MIAC's surveillance powers and the impact of MIAC operations on vulnerable populations. The report also includes an independent analysis of the MIAC's privacy policy and a recently available privacy audit that identifies and addresses omissions and deficiencies in MIAC's privacy audit process. This work allows us to anticipate the limitations of the DPS report before it is released.

Moreover, the goal of shadow reports, this one included, is to broaden the parameters of the discussion. In this case, we must move beyond the limits of privacy to address all the concerns raised by the controversy that overtook the MIAC in 2020. Indeed, many documents in the BlueLeaks archive raise concerns that fall outside the rubric of privacy protection. The scandals of 2020 raise sharp questions about the fundamental rigor and quality of MIAC intelligence analysis and the substantive focus of MIAC operations. Is the MIAC sharing useful, vetted information? What populations and social problems is the MIAC monitoring? In what ways and to what ends? These substantive questions are excluded from the privacy audit. What is more, there is nothing in the language of LD 12 to suggest that the official DPS report will do more than provide a narrative summary and descriptive statistics of the MIAC's operations.

The *MIAC Shadow Report* takes on these questions. The first part of this report covers what we know about MIAC. We begin with a profile of the center. From here, we raise concerns regarding the overbroad mission and unclear guidelines, the biased focus of MIAC intelligence operations, and concerns with oversight. Then, we provide a comprehensive analysis of the MIAC's privacy policy and privacy audits. Here, we directly counter the main component of the DPS report, exposing the flaws in their process and identifying several instances where the MIAC failed to follow its stated privacy policy. The second part of the report details what we still do not know. We explain the secrecy that surrounds the MIAC and the unanswered questions regarding the full extent and scope of the MIAC's surveillance capabilities.

This report is a collaborative, grassroots research project. The core research and writing team is a small, ad-hoc group that formed in October 2020: Chris Cushing, a social worker; Michael LeComte, a privacy advocate and public interest technologist; Brendan McQuade, a University of Southern Maine professor and expert on fusion centers; Mark Sayre, a Maine Law student; and Maxine Secskas, a monitoring, evaluation, and learning professional. For months, we have been meeting to study the MIAC and fusion centers, analyze BlueLeaks documents, write Freedom of Access Act requests, and plan and draft this report. We have been doing this work in dialogue with social movement and civil society organizations across Maine and the nation. The Church of Safe Injection, the Electronic Privacy Information Center (EPIC), the Maine Association of Criminal Defense Lawyers, Maine Democratic Socialists of America, Maine Youth Justice, and the Muslim Justice League endorse the findings and recommendations of this report

The case for closing the MIAC is still strong. Although the courts dismissed whistleblower's allegations about spying and illegal data retention on a technicality, recent reporting and research on the MIAC have strengthened the case for shuttering Maine's intelligence center. The whistleblower allegations and similar scandals surrounding the abusive behavior of a federal official assigned to the MIAC suggest that the fusion center has the type of unprofessional work environment that encourages incompetence and abuse. While pre-existing reporting and research have earned fusion centers a bad reputation, journalists found shocking examples where the MIAC shared unconfirmed social media rumors as intelligence for "situational awareness." Further reporting and research have established that the MIAC is focused on minor crimes, especially property and drug crimes—i.e., the surveillance and monitoring of domestic subjects—instead of national security threats. In practice, this work often translates into an intense focus on vulnerable populations, particularly people that use drugs, people with mental illness, and unhoused people. The United States became the global leader in incarceration by treating all social problems as issues for the cops and courts. The MIAC, and other fusion centers, are part of this process. Fusion centers are the nerve system of mass criminalization.

*Fusion centers are the **nerve system of mass criminalization***

While this shadow report and the organizations endorsing it call for the MIAC to be closed, the legislature voted for oversight. However, the solution proposed by LD 12 – self-policing of the MIAC by its Advisory Board – is not meaningful oversight. Our original analysis of previous audits and related review of BlueLeaks documents identifies serious flaws in this approach. The MIAC's Advisory Board is not an independent entity and includes the senior leadership of the MIAC. Such self-policing is a clear conflict of interest. Our review of past audits and related BlueLeaks documents suggests that this arrangement is not facilitating meaningful oversight. We have found several documents in BlueLeaks, which appear to violate the MIAC's privacy policy. These documents–and others potentially like them–can easily slip through the cracks of the MIAC's flawed privacy audit process. The Advisory Board audits a random selection of documents and, as such, avoids scrutinizing many of the documents that pose the greatest risk to privacy and other civil liberties.

Most importantly, the parameters of the privacy audit are too narrow to capture all the concerns posed by MIAC. In recent years, Americans and Mainers have raised serious questions about the criminal legal system. Widespread concerns about privacy and civil liberties protection led the Maine State Legislature to pass and the governor to sign the first statewide regulations on facial recognition technology in the nation in 2021. This legislation bans the use of the technology in most areas of government and strictly limits its use by law enforcement.[9] In our review of BlueLeaks documents, we found documents that raise questions about the MIAC's use of private data brokers and ability to analyze cell phone data. These systems, like the recently regulated facial recognition technology, also pose existential threats to privacy and

[9] Grace Woodruff, "Maine Now Has the Toughest Facial Recognition Restrictions in the U.S." *Slate*, July 2, 2020, https://slate.com/technology/2021/07/maine-facial-recognition-government-use-law.html.

other basic rights. The privacy audit process does not extend past the bulletins produced and shared by the MIAC to assess the surveillance technologies purchased and used by the intelligence center. The public concern for privacy and civil liberties protection is not limited to facial recognition surveillance. These surveillance systems and their current use by the MIAC deserve the same scrutiny. The privacy audit will not touch on this issue.

Even if the privacy audit was extended to cover the full scope of MIAC operations, privacy is not the only concern posed by the MIAC. Should police surveillance be part of Maine's response to social problems like mental illness or substance use disorder? Does such surveillance even have a positive impact on these issues? The cases of Joshua Hussey and Jesse Harvey, discussed in detail in the subsection titled "the MIAC's impact on vulnerable populations," are reasons to believe that this criminalization is part of the problem. Police surveillance was involved in the preventable deaths of both Hussey and Harvey. The former needed help, and the latter needed to be free to do his harm reduction work without police harassment. Instead, both were criminalized and targeted by police. At a time of broad questioning of the criminal legal system, including a nearly successful bill to decriminalize possession of illegal substances in Maine, the MIAC's hyper-focus on minor crimes demands reflection.

*Should **police surveillance** be part of Maine's **response to social problems** like mental illness or substance use disorder?*

This report is a contribution to this needed reflection and provocation that renews the calls of LD 1278–Defund the MIAC!–and questions the efficiency of LD 12. Self-policing is not meaningful oversight. Meaningful for oversight would be a thorough, open, and independent investigation. To this end, this report also outlines what a real investigation of the MIAC would entail. We detail procedures that could guide a more meaningful privacy audit. We also identify a series of unanswered questions and unaddressed issues. The current situation is not a serious solution to the problems raised in 2020: investigate and defund the Maine Information Analysis Center!

*The current situation is **not a serious solution** to the problems raised in 2020: **investigate and defund the Maine Information Analysis Center!***

What We Know about Fusion Centers and the MIAC

The MIAC and Fusion Centers

The Maine Information and Analysis Center (MIAC) is part of the National Network of Fusion Centers, a group of interagency intelligence hubs recognized by the Department of Homeland Security but managed by either state or municipal police. Originally set up for national security purposes, most fusion centers now have a potentially limitless "all crimes, all threats, all hazards mission."[10] In practice, fusion centers are managed by police agencies and are adjuncts to policing.

Organizationally, fusion centers are data analysis and processing nodes in information-sharing networks. While managed by municipal or state police, personnel from other federal, state, and local agencies also work out of fusion centers. These personnel often have access to different databases than the ones available to police officers managing the fusion center. This arrangement is intentional and designed to facilitate information sharing. The Maine State Police officers running the MIAC may not be able to directly search a federal database, but they can indirectly access it through the federal personnel who work out of the MIAC.

In addition to these arrangements, fusion centers will also enter agreements with other entities that allow them to remotely access their records. Fusion centers often buy databases from private brokers, companies that collect personal identifying information and sell it. The information that data brokers collect is extensive. It can encompass court records, motor vehicle records, census data, birth certificates, marriage licenses, voter registration information, bankruptcy records, divorce records, cell phone geolocation data, data purchased from credit card providers and retailers, and information gleaned from social media.

Fusion centers also can become repositories for new sources of data from specialized surveillance systems connected to a given fusion center. The Boston Regional Intelligence Center, for example, operates a real-time crime center that monitors the thousands of surveillance cameras throughout the Boston metro area.[11] The New Jersey Regional Operations Center, a fusion center operated by the New Jersey State Police, receives data from automated license plate readers operated and set up by municipal law enforcement throughout the state.[12]

With all these data streams flowing into the fusion center, analysts try to identify patterns and produce intelligence for other government agencies and the private sector. Often, fusion

---

[10] For an in depth discussion of the origins and creation of fusion centers see, Brendan McQuade, *Pacifying the Homeland: Intelligence Fusion and Mass Supervision* (Oakland: University of California Press, 2019), 1-4, 21-25, 60-88.

[11]Rebecca Cadenhead, "The State of Surveillance in Boston Public Schools," *The Harvard Crimson*, November 11, 2021, https://www.thecrimson.com/article/2021/11/11/boston-school-surveillance/; "Get the BRIC out of Boston," Muslim Justice League, undated, https://muslimjusticeleague.org/our-work/get-the-bric-out-of-boston/.

[12] Attorney General Paula T. Dow to Director of Office of Homeland Security and Preparedness, Director of Division of Criminal Justice, Superintendent of New Jersey State Police, All County Prosecutors All County Sheriffs, All Police Chiefs, All Law Enforcement Chief Executive, December 3, 2010, State of New Jersey, Office of Attorney General, Directive No.2010-5 "Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data," https://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf.

centers provide simple case support. Analysts will perform basic searches for police investigators who call into the fusion center to get more information, usually about a suspect or person of interest: addresses, criminal histories, known family members, and friends. This is how fusion centers act as Google for cops. Other times, fusion centers, and especially the largest among them, will work with police investigators for weeks or months. They will complete multiple rounds of data analysis and may even get deeply involved in intelligence collection. In these situations, fusion centers will often use specialized software to create sophisticated intelligence products. This is how fusion centers act as an outsourced intelligence division, a miniature CIA or NSA on call for municipal police and other registered users of the fusion center in government and the private sector.

Different fusion centers, for example, are known to have the capability to run facial recognition searches or automatically monitor social media.[13] Many fusion centers have software that allows them to analyze telephony metadata and produce a pattern of life analysis. In other words, some fusion centers have the capability to take an unwieldy mass of data about calls, messages, and locations taken from an individual phone and run it through software that produces a concise report about other phone numbers which have been frequently contacted, the geographical locations frequented, and, hence, the general rhythms of the user of the phone in question. Using similar software, some fusion centers have the capability to combine various sources of data and produce a social network or link analysis that maps out the connections among people, businesses, properties, cars, guns, and other data points.[14] Data mapping is another common analytic capability of fusion centers. The most basic version of data mapping in law enforcement is a “hotspot” map that shows the geographical distribution and clustering of criminal incidents. Today, analysts at fusion centers go beyond crime data. They will geocode and map crime incidents often in relation to demographic information and other data sources.[15] Some fusion centers have software packages that take this mapping further and try to predict the likely location of future crimes by analyzing hundreds of layers of data and identifying the correlations associated with particular crime types.[16]

---

[13]Fusion centers in Boston and Oakland are known to have (or have had) automated systems to monitor social media. Micah Lee, How Northern California’s Police Intelligence Center Tracked Protests, The Intercept (Aug. 17, 2020), https://theintercept.com/2020/08/17/BlueLeaks-california-ncric-black-lives-matter-protesters/; At least ten fusion center are known to have the ability to run facial recognition searches: Nasser Eledroos and Kade Crockford, “Social Media Monitoring in Boston: Free Speech in the Crosshairs,” *Privacy SOS,* 2018, https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/;Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA,” *Buzzfeed News,* February 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement;

[14] This report explains common software systems used at many fusion centers to analyze telephony metadata and produced patterns of life and social network analyses. This capability is used on a case-by-case basis as part of police investigation. Chris Schiano, “Reveal: Denver Police Using NSA-Grade Surveillance Software,” *Unicorn Riot*, April 4, 2016. https://unicornriot.ninja/2016/revealed-denver-police-using-nsa-grade-surveillance-software/

[15] Esri, *Geospatial Intelligence for Fusion Centers*. An Esri White Paper, April 2011. https://silo.tips/download/an-esri-white-paper-april-2011-geospatial-intelligence-for-fusion-centers

[16] Brendan McQuade, "World Histories of Big Data Policing," *Journal of World-Systems Research* 27, no. 1 (2021): 128.

While some fusion centers are "co-located" with other government entities, often FBI field offices or the headquarters of regional High Intensity Drug Trafficking Areas, the MIAC, like most fusion centers, was created as a new, standalone entity in the mid-2000s. At the time, the newly created Department of Homeland Security (DHS) encouraged state governments to set up fusion centers. In 2004, a year after DHS officially opened its doors, the department recognized 18 fusion centers. Two years later, an executive order issued by Maine Governor Baldacci created the MIAC, which joined the then-37 fusion centers recognized by the DHS. Today, there are 80 DHS-recognized fusion centers.[17]

Fusion centers can be hard to evaluate. As a grant-driven federal initiative with "baseline capabilities" but no binding standards, no two fusion centers are alike. The variation from fusion center to fusion center can be dramatic. The phrase—"If you've seen one fusion center, you've seen one fusion center"—has become clichéd within the intelligence and law enforcement community and reflects the wide variations among fusion centers.[18] Official secrecy, moreover, cloaks fusion centers, so what little public information is available on a particular fusion center rarely provides much detail on its unique profile.

In general, however, fusion centers have earned a poor reputation within the government. The first warnings came in 2007 and 2008. Government auditors found that fusion centers duplicated the mission of existing agencies and offices, exacerbating existing bureaucratic rivals.[19] At this time, the ACLU raised civil liberties concerns and brought attention to the role of the military and private sector in the fusion centers.[20]

In October 2012, the US Senate Permanent Subcommittee on Investigations excoriated fusion centers. After two years of investigation, they could not identify any "reporting which uncovered a terrorist threat…[or any] contribution such fusion center reporting made to disrupt an active terrorist plot."[21] The Senate reiterated the findings of earlier audits and brought

---

[17]Executive Order 25 FY 06/07 of December 8, 2006, "An Order Establishing the Maine Intelligence Analysis Center," Office of the Governor, http://lldc.mainelegislature.org/Open/Exec/ExecutiveOrders/72_Baldacci/2006-07/eo_2006-07no24.pdf; US Senate, Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers, October 3, 2012, http://www.coburn.senate.gov/public/index.cfm/files/serve?File_id=693b820a-0493-405f-a8b5-0e3438cc9b24, 11-3.

[18] Proponents and critics of fusion centers both use the expression to, respectively, assert that fusion centers meet the unique needs of their jurisdictions or bemoan the lack of standardization. See: Justin Lewis Abold, Ray Guidetti, and Douglas Keyer. "Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining 'Centers of Analytical Excellence,'" *Homeland Security Affairs* 8, no.1 (2012); Hilary Hylton, "Fusion Centers: Giving Cops Too Much Information?" *Time*, March 9, 2009.

[19] DHS Office of Inspector General, "DHS' Evolving Role in State and Local Fusion Centers*"* The Department of Homeland Security, OIG-9-2012, 2008, http://www.oig.dhs.gov/assets/Mgmt/OIG_09-12_Dec08.pdf; Todd Masse, Siobhan O'Neil, and John Rollins, "Fusion Centers: Issues and options for Congress" Congressional Research Services, 2007: http://epic.org/privacy/fusion/crs_fusionrpt.pdf; John Rollins, "Fusion centers: Issues and options for Congress," Library of Congress, Washington, DC, 2008: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA482006, 29-32

[20] Mike German and Jay Stanley, "What's Wrong with Fusion Centers," ACLU, December 2007, http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

[21] US Senate, Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, October 3, 2012,

uncomfortable national attention to the fusion centers. “DHS ‘fusion centers’ portrayed as pools of ineptitude and civil liberties intrusions” read *The Washington Post*’s headline.[22] *The New York Times* reported that “One of the nation’s biggest domestic counterterrorism programs has failed to provide virtually any useful intelligence.”[23] Within the fusion center community, this problem carries the name “intelligence spam.”[24]

Seven months later, these criticisms were confirmed in horrific fashion by the Boston Marathon Bombing. In the preceding two years, the FBI and CIA neglected to share information about Tamerlan Tsarnaev, the elder brother implicated in the attack, with the Boston Regional Intelligence Center. Even if they had, Boston’s fusion center was most concerned with surveilling Occupy Boston.[25]

By 2012, the failure of fusion centers was plain. It led to the first calls to close them. They came from conservative think tanks.[26] In response to the Senate Report, the Heritage Foundation recommended that DHS “dramatically reduce the number of fusion centers” to 32 because the “terrorist threat is not high and…financial support is too thin or could be allocated more effectively.”[27] In 2016, The American Enterprise Institute called for eliminating many fusion centers and merging others into Joint Terrorism Task Forces, an older interagency counterterrorism program run by the FBI.[28]

While fusion centers have long been criticized, there has not been a serious attempt to address these problems until recently. LD 1278, debated in Maine in the summer of 2021, was the first legislative effort to close a fusion center. While unsuccessful, it resulted in the passage

---

http://www.coburn.senate.gov/public/index.cfm/files/serve?File_id=693b820a-0493-405f-a8b5-0e3438cc9b24, 3.

[22] Robert O’Harrow, “DHS ‘fusion centers’ portrayed as pools of ineptitude and civil liberties intrusion,” *The Washington Post,* October 2, 2012, https://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html

[23] James Risen, “Inquiry Cites Flaws in Counterterrorism Offices,” *The New York Times,* October 2, 2012, http://www.nytimes.com/2012/10/03/us/inquiry-cites-flaws-in-regional-counterterrorism-offices.html

[24] Brendan McQuade, "The Puzzle of Intelligence Expertise: Spaces of Intelligence Analysis and the Production of ‘Political’ Knowledge," *Qualitative Sociology* 39, no. 3 (2016); 261;Joshua M.Dennis, *Standing on the Shoulders of Giants: Where Do We Go from Here to Bring the Fire Service into the Domestic Intelligence Community?* MA Thesis (Naval Postgraduate School, 2012); 12; Andrew Becker and G. W. Schulz, “Homeland Security Office Creates Intelligence Spam InsidersClaim,” The Center for Investigative Reporting, September 5, 2011, http://cironline.org/reports/homeland-security-office-creates-intelligence-spam-insiders-claim-2915

[25] Michael Iskioff, “Unaware of Tsarnaev warnings, Boston counterterror unit tracked protesters” *NBC News*, May 9, 2013, http://investigations.nbcnews.com/_news/2013/05/09/18152849-unaware-of-tsarnaev-warnings-boston-counterterror-unit-tracked-protesters

[26] The 2007 ACLU report had only called for regulating fusion centers, Mike German and Jay Stanley, “What’s Wrong with Fusion Centers,” ACLU, December 2007, http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

[27]Matt Mayer and Micheal Downing, “The Domestic Counterterrorism Enterprise: Time to Streamline,” The Heritage Foundation, October 3, 2012, https://www.heritage.org/terrorism/report/the-domestic-counterterrorism-enterprise-time-streamline

[28] Matt Mayer, “Consolidate Domestic Intelligence Entities Under the FBI,” American Enterprise Institute, March 2016: https://www.aei.org/wp-content/uploads/2016/03/Fusion-Center.pdf (Accessed March 27, 2016).

of another bill, LD 12, which set up the first requirement for a fusion center to report to legislators.

Recently, fusion centers have become subjects for debate in more jurisdictions. In December 2021, a group of citizens in Oregon filed a class-action suit alleging that the state's TITAN Fusion Center overstepped its initial focus on information sharing for national security purposes and, instead, unlawfully spied on peaceful demonstrators opposing natural gas infrastructure. The plaintiffs want the court to declare Oregon's TITAN Fusion Center unlawful, halt its operations, and order the center to destroy or expunge all records on them and their organizations.[29] In Milwaukee, candidates in the mayoral primary have called to close that city's fusion center.[30]

In other jurisdictions, legislators have responded to pressure from below and reduced funding for fusion centers or denied budget increases. In Boston, concerns about racial profiling and political policing have focused attention on the activities of the Boston Regional Intelligence Center, leading to calls to dismantle the "gang" database maintained by the fusion center.[31] In July 2021, the Boston City Council declined to approve an $850,000 grant awarded to the Boston Regional Intelligence Center in recognition of these concerns.[32] In Minnesota, mobilization from privacy advocates and racial justice activists compelled state legislators to abandon a proposed $5 million budget increase for the state's fusion center.[33]

The Profile and History of the MIAC

As a result of this increased public scrutiny, most basic details regarding the MIAC are now public information. In 2015, when the MIAC first received meaningful attention from journalists, the Department of Public Safety would not provide budget or staffing figures.[34] Now, these figures are known as a result of open records requests filed in the Spring of 2020 and related efforts of the Department of Public Safety to address public concerns about the MIAC.

---

[29] Maxine Bernsein, "Oregon's anti-terrorism fusion center lacks legislative authority, collects intelligence on protesters, lawsuit says," *The Oregonian*, December 14, 2021, https://www.oregonlive.com/crime/2021/12/oregons-anti-terrorism-fusion-center-lacks-legislative-authority-collects-intelligence-on-protesters-lawsuit-says.html.

[30] Isaiah Holmes, "Milwaukee mayor's race builds to crescendo prior to Tuesday election," *Wisconsin Examiner*, February 11, 2022, https://wisconsinexaminer.com/2022/02/11/milwaukee-mayors-race-builds-to-crescendo-prior-to-tuesday-election/

[31] Sandra Susan Smith, Felix Owusu, and Stacey Borden, "Boston's gang database should be dismantled," *The Boston Globe*, January 31, 2022, https://www.bostonglobe.com/2022/01/31/opinion/bostons-gang-database-should-be-dismantled/

[32] Sean Philip Cotter, "Boston City Council rejects $850G for the Boston Regional Intelligence Center," *Boston Herald*, June 30, 2021, https://www.bostonherald.com/2021/06/30/boston-city-council-rejects-850k-for-the-boston-regional-intelligence-center/

[33] José Martín, "Restore the 4th Minnesota: Racking Up Victories in 2021," The Electronic Frontier Foundation, December 8, 2021, https://www.eff.org/deeplinks/2021/12/restore-4th-minnesota-racking-victories-2021

[34] Steve Mistler, "Secretive fusion center to play key role in Maine drug crackdown," *The Portland Press Herald*, September 6, 2015, https://www.pressherald.com/2015/09/06/secretive-fusion-center-to-play-key-role-in-maine-drug-crackdown

The MIAC is one of the smaller fusion centers. The staffing levels of fusion centers vary. Some have less than ten staff; others have as many as 80 or 100.[35] In July 2020, the MIAC had six full-time positions, ten part-time positions, and four management positions. Personnel from Maine State Police and Maine Emergency Management provide much of the leadership and full-time staff. However, personnel from the FBI, Border Patrol, National Guard, New England High Intensity Drug Trafficking Initiative (HIDTA), Bureau of Motor Vehicles, Maine Warden's Service, Kennebec County Sheriff's Office, and Franklin County Sheriff's Office also staff the center, many on a part-time basis.[36] In recent years, the MIAC's budget ranged from a low of $743,903 in 2019 to a high of $1.07 million in 2017. Importantly, these budgets do not include the salary cost assigned to MIAC from agencies other than the Maine State Police.

For the first nine years of its operation, the MIAC garnered little attention. That situation changed in 2015 when the LePage Administration tasked the MIAC with analyzing arrests and overdoses as part of the state's response to the opioid epidemic. This attention brought scrutiny. At the time, *The Press Herald* reported that MIAC's three-member Oversight Board had not met in years.[37] In response, Representative Charlotte Warren called for strengthening and expanding the MIAC's Advisory Board, but the proposal did not get out of legislative council.[38]

The MIAC soon returned to headlines when the LePage administration held a press conference in 2016 urging Mainers to take part in the "See something, say something" campaign and report suspicious activity to the MIAC.[39] "See Something, say something" is the public face of the National Suspicious Activity Reporting Initiative, an effort to encourage widespread monitoring of "suspicious activity", which the federal government defines as "observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity."[40] "See Something, say something" encourages civilians to call 9-11 or

---

[35] Priscilla Regan and Torn Monahan, "Beyond Counterterrorism: Data Sharing, Privacy and Organizational Histories of DHS Fusion Centers," International Journal of E-Politics 4, no. 3 (2013): 5; Brendan McQuade, *Pacifying the Homeland: Intelligence Fusion and Mass Supervision.* (Oakland: University of California Press, 2019), 77.

[36] Maine State Police, "The Maine Information and Analysis Center" July 2020, http://legislature.maine.gov/doc/4165.

[37] Steve Mistler, "Secretive fusion center to play a key role in Maine drug crackdown," *Portland Press Herald*, September 6, 2015, https://www.pressherald.com/2015/09/06/secretive-fusion-center-to-play-key-role-in-maine-drug-crackdown

[38]Steve Mistler, "Maine legislator seeks more oversight of secretive surveillance unit," *Portland Press Herald*, October 20, 2015, https://www.pressherald.com/2015/10/20/maine-lawmaker-wants-oversight-of-states-secretive-fusion-center/; Steve Mistler, "Maine's drug abuse epidemic front and center as legislation advances to next session," *Portland Press Herald*, November 19, 2015, https://www.pressherald.com/2015/11/19/maines-drug-abuse-epidemic-front-and-center-as-legislation-advances-to-next-session/

[39] Charles Eichacker, "Mainers urged to report suspicious activity, but LePage steers clear of race," *Kennebec Journal*, September 13, 2016, /2016/09/13/mainers-urged-to-report-suspicious-activity-as-part-of-national-security-initiative/?_gl=1*1asfuc7*_ga*MjA4MzQxNDE4My4xNjIyNTU5NjQ2*_ga_ZYHMH0BHHB*MTY0NDc4MDYyMC4xMjQuMS4xNjQ0NzgxMDg4LjA.&_ga=2.176202274.604837151.1644711934-2083414183.1622559646

[40] Program Manager for the Information Sharing Environment, "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5," Office of the Director of National Intelligence, May 21, 2009, https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf

the non-emergency phone number of local law enforcement to report suspicious activity. If warranted, local law enforcement forwards the resultant Suspicious Activity Report (SAR) to a nearby fusion center, which reviews the reports. If the fusion center concludes that the report is credible, it is entered into the Nationwide Suspicious Activity Reporting System.

There is little oversight over the suspicious activity reporting process, and the few examples of audits raise concerns of racial profiling. The Los Angeles Police Department Office of Inspector General conducted several audits of SARs, which documented a clear pattern of racial profiling. The March 2013 audit showed 82% of SARs were written on non-white people, with the largest sample written on the black community.[41] The January 2015 audit showed 79% of SARs were written on non-whites and 30% of SARs concerned black people.[42] The September 2016 audit found 79% of SARs were written on non-whites.[43] There is no similar publicly available information about the MIAC's work processing SARs, but the webpage of the Maine Emergency Management Agency on the "See Something, Say Something" campaign identifies MIAC as the Maine government entity that vets SARs.[44]

The MIAC receded from public attention until 2020 when it became the subject of sustained debate. Amid mounting concern, both in Maine and around the country, around facial recognition surveillance, *The Press Herald* published a February 2020 feature story on the surveillance programs of the Maine State Police, which included coverage of the MIAC. At this point, the Department of Public Safety would not provide any information about the MIAC's technological capabilities and refused to "provide a detailed budget, meeting minutes from an advisory committee tasked with oversight, or any audits of the center's operation." The story noted that a representative from Central Maine Power– Bruce Lewis, the utility's director of security–sat on the MIAC's advisory board.[45]

The connection between CMP and MIAC soon became controversial. In May 2020, a whistleblower alleged that the MIAC gathered information on the Say No to the New England Clean Energy Corridor campaign and passed that information to staff at CMP.[46] George Loder, a Maine State Trooper, filed a whistleblower complaint that alleged the MIAC gathered information on the opposition to Central Maine Power's The New England Clean Energy Connect, a

---

[41] Alexander Bustamante, "Los Angeles Police Commission Suspicious Activity Reporting System Audit," Los Angeles Police Department Office of the Inspector General, March 12, 2013, https://stoplapdspying.org/wp-content/uploads/2013/03/IG-audit.pdf

[42] Alexander Bustamante, "Los Angeles Police Commission Suspicious Activity Reporting System Audit, Fiscal Year 2013/2014" Los Angeles Police Department Office of the Inspector General, January 23, 2015, http://www.lapdpolicecom.lacity.org/012715/BPC_15-0014.pdf

[43] Alexander Bustamante, "Los Angeles Police Commission Suspicious Activity Reporting System Audit," Los Angeles Police Department Office of the Inspector General, September 7, 2016, http://www.lapdpolicecom.lacity.org/091316/BPC_16-0312.pdf

[44] "See Something, Say Something," Maine Emergency Management Agency, undated, https://www.maine.gov/mema/homeland-security/see-something-say-something

[45] Randy Billings, "Maine State Police may be spying on you," *Portland Press Herald*, February 10, 2020, https://www.pressherald.com/2020/02/09/maine-state-police-may-be-spying-on-you/

[46]Matt Byrne, "CMP corridor opponents seek info gathered during alleged police spying," *Portland Press Herald*, https://www.pressherald.com/2020/05/21/cmp-corridor-opponents-seek-info-gathered-during-alleged-police-spying/

transmission line project that was ultimately rejected by Maine voters in a referendum in November 2021. Loder claimed that the MIAC passed this information on to CMP.

The whistleblower complaint also alleged that the MIAC illegally collected and retained other information. Loder charged that the MIAC maintained information on counselors and volunteers for the group Seeds of Peace, a camp for young people from conflict areas around the world to learn peacebuilding and leadership skills. It claimed that the MIAC has agreements with "agencies in other states having plate readers to provide information on Maine registered vehicles." This alleged arrangement would allow the MIAC to circumvent Maine law, which prohibits the retention of data from automated license plate readers for more than 21 days. Loder also charged that "the information is mined from the license plate data of the other agencies by computer without any pre-existing suspicion of criminal activity." The suit also claimed that the MIAC retains information from the background checks that the state police conducts on people seeking to buy guns, effectively creating a database of gun owners. Finally, the suit alleged that the MIAC "conducts electronic surveillance of people's social media and other accounts and permanently retains personal and private information on those individuals because they engaged in constitutionally protected activity such as participating in a lawful protest or purchasing a firearm."[47]

In June 2020, the publication of BlueLeaks created an even greater scandal. The transparency collective Distributed Denial of Secrets published 269 gigabytes of hacked police files, including 5 gigabytes from the MIAC. The hacks compromised the MIAC's website and email system, resulting in the publication of the records shared by and with the MIAC. Subsequent analysis and reporting showed that the MIAC focused mostly on minor crimes and produced intelligence with a clear political bias.[48] This coverage added fuel to the fire sparked by the whistleblower complaint and led legislators to propose two bills related to the MIAC in the summer of 2020.

The hacks, however, did not touch the MIAC's internal information systems, which means the archive cannot confirm or refute Loder's allegations concerning illegal data retention on protestors and gun owners, as well as circumventing Maine law by accessing data license plate readers set up by law enforcement out of state. BlueLeaks does provide some confirmation of monitoring of CMP. An August 28, 2018, situational awareness report published by the MIAC details a case of "criminal mischief and littering in The Forks, ME, in protest of the New England Clean Energy Connect (NECEC) project… Signs were hung on trees and on a wire suspended across a gorge that is used by local rafting companies… Paint stirring sticks

[47] Complaint and Demand for Jury Trial, *supra* note 1, ¶ 63.

[48] Matt Byrne, "Stolen documents who Maine police unit shifted focus from terrorism to routine crimes," *The Portland Press Herald*, July 12, 2020, https://www.pressherald.com/2020/07/12/stolen-documents-show-maine-police-unit-shifted-focus-from-terrorism-to-routine-crimes/; Nathan Bernard and Caleb Horton, "Teenager or Terrorist?" *The Mainer,* July 29, 2020, https://mainernews.com/teenager-or-terrorist/; Brendan McQuade, "Police Surveillance is Criminalization and it Crushes People," *Counterpunch*, October 15, 2020, https://www.counterpunch.org/2020/10/15/police-surveillance-is-criminalization-and-it-crushes-people/; Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021)

with hand-written messages were also thrown into the gorge."The document also asks law enforcement to report any information on the incident to the Maine Warden Service.[49]

At this point, it seems unlikely that the allegations in the Loder complaint will be settled in the courts in the near future. In March 2021, the US District Court for Maine dismissed the charges in the Loder complaint but did so on a technicality and without addressing the substance of the allegations. The Loder complaint charged that the MIAC violated the Privacy Act, the federal statute that governs how federal agencies collect, store, and share personal identifying information. However, the court found that Privacy Act does not apply to the MIAC, which, despite its multi-jurisdictional nature, is classified as part of state government. Hence, the court dismissed the charges on procedural grounds and did nothing to either confirm or refute the allegations.[50] The case may still go to trial, but the only counts still under consideration concern wrongful termination. It is possible the substantive claims regarding illegal surveillance could be re-litigated in an appeal, but this is not assured.[51]

The status of the whistleblower complaint notwithstanding, all the controversy and contention around the MIAC put sustained focus on the secretive intelligence center. We now know more about the MIAC than ever before, and it is clear that there are serious issues that need to be addressed and will not be touched by the DPS report.

Organization

The MIAC, like other fusion centers, has a task force organization, which muddles command hierarchies, creates organizational confusion, and undermines accountability measures. Many of the personnel working at fusion centers have two supervisors: the fusion center director and the supervisor at their home agency. As a result, chains of command at fusion centers can be unclear. Multiple reports and studies from government auditors and scholars document this issue and detail how it can cause confusion and misconduct.[52]

This dynamic is on display in the MIAC. From 2013 to 2018, Loder was assigned to the Joint Terrorism Task Force (JTTF) operated by the FBI's Boston field office but also was required to report to the MIAC's supervisor. Loder alleged that the MIAC command pressured him to share information with the MIAC about the cases the JTTF was pursuing, which would violate both FBI policy and the Privacy Act. Loder's position between his home agency and two interagency agency task forces created a tense and ambiguous situation that unsurprisingly led to confusion and conflict. [53]

---

[49] The Maine Information and Analysis Center, "Situational Awareness," MIAC-2018-1570, August 28, 2018, https://ddosecrets.com/wiki/BlueLeaks.

[50] *Loder v. Me. Intel. Analysis Ctr.*, 2:20-cv-00157, 2021 WL 816470 at *7, *9 (D. Me. 2021), 7-9, 14-15.

[51] Emily Allen, "State denies trooper faced whistleblower retaliation," *Portland Press Herald*, March 25, 2022.

[52] US Senate, Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, October 3, 2012, http://www.coburn.senate.gov/public/index.cfm/files/serve?File_id=693b820a-0493-405f-a8b5-0e3438cc9b24, 51-52;John Rollins, "Fusion centers: Issues and options for Congress," Library of Congress, Washington, DC, 2008: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA482006, 23; Brendan McQuade, "The Puzzle of Intelligence Expertise: Spaces of Intelligence Analysis and the Production of 'Political' Knowledge," *Qualitative Sociology* 39, no. 3 (2016); 250-251.

[53] Complaint and Demand for Jury Trial, *Loder v. Me. Intel. Analysis Ctr.*, 2:20-cv-00157, 2021 WL 816470 (D. Me. 2021),

These muddled command hierarchies can also allow inappropriate behavior to slip through the cracks. In May of 2021, the *Bangor Daily News* reported that James Minkowsky, a former officer with the Lewiston Police Department who resigned in 2014 after two women accused him of harassment and intimidation, was working out of the MIAC. The allegations in the second complaint are particularly serious. According to a statement the second accuser wrote when she applied for a temporary protection from abuse order against Minkowsky, he "intimidated" her into sex by "placing his gun and badge on the chair," claimed he was "above the law" and "can get away with anything" because of his job as a police officer. The woman also alleged that Minkowsky threatened to inform her abusive ex-husband about her current whereabouts. [54]

How did a disgraced officer, twice accused of abuse, come to work at the MIAC? Reflecting the MIAC's task force structure, Minkowsky is not employed by the State of Maine. He is employed by the New England High Intensity Drug Trafficking Area, a federal program that, among other initiatives, pays for specialized intelligence officers to work with state and local agencies. A spokesperson for the Department of Public Safety tried to deflect the controversy, noting that pre-employment vetting was the responsibility of the federal agency that employs him.[55] It is unclear whether DPS or the MIAC investigated these allegations.[56] According to Minkowsky's LinkedIn profile, he is still employed by HIDTA and still works out of the MIAC.[57]

These same dynamics also create opportunities to evade regulation. The ACLU named one aspect of this problem "policy shopping," a situation where fusion center personnel can "pick and choose from overlapping sets of laws so they can collect and use personal information as freely as possible while avoiding privacy laws, open-records acts, and civil liability."[58] This is precisely the issue at stake in Loder's claims regarding automated license plate readers. The MIAC allegedly circumvents Maine law regarding data retention by remotely accessing data from automated license plate readers in other states.[59]

The dismissal of the Loder suit on technical grounds also underscores the regulatory problems posed by interagency task forces. The MIAC operates in an organizational no-man's-land among federal, state, and local governments. The court could dismiss Loder's suit on a technicality precisely because of this ambiguous position. The court deemed that the MIAC was not a federal entity, undermining a legal complaint against the MIAC premised on the Federal Privacy Act. This problem is a structural issue with the institutional design of fusion centers. Addressing this problem means reckoning with the very concept of a fusion center. Indeed, some scholars and policy advocates contend that fusion centers are inherently

---

[54] Callie Ferguson, "Former cop accused twice of intimidation now works at Maine's controversial intelligence center," *Bangor Daily News*, May 12, 2021, https://bangordailynews.com/2021/05/12/mainefocus/former-cop-accused-twice-of-intimidation-now-works-at-maines-controversial-intelligence-center/

[55] Ibid.

[56] There has been no reporting following up on the initial story. The research team writing this report decided not to file Freedom of Access Act requests related to this story, as they would likely be denied to protect Minkowsky's privacy.

[57] James Minkowsky, LinkedIn, https://www.linkedin.com/in/james-minkowsky-85489a78.

[58] Mike German and Jay Stanley, "What's Wrong with Fusion Centers," American Civil Liberties Union, December 2007: http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf, 11.

[59] *Loder v. Me. Intel. Analysis Ctr.*, 2:20-cv-00157, 2021 WL 816470 at *7, *9 (D. Me. 2021), 10.

unaccountable, whether due to organizational complexity and or a deliberate design to evade privacy protections put in place in the 1970s.[60] For this reason, this shadow report renews the call to close the MIAC. Oversight and reform cannot fix fundamental design flaws.[61]

Mission and Operations

While fusion centers were created after 9-11 with an emphasis on terrorism, their scope quickly grew to an expansive "all-crimes, all-threats, all hazards" mission. This ill-defined mission makes fusion centers hard to evaluate and manage, a problem documented by the DHS Office of the Inspector General, the Congressional Research Service, and the Senate Permanent Committee on Investigations.[62]

In effect, the expansion to all-hazards was a practical matter and recognition that there is not enough political violence to justify the expansion of the national security apparatus down to the state and local level.[63] Monahan and Regan, in their survey of 36 fusion centers, find three "predictable" reasons for this expanding mission: "fusion centers have to be valuable to their states, there is too little activity that is clearly terrorism related, and fusion center personnel have to use their time and skills constructively."[64] In the face of practical political demands, fusion centers have become supplements to law enforcement.

Analysis of BlueLeaks documents from the MIAC confirms exactly this point. For a recently published peer-reviewed academic article, McQuade, Horne, Wehrwein, and Trujillo conducted a document analysis of MIAC records and a network analysis of MIAC email access logs. The findings clarify the substantive focus of MIAC and provide needed context to the public claims of the MIAC's leadership.[65] During debates over LD 1278, the MIAC director cited the disruption of a potential mass shooting, the prevention of potential suicide, and the location

---

[60] Brendan McQuade, *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*, (Oakland: University of California Press, 2019), 115-119; Torin Monahan and Priscilla Regan, "Zones of Opacity: Data Fusion in Post-9/11 Security Organizations," *Canadian Journal of Law and Society* 27 no. 3; Anthony Newkirk, "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance after 9/11." *Surveillance & Society*, 8 no. 1 (2010); Michael Price, "National Security and Local Police." The Brennan Center for Justice, December 10, 2013: https://www.brennancenter.org/publication/national-security-local-police, 17-20, 27-28,35-36.

[61] For more on the perils of reforming and regulating police surveillance, see: Shakeer Rahman and Brendan McQuade, "Police Bureaucracy and Abolition: Why Reforms Driven by Professionals will Renew State Oppression," *Counterpunch*, September 17, 2020, https://www.counterpunch.org/2020/09/17/police-bureaucracy-and-abolition-why-reforms-driven-by-professionals-will-renew-state-oppression/

[62] US Senate, Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, October 3, 2012, http://www.coburn.senate.gov/public/index.cfm/files/serve?File_id=693b820a-0493-405f-a8b5-0e3438cc9b24, 93-96;John Rollins, "Fusion centers: Issues and options for Congress," Library of Congress, Washington, DC, 2008: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA482006, 23;

[63] Brendan McQuade. *Pacifying the Homeland: Intelligence Fusion and Mass Supervision* (Oakland: University of California Press, 2019), 30-34.

[64] Priscilla Regan & Torn Monahan, "Beyond Counterterrorism: Data Sharing, Privacy and Organizational Histories of DHS Fusion Centers," *International Journal of E-Politics 4*, no. 3 (2013): 10.

[65]Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021)

of sex offenders as examples of the MIAC's work.[66] The document and network analysis shows that these selections, obviously chosen for their feel-good optics, do not accurately represent the work of the MIAC. Instead, the analysis of MIAC documents and email access logs show that the MIAC overwhelmingly focuses on property and drug crimes, neglecting other, arguably more harmful public safety issues like domestic violence and wage theft. The point here is not that the MIAC should be put to work to address issues but that the fusion center, despite its expansive "all hazards" mission, remains preoccupied with traditional concerns of policing: the conventional crimes associated with poverty and powerlessness.

During debates over LD 1278, the MIAC director cited the disruption of a potential mass shooting, the prevention of potential suicide, and the location of sex offender as examples of the MIAC's work. The document and network analysis shows that these selections, obviously chosen for their feel-good optics, ***do not accurately represent the work of the MIAC.*** *Instead, the analysis of MIAC documents and email access logs show that the MIAC overwhelmingly* ***focuses on property and drug crimes****, neglecting other, arguably more harmful public safety issues like domestic violence and wage theft. The point here is not that the MIAC should be put to work to address issues but that the fusion center, despite its expansive "all hazards" mission,* ***remains preoccupied with traditional concerns of policing: the conventional crimes associated with poverty and powerlessness.***

The majority of MIAC documents concern the sharing of criminal information. Two-thirds of the BlueLeaks documents definitely shared by the MIAC—939 of 1,382—are (1) requests to identify a suspect or a wanted person, locate a person of interest or missing person, or provide information about possible crimes or suspicious circumstances or (2) bulletins and reports on specific incidents, cases, or individuals considered relevant to law enforcement but not directly connected to a criminal investigation by a police agency in Maine. Add in the 147 cancellations and updates that follow up on requests for information, and nearly 80 percent of these documents concern the sharing of criminal information.[67]

The remaining 283 documents, either produced or clearly disseminated by the MIAC, are more substantial intelligence reports. The most detailed intelligence reports produced by the MIAC have a clear focus: drugs. The 2018 *Official State of Maine Threat Assessment* finds "no specific, credible intelligence to indicate a terrorist threat to the state of Maine" and concludes

[66] Michael Johnston, "Testimony of Lieutenant Michael Johnston, Maine State Police, in Opposition to of (LD 1278)" April 12, 2021, https://mainelegislature.org/legis/bills/getTestimonyDoc.asp?id=151607.
[67] BlueLeaks included 2883 unique documents hacked from the MIAC website. The dates range from June 2017 and June 2020. There are 1,382 documents either produced by Maine's fusion center or labeled "pass through," meaning that the MIAC shared the item with at least some of their 4,526 registered users. Over half of the total documents, 1,501, were produced by other local, state, federal, and private units but were not labeled "pass through," meaning other agencies shared the documents with Maine's fusion center but the MIAC did not necessarily disseminate them. Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021): 11.

"that heroin and opioids present the most significant near term drug threat to public health and public safety."[68] This finding is reflected in the focus of other MIAC intelligence reports: 20 reports titled "Maine Drug Monitoring Initiative" and 16 "Opioid Arrest Bulletins." The other major MIAC intelligence product is the COVID Daily Update. There are 100 of these reports—35 percent of the 283 analytic products included the MIAC's contribution to BlueLeaks. The rest of the documents produced by the MIAC mostly concern protest and political violence, which intelligence reports lump together as "civil unrest," "extremism," or "terrorism:" 27 were produced by the MIAC and 132 were "pass throughs" from other agencies. All told, the MIAC's intelligence reporting–and particularly its original analysis (as opposed to the reports from other agencies it disseminates as "pass throughs)"– is preoccupied with drug use. Remove the COVID reports from consideration, and over one-third of the intelligence reports produced or otherwise disseminated by the MIAC concern drugs.[69]

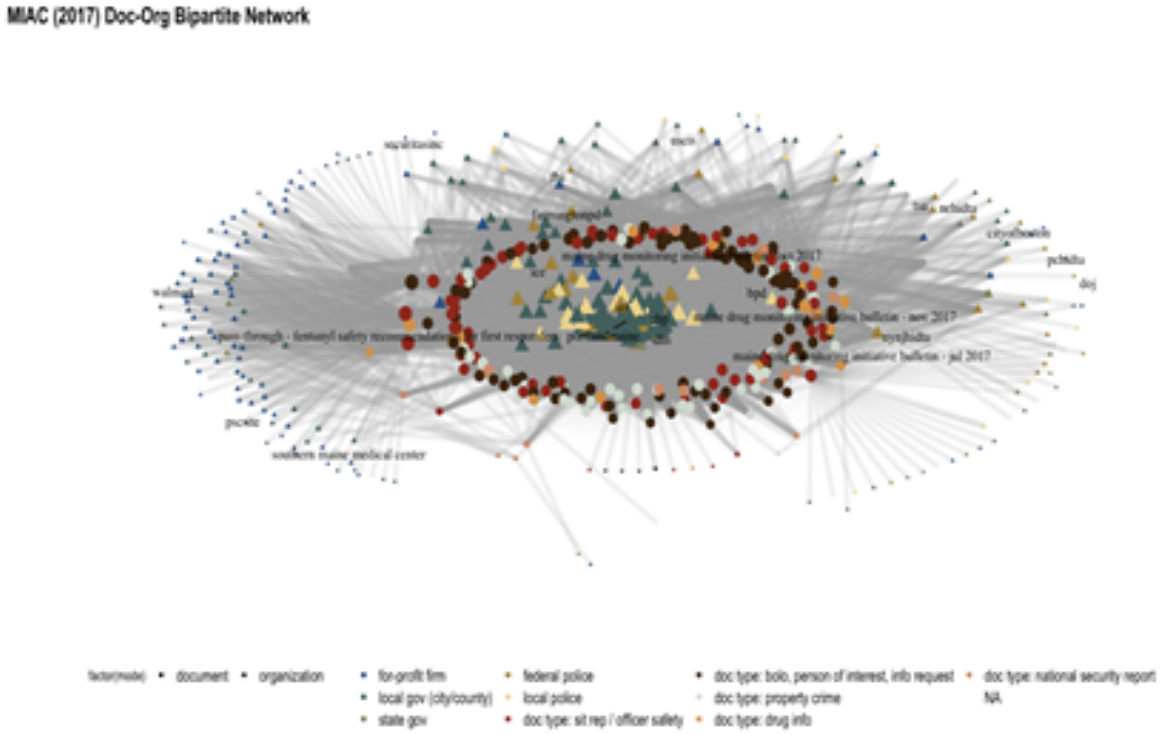
The network analysis of email access logs confirms the findings of the document analysis while also providing insight into the larger information sharing network that surrounds the MIAC. The email access logs provide the metadata about the intelligence products disseminated by the MIAC: the emails that download a given document and a timestamp for the download. By analyzing the types of documents different organizations accessed, we can understand their priorities and gain insight into police discretion: what behaviors and issues are viewed as security problems and by which institutions?

The MIAC's distribution list has a wide reach. As a result of BlueLeaks, we know that there were 4526 registered users of MIAC as of June 2020. This expansive list includes law enforcement officers and intelligence officials from across Maine, the New England Region, and across the country. It extends beyond law enforcement and intelligence to other government officials such as Department of Motor Vehicles personnel and school superintendents. The MIAC's reach extends outside of the public sector. Many large corporations receive MIAC products, including Avangrid, Hannaford's, ExxonMobile, and Bath Iron Works. Civil society organizations and nonprofits are also involved, such as universities, hospitals, and even special interest groups. The president of the Maine Chamber of Commerce, for example, is a registered user of the MIAC but, in contrast, there are no representatives from organized labor listed.[70]

Figure 1 below depicts the overall structure of the network.

[68] Maine Information and Analysis Center, "The Official State of Maine Threat Assessment, 2018," BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks, 2, 6.
[69] Ibid, 11-12.
[70] Dan Neumann, "Maine's police intelligence center sent reports on activists to corporations," *The Beacon*, July 16, 2020, https://mainebeacon.com/maines-police-intelligence-center-sent-reports-on-activists-to-corporations/

Figure 1: Network Analysis of MIAC Email Access Logs



Information does not flow uniformly. At the center of the network are a core of local and state government organizations that disproportionately read and disseminate documents. This list includes emails from the state government (Maine.gov) as well as many – but not all – of the most populous municipalities in the state. Bangor is notable for its absence. Other small municipalities like Penobscot, Ogunquit, and South Berwick download almost every MIAC product. Why do these tiny towns consume so much MIAC intelligence? McQuade, Horne, Wehrwein, and Trujillo conjectured that these are bored cops downloading “intelligence spam” that busier police in larger jurisdictions simply ignore.[71]

Many organizations from outside of Maine are connected to the MIAC network. The most prolific out-of-state readers of MIAC products are the Northern California Intelligence Center, State of Connecticut, the District of Columbia. They most frequently accessed documents on opioid arrestees and persons of interest who are suspects crossing state lines. The Department of Homeland Security and Customs and Border Protection are the two federal agencies whose officers most frequently downloaded documents from the MIAC. These officers frequently viewed opioid arrests and national security reports passed through from other intelligence operations. The role of Customs and Border Protection speaks to the fusion center’s role in the policing of undocumented people. There are a handful of documents in the BlueLeaks archive detailing undocumented people wanted to by Immigration and Customs Enforcement or Customs and Border Protection.[72]

[71] Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021): 12-16.
[72] Iib, 13

The substance of documents shows a preoccupation with property crime: 14 of the 15 most downloaded documents concern property crime. Domestic violence is largely ignored. The most central 'wanted poster' for a domestic assault circulated roughly as frequently as a wanted poster for someone who had stolen a rare coin collection. The silence on domestic violence is a damning reflection of the priorities of law enforcement. Maine has one of the lowest crime rates in the United States. In recent years, the state records about 20 homicides annually, and over half are connected to domestic violence situations. The MIAC ignores what is arguably the most pressing public safety issue in the state in favor of property crime.[73]

Private firms also access documents. The most prolific private sector reader of MIAC reports is the Auburn Mall. Auburn, along with neighboring Lewiston, are the twin cities of Maine. They are post-industrial mill towns, which have not yet been gentrified. They contain the four highest poverty census tracts in the state. The opioid epidemic has devastated this region. Mall security at the Auburn Mall mostly reads documents on persons who have been arrested for opioid use and shoplifting. [74]

In this regard, the MIAC's "all crimes, all threats, all hazards" mission practically translates into supercharged policing. The MIAC gives police in Maine more resources to chase the familiar targets of law enforcement. In a state with one of the lowest crime rates in the country, the most common targets are property crime and drug use. Moreover, the MIAC operations display the same discretionary focus on certain crimes that characterizes most law enforcement. The low priority the MIAC places on domestic violence is indicative of a larger trend in law enforcement, where police agencies tend to underreport, neglect, and even ignore crimes against women.[75]

Similarly, the MIAC, like police in general, focuses on the crimes of the powerless: the violent, property, and drug crimes that dominate conventional discussions of crime. There is no evidence in BlueLeaks that MIAC focuses on white-collar crime of any kind, which, in fact, is more harmful to society than conventional crime. The costs of wage theft, to consider just one kind of white-collar crime, are greater than all property crimes combined. Recent studies of wage theft in the United States concluded that the total nationwide losses of wage theft dwarf those of property crimes. In 2014, for example, Employers stole an estimated $50 billion in wages from their workers, more than the $14 billion in losses from all reported property crimes.[76] Indeed, the Maine Department of Labor recently recovered nearly half a million dollars in back wages and issued citations to 29 different employers.[77]

---

[73] Ibid, 19
[74] Ibid, 13, 16.
[75] Michele R Decker, Charvonne N. Holliday, Zaynab Hameeduddin, Roma Shah, Janice Miller, Joyce Dantzler, and Leigh Goodmark, ""You do not think of me as a human being": Race and gender inequities intersect to discourage police reporting of violence against women." *Journal of Urban Health* 96, no. 5 (2019).
[76] Brady Meixell and Ross Eisenbrey, "An Epidemic of Wage Theft is Costing Workers Hundreds of Millions of Dollars a Year," *The Economic Policy Institute*, September 11, 2014, https://www.epi.org/publication/epidemic-wage-theft-costing-workers-hundreds/; see also: David Cooper and Teresa Kroegerm, " Employers steal billions from workers' paychecks each year." *Economic Policy Institute*, May 10, 2017, https://www.epi.org/publication/employers-steal-billions-from-workers-paychecks-each-year/
[77] "Maine Dept. of Labor Announces Recovery of Nearly $500,000 in Owed Back Wages for Maine Workers in 2021." Maine Department of Labor, January 25, 2022, https://www.maine.gov/labor/news_events/article.shtml?id=6595476

The problems posed by MIAC, then, are not just the fact of surveillance and related concerns about privacy but also the structural bias of law enforcement: the overcriminalization of the crimes of the powerless and an undercriminalization of crimes of the powerful. This structural bias is also racialized. The racial biases of the criminal legal system in the United States are well documented. The criminal legal system in the United States is shaped by racialized structural inequalities and animated by anti-black racism. As Michelle Alexander's breakthrough study puts it, mass incarceration is the new Jim Crow.[78]

The problems posed by MIAC, then, are not just the fact of surveillance and related concerns about privacy but also the structural bias of law enforcement: the ***overcriminalization of the crimes of the powerless and an undercriminalization of crimes of the powerful.*** *This structural bias is also racialized.*

Maine is not exempt from this issue. In 2019, The Council on State Government conducted a comprehensive study for the Maine Commission to Improve the Sentencing, Supervision, Incarceration, and Management of Prisoners. They reviewed ten years of arrest records, court filings, and prison and probation admissions. They found that black people are overrepresented in Maine's prisons: one percent of the population is black, but 11 percent of incarcerated people in Maine are black. What's more, black people in the state's carceral system are sentenced disproportionately more when compared to white people. That disproportionality is more pronounced for more serious crimes that bear harsher punishments: black people account for 21 percent of class-A felony drug arrests (aggravated trafficking) and 15 percent of class-B felony drug arrests (trafficking).[79]

The impression left by the BlueLeaks documents supports these findings, although inconsistencies in bulletins make a systematic analysis impossible. Not all documents specify the race of individuals detailed in various bulletins. Often a picture and name are the only demographic information provided. Since race is a matter of self-identification, it would have been inappropriate to impute race by other data points such as last name or skin color. While the data does not allow for precise analysis on questions of race, the analysis of MIAC documents and email access logs shows a clear pattern and a hyper-focus on the crimes of the powerless.

---

[78] MIchelle Alexander. *The New Jim Crow: Mass Incarceration in the Age of Colorblindness* (New York: The Free Press, 2012); see also: Loïc Wacquant, *Deadly Symbiosis: Race and the Rise of the Penal State* (Malden: Polity, 2009); Loïc Wacquant, *Punishing the Poor: The Neoliberal Government of Social Insecurity* (Durham: Duke University Press Books, 2009); Bruce Western, *Punishment and Inequality in America* (New York: Russell Sage Foundation, 2006).

[79] Ben Shelor, Jessica Gonzales-Brickner and Carl Reynolds, *Justice Reinvestment in Maine*. Justice Center of the Council on State Governments, December 11, 2019, https://csgjusticecenter.org/publications/justice-reinvestment-in-maine-third-presentation/

Bias and Disinformation in MIAC Civil Unrest Reports

The structural biases of law enforcement that are baked into the MIAC's mission and operations are also complemented by a more explicit political bias in the MIAC's intelligence bulletins. When the news of BlueLeaks broke in Maine, much of the discussion centered on a series of "Civil Unrest Daily Reports" on the racial justice protests in the summer of 2020. These MIAC bulletins laundered right-wing conspiracies about paid protesters and bricks pre-staged at protests for rioting as intelligence. They exemplify the shoddy and unprofessional work for which fusion centers are now known.[80]

In terms of fusion centers, these "Civil Unrest Daily Reports" were situational awareness reports. They were not part of an investigation. No informants were involved. Fusion center analysts gathered open-source data and intelligence reports from other agencies in order to brief law enforcement on the public safety issues presented by the protests. In this case, however, situational awareness meant sharing unsupported and easily disproved claims.

The June 5, 2020 civil unrest reports warned that "unidentified individuals discussed various websites for payment to agitate and commit violent acts."[81] To support this claim, the report cited a bulletin from the San Antonio Division of the FBI that detailed two websites "used to facilitate payments to violent agitators." Nathan Bernard and Caleb Horton, independent journalists, followed this lead, eventually publishing their findings in a long-form exposé in *The Mainer*. They found that two websites referenced in the report, crowdsondemand.com and protestjobs.com, were in no way providing "payment to agitate and commit violent acts." Crowds on Demand is a Beverly Hills-based public-relations firm that provides paid participants for corporate and media events. Protest Jobs is a satirical website created in 2017 to mock conspiracies about paid protests.[82]

It appears that this disinformation started to spread on far-right social media before reaching the FBI and, from there, the national network of fusion centers and the MIAC. Protest Jobs had been dormant for years until the racial justice protests during the summer of 2020 caused the website to go viral in far-right Facebook groups. Facebook users shared posts about the site over 30,000 times, generating upwards of a million visits to Protest Jobs. This attention led Snopes, a fact-checking website, to publish a story debunking claims that protestjobs.com is a real business on May 31, 2020. The next day, the creator of Protest Jobs added a prominent disclaimer that read: "REAL: 120,000+ AMERICANS ARE DEAD. FAKE: THIS WEBSITE. REAL: TRUMP IS A FAILURE." Then on June 3, Reuters published another article debunking

---

[80] Maine Information and Analysis Center, "Civil Unrest Daily Report," June 2, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 3, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
Maine Information and Analysis Center, "Civil Unrest Daily Report," June 4, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 5, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[81] Maine Information and Analysis Center, "Civil Unrest Daily Report," June 5, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[82] Nathan Bernard and Caleb Horton, "Teenager or Terrorist?" *The Mainer,* July 29, 2020, https://mainernews.com/teenager-or-terrorist/; David Mikkelson, Is ProtestJobs.com a Real Service for Hiring Protesters?" *Snopes*, May 31, 2020, https://www.snopes.com/fact-check/protestjobs-hiring-service/; Reuters "Fact check: Satirical website ProtestJobs.com take seriously.:" Reuters, June 3, 2020, https://www.reuters.com/article/uk-factcheck-protestjobs-idUSKBN23A32M.

claims that protestjobs.com was a real business.[83] On June 5, the MIAC shared this disinformation with law enforcement in Maine without, apparently, taking a moment to visit the website and see the disclaimer or perform a simple internet search that would have provided the two articles debunking the claim.

This was not the only disinformation shared by the MIAC as “intelligence” on the racial justice protests in the summer of 2020. All the“Civil Unrest Daily Reports” warn of "Possible pre-staging of bricks for access during Maine-based protests." [84] These reports provide two different sources for these claims. The first source is a document from the FBI’s field office in Boston, which states, “FBI Boston received a screenshot from the Facebook page…[that]… stated that there are rumors of stacks of bricks and stones that have been placed strategically throughout protests. The post indicated that ‘we think this is all part of the big plan.’”[85]

Again, Bernard and Horton did the basic fact-checking that MIAC personnel neglected to do. They found that the Facebook page cited in the FBI document is owned by a pro-Trump biker who refers to himself as “the Wolfmannn.” On Facebook, “the Wolfmannn” criticized efforts to limit the spread of COVID as part of a tyrannical conspiracy to strip Americans of their rights. He promoted a protest at the home of Massachusetts Governor Charlie Baker. The demonstration was co-sponsored by Super Happy Fun America, a hate group that organized the Boston Straight Pride Parade last year, and a rally at Boston Police headquarters in support of Immigration and Customs Enforcement crackdowns on immigrants. Super Happy Fun America is alleged to be a front for the white-nationalist group Resist Marxism.[86]

The other source for the claim about “pre-staged bricks” was an “Open Source Intelligence Report” from the DHS Office of Intelligence and Analysis. This report cited a post from a Twitter account called Marlene45MAGA. Again, Bernard and Horton investigated these claims, finding compelling reasons to question the quality of the source:

> A scroll through Marlene45MAGA’s Twitter feed reveals a cesspool of racist, pro-Trump, COVID-conspiracy rantings similar to the posts and comments on the Wolfmannn’s page. The account almost exclusively re-tweets other posts, at all hours of the day and night; it has over 51,000 followers and is “following” nearly 49,000 other users — strong indications that its function is purely political and at least partly automated. Yet this anonymous, bot-like account was also treated by MIAC as a credible source of intelligence about potential violence at Black Lives Matter protests. [87]

---

[83] Nathan Bernard and Caleb Horton, “Teenager or Terrorist?” *The Mainer,* July 29, 2020, https://mainernews.com/teenager-or-terrorist/

[84] Maine Information and Analysis Center, “Civil Unrest Daily Report,” June 2, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, “Civil Unrest Daily Report,” June 3, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
Maine Information and Analysis Center, “Civil Unrest Daily Report,” June 4, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, “Civil Unrest Daily Report,” June 5, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[85] Nathan Bernard and Caleb Horton, “Teenager or Terrorist?” *The Mainer,* July 29, 2020, https://mainernews.com/teenager-or-terrorist/

[86] Ibid

[87] Ibid

These were not the only dubious sources cited by the MIAC to support claims that the demonstrations were violent and uniquely threatening to law enforcement. Bernard and Horton also found other obviously satirical social media posts that the MIAC interpreted as evidence of imminent danger, including "a similarly farcical incident involv[ing] the claim that a 19-year-old was training terrorists via a comedy video she posted on the social media platform TikTok."[88]

When asked about these sources, the Maine State Police Major, who at the time oversaw administrative functions at the center, explained that when reports of suspicious activity are sent to MIAC, "we are certainly considering the source and veracity of the source…Sometimes we can independently verify that, other times we take it at face value. If we set as a threshold that we are going to independently verify every piece of information that goes out, then we would be sharing almost no information." In response to the allegation of pre-staged bricks, the major said, "we don't need to verify that, it's not important." Wolfmannn and Marlene4MAGA did not describe a specific threat but rather a general tactic allegedly used by violent agitators. "This type of information, even if unconfirmed, is useful because it enhances local cops' "situational awareness," he said. "Now law enforcement prepares for that. They can work with others to be prepared for bricks, and other weapons."[89]

These reports alone should be a major scandal but have been largely ignored. This lack of response presents a stark contrast to the decisive action taken by the Department of Public Safety in response to a lesser, similar scandal. In January 2021, a public controversy erupted around Maine Capitol Police Chief Russle Gauvin, now retired, after *The Mainer* reported that he shared right-wing conspiracy theories about the COVID-19 pandemic and 2020 election.[90] This story resonated widely because it broke in the immediate aftermath of the insurrection at the US capitol on January 6, 2021. In response to the scandal, DPS placed Gauvin on administrative leave. After three months of investigation, the state reached a separation agreement with Gauvin, who then retired.[91]

The contrast between these two scandals is hard to square. Why was Gauvin forced to retire just for sharing right-wing conspiracy theories on social media, while the MIAC has faced no consequences for laundering similar conspiracy theories as verified intelligence and sharing them with law enforcement throughout the state?

Governance and Privacy Issues

In theory, the MIAC's internal policies should guard against the kind of shoddy work seen in the Civil Unrest Daily Reports. However, a careful review shows that the MIAC has violated its own privacy policy and cannot be trusted to police itself. The mission of the MIAC, as stated in their official Privacy Policy, is to "seek, acquire, and receive information, analyze such

---

[88] Ibid
[89] Ibid
[90] Nathan Bernard, "Chief of Maine's Capitol Police Radicalized by Far-Right Conspiracies," *The Mainer,* January 15, 2021, https://mainernews.com/chief-of-maines-capitol-police-radicalized-by-far-right-conspiracies/
[91] Gillian Graham and Eric Russell, "Maine Capitol Police chief steps down after outcry over social media posts," *The Portland Press Herald*, April 30, 2021, https://www.pressherald.com/2021/04/30/capitol-police-chief-steps-down-after-outcry-over-social-media-posts/

information, and, when *lawful and appropriate*, retain and disseminate such information to individuals and agencies *permitted access* to the information.[92] The very first guiding principle of the MIAC is that "[i]n carrying out its work, the MIAC shall: *[p]rotect privacy, civil rights, civil liberties, and other protected interests of all individuals*."[93] The policy explicitly states that law enforcement intelligence gathering and monitoring of activities that involve Freedom of Speech, Freedom of the Press, and Freedom of Assembly must be based on whether criminal activity and/or suspicious activity has or is occurring as shown by specific, articulable facts.[94]

Our analysis of the MIAC's Governance Structure and Privacy Audit procedures and a related review of BlueLeaks documents reveals that the MIAC fails to adhere to its own explicitly stated mission, guiding principles, and legal standards. It collects and maintains information that violates individuals' fundamental civil rights in the absence of specific, articulable facts related to criminal or suspicious activity. It fails to protect the privacy of individuals swept up in its indiscriminate dragnet.

Governance

MIAC's Governance structure consists of four key roles, as outlined in Figure 2 below. The structure combines four specific roles (Director, Privacy Officer, Compliance Officer, and Security Officer) with an Advisory Board. However, two of the roles (Compliance Officer and Security Officer) are held by the same individual, the MIAC Sergeant. The other two roles are held by the MIAC Lieutenant and the MIAC Staff Attorney, respectively. As a result, some members of the Advisory Board are the only individuals involved in the governance structure of the MIAC who are not also involved in its operations.

Figure 2 - MIAC Governance Structure

Role	Key Responsibilities	Individual(s)
MIAC Director	● Primary operational oversight ● Personnel and technology oversight ● Enforcing the privacy policy, including assessing the quality of and destroying information maintained by MIAC	MIAC Lieutenant
MIAC Privacy Officer	● Ensuring that privacy, civil rights, and civil liberties are protected as provided in the Privacy Policy ● Receiving and responding to inquiries about privacy, civil rights, and civil liberties ● Recommending updates to the Privacy Policy every year in response to the results of audits	Maine State Police Staff Attorney

[92] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pdf, 2.
[93] Ibid
[94] Ibid n.1.

MIAC Compliance Officer	● Conducting Privacy Audits every year ● Privacy training, business process, and technology system changes to ● Investigating suspected or known misuse of information or violations of the policy	MIAC Sergeant
MIAC Security Officer	● Maintaining a record of all training ● Determining whether a data breach has occurred and managing notifications as needed ● Maintaining a record of all audits	MIAC Sergeant
MIAC Advisory Board	● Responsible for reviewing new and revised written MIAC privacy policies	Various Members, nearly all of whom are unelected public officials, and two of whom are members of the public.[95]

However, the Advisory Board is made of individuals who are largely unaccountable to the public at large or who lack the necessary expertise to provide meaningful oversight. The colonel of the Maine State Police or his designee, in consultation with the director of the Maine Emergency Management Agency, appoints advisory board members. The board contains numerous public officials, none of whom are elected. Additionally, the board contains two Public Members serving in a private capacity. The first is a litigation attorney from Bangor, ME, who specializes in estate planning and criminal defense and does not list privacy or intelligence as areas of expertise,[96] and the second is a real estate agent from Brunswick, ME, with no experience in privacy or intelligence.[97] The director of security for CMP, Bruce Lewis, once sat on the Advisory Board but stepped down after his post became controversial in light of the allegations in the whistleblower complaint that the MIAC passed intelligence on the Say No to the New England Clean Energy Corridor campaign to the utility.[98] While MIAC leadership denied that Lewis's departure from the Advisory Board was related to the allegations at a July 30, 2020 open house meeting held at the MIAC for journalists, legislators, and members of the public, the timing of the move speaks for itself.

---

[95] "About the MIAC, Maine State Police, 2019, https://www.maine.gov/dps/msp/specialty-units/MIAC/About

[96] Tracy B. Collins, Senior Associate, Rundman Winchell, 2022, https://www.rudmanwinchell.com/attorneys/tracy-b-collins/

[97] Matt Byrne, "Stolen documents show Maine police unit shifted focus from terrorism to routine crimes," *The Portland Press Herald*, July 12, 2020, https://www.pressherald.com/2020/07/12/stolen-documents-show-maine-police-unit-shifted-focus-from-terrorism-to-routine-crimes/

[98] Megan Gray, "Hack included documents from secretive Maine police unit," *The Portland Press Herald,* June 27, 2020, https://www.pressherald.com/2020/06/26/hack-included-documents-from-secretive-maine-police-unit/

A review of the Advisory Board's minutes from the October 4, 2021 meeting provides evidence that even the Board itself has recognized a need for more independent oversight.[99] During the meeting, Major Brian Scott of the Maine Police asked "[s]hould we fill [the Privacy Officer position] with someone from the Maine Police?" and suggested instead that the Board consider "someone outside" with a "neutral[,] objective viewpoint" in order to promote "transparency and legitimacy."[100] However, the current MIAC Privacy Officer continues to be the Staff Attorney for the Maine State Police.[101]

MIAC's Privacy Policy

MIAC's Privacy Policy, which was last updated in March 2019, prior to the murder of George Floyd, the subsequent protests, and BlueLeaks, applies to all MIAC personnel, participating agency personnel, IT services support personnel, and contractors, and requires that all such personnel "shall protect individuals' rights as guaranteed by the United States of America and Maine Constitutions and other applicable laws protecting privacy, civil rights, and civil liberties."[102] The policy itself claims that the MIAC's policies are in compliance with numerous Federal and State laws, including the Civil Rights Act of 1964, the Americans with Disabilities Act, the Civil Rights of Institutionalized Persons Act, the Health Insurance Portability and Accountability Act, the Maine Criminal History Record Information Act (16 M.R.S. c.7), the Maine Intelligence and Investigative Record Information Act (16 M.R.S. c.9), and others; however, the recent whistleblower lawsuit in the Federal District of Maine alleged that the MIAC's practices, in fact, violate a number of these Federal and State laws.[103]

Limitations on Information-gathering by MIAC: According to the policy, the MIAC can only "seek, acquire, retain, or share information" that meets the criteria outlined in Figure 3. Some of these criteria provide little to no actual limitation to the MIAC's information gathering and retention capabilities. For example, the MIAC may, under its policy, acquire and retain information that is unrelated to a specific criminal or public safety threat, as long as it determines that such information is "useful" in the "administration of criminal justice and public

[99] Maine Information and Analysis Center Advisory Board Meeting Minutes, October 4, 2020, Maine State Police, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/2021%20Oct%20Minutes%20MIAC%20Advisory%20Board%20Meeting%20Minutes%20Final.docx.pdf

[100] Ibid.

[101] Minutes from the March, 2022 MIAC Advisory Board meeting indicate that there is an open position posted for MIAC Privacy Officer, and that the role may be filled in the short-term by a member of the Attorney General's staff; however, we were not able to verify this information through public records prior to the report's publication. Maine Information and Analysis Center Advisory Board Meeting Minutes, March 3 2022, Maine State Police, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Advisory%20Board%20Meeting%20Agenda%20and%20Minutes%20March%202022.docx.pdf

[102] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pdf, 5.

[103] *Loder*, 2021 WL 816470, at *3 (dismissing the relevant counts upon a Fed. R. Civ. P. 12(b)(6) motion, and thus counsel for the MIAC did not specifically admit or deny any of the whistleblower's alleged violations)

safety." The policy provides no definitions or standards for determining when information is useful in the administration of public safety.[104]

Much of the intelligence-gathering done by the MIAC and other fusion centers occurs under the rubric of "situational awareness," which is defined Chapter 6 § 321d of the United States Code as "information gathered from a variety of sources that, when communicated to emergency managers, decision-makers, and other appropriate officials, can form the basis for incident management decisionmaking and steady-state activity." This broad definition allows the MIAC boundless discretion to monitor everyone from people that use (but do not traffic) drugs to unhoused people with mental illness to seemingly random social media users to protesters of all kinds.

Requirements on Information Sources: Additionally, the policy requires that the information collected by MIAC come from a reliable and verifiable source, or, where the source may not be reliable and verifiable, that the limitations on the quality of the information be clearly identified in the record, and that the source of the information be appropriately documented. As discussed below in a review of a MIAC Privacy Audit, there is circumstantial evidence from its own internal analysis that MIAC is violating this requirement.[105]

Moreover, the BlueLeaks records provide countless examples of the MIAC's failure to follow this point. The closest the MIAC comes to addressing the quality of information it disseminates is the official disclaimer included on all MIAC bulletins: "DATA CONTAINED IN THIS RECORD SHOULD BE INDEPENDENTLY VERIFIED." Simply put, the MIAC does not stand behind the quality of its work and provides no guarantee that the information it shares is accurate. Case in point: the aforementioned Civil Unrest Daily Reports, which show the collection and dissemination of misinformation, sourced from Facebook posts by individuals with no connection to law enforcement, without any indication as to the reliability of the source of the information.[106] This incident is evidence that MIAC is violating its own policies.

Information on Political Participation and Beliefs: One aspect of the information released by BlueLeaks, which generated significant public and media concern, in particular, was the evidence that the MIAC both collected and disseminated information related to planned protests, by both left-leaning and right-leaning organizations, without any indication of criminal conduct or a possible threat.[107] The acquisition and dissemination of this information is a direct

---

[104] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pdf, 6.

[105] Ibid, 6.

[106] Maine Information and Analysis Center, "Civil Unrest Daily Report," June 2, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 3, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;Maine Information and Analysis Center, "Civil Unrest Daily Report," June 4, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 5, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[107]Maine Information and Analysis Center, "Civil Unrest Daily Report," June 2, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 3, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;Maine Information and Analysis Center, "Civil Unrest Daily Report," June 4, 2020 BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Daily Report," June 5, 2020 BlueLeaks, Distributed Denial

violation of MIAC's own policy, which states that the MIAC "shall not intentionally seek, acquire, retain or share information about individuals or organizations solely on the basis of their religious, political, or social views or activities" or "their participation in a particular non-criminal organization or event."[108] Moreover, the acquisition and dissemination of this information is likely a direct violation of 28 C.F.R. § 23.20(b).[109]

Even members of the MIAC Advisory Board have indicated that they do not believe the MIAC should collect and retain information based on their political beliefs alone. In the minutes to the Advisory Board's December 2020 meeting, the MIAC Privacy Officer expressed concern, with respect to "sovereign citizens," about the "collection of information on people based on their beliefs - in this case, their beliefs regarding the authority of government agencies and officials."[110] Indeed, the Blueleaks archive includes four MIAC bulletins on individuals identified as Sovereign Citizens and one more detailing behaviors associated with the movement.[111] While it is encouraging to see this concern discussed, it is inexplicable that the MIAC Privacy Officer would not raise similar concerns about the MIAC's reporting on 2020 racial justice protests. After all, this privacy audit occurred after the publication of BlueLeaks and the subsequent criticism of the MIAC's monitoring of these protests. Instead, the meeting minutes give the impression that the MIAC Privacy officer is more concerned about violating the civil rights and liberties of "sovereign citizens," a group whose political beliefs by definition require the violation of numerous Federal and state laws, than violating the civil rights of individuals attending a Black Lives Matter protest.[112] This selective concern underscores the need for independent oversight. Even when the press has done its duty and brought a troubling issue to public attention, the MIAC's Advisory Board ignores it in favor of more quixotic concerns.

---

of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Maine Information and Analysis Center, "Civil Unrest Situation Report," January 15, 2021; Maine Information and Analysis Center, "Civil Unrest Situation Report," January 19, 2021

[108] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pdf, 6.

[109] 28 C.F.R. § 23(b) provides that "[an intelligence project] shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity." 28 C.F.R. § 23(b) (1998).

[110]Maine Information and Analysis Center Advisory Board Meeting Minutes, December 2, 2020, Maine State Police,https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Advisory%20Board%20Agenda%20and%20Notes%20from%2012022020.pdf, 6.

[111] The Maine Information and Analysis Center, "Situational Awareness (MIAC-2018-0144)," February 13, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; The Maine Information and Analysis Center, "Situational Awareness (MIAC-2019-0343)," February 11, 2019, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; The Maine Information and Analysis Center, "Situational Awareness (MIAC-2019-1104)," May 20, 2019,, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; The Maine Information and Analysis Center, "Situational Awareness (MIAC-2020-01753)," July 12, 2020, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; The Maine Information and Analysis Center, "Situational Awareness (MIAC-2020-0173)," January 27, 2020, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[112] "Sovereign Citizens Movement," Southern Policy Law Center, undated, https://www.splcenter.org/fighting-hate/extremist-files/ideology/sovereign-citizens-movement

Restrictions on Access and Dissemination: MIAC's policy requires that the MIAC label information added to its system "to the maximum extent feasible and reasonable, and pursuant to applicable limitations on access and sensitivity of disclosure, in order to . . . [p]rotect individuals' right of privacy and their civil rights and civil liberties" and "[p]rotect legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter."[113]

Records released as part of BlueLeaks provide direct evidence that the MIAC has violated its own policy by disseminating unnecessary information about individuals' past or current history of mental health treatment. For example, an August 2018 "Situational Awareness" bulletin on an individual with "possible mental health concerns" notes that the individual "was taken to St. Mary's hospital for evaluation."[114] These types of disclosures are common in MIAC reports. An "Officer Safety" bulletin on a "Transient Maine (ME) resident with history of mental health issues" divulges the individual's "history of crisis evaluations and psychiatric hospitalization."[115] Two other documents on missing juveniles violate the MIAC's privacy policy by providing inappropriate detail about mental health treatment. An April 2019 "Attempt to Locate" bulletin requests assistance "locating a female juvenile that has recently run-away from the Sweetser Behavior Health Crisis Unit."[116] Similarly, an April 2020 "Missing Person" report seeks information "on the whereabouts of two missing teenage girls from a behavior health facility in the Central Maine area."[117]

Sourcing Information from Commercial Databases: the privacy policy requires that the MIAC comply with all applicable laws when acquiring and retaining records from a nongovernmental information provider or a commercial database. Further, the policy prohibits MIAC from acquiring or retaining information from such external sources when it knows or has reason to believe that the provider or database: (1) is legally prohibited from acquiring or disclosing the information; (2) uses methods that the MIAC cannot use; or (3) has acquired information that the MIAC could not legally acquire.

Documents received in response to FOAA requests provide evidence that the MIAC currently uses commercial databases as part of its investigations. For example, one heavily redacted record shows a TransUnion report on a redacted individual, which provides information on jobs, emails, usernames, aliases, and numerous social media profiles and internet sites.[118] Another document traces a case that begins with a citizen report of "violent politically motivated rhetoric on Facebook" and leads immediately to a request to "begin to look into this individual" by a MIAC staffer. A case number and record are then created, and multiple reports are

---

[113] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pdf, 7.
[114] The Maine Information and Analysis Center, "Situational Awareness (MIAC-2018-1510)," August 9, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
[115] The Maine Information and Analysis Center, "Officer Safety (MIAC-2018-2019)," October 23, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
[116] The Maine Information and Analysis Center, "Attempt to Locate (MIAC-2018-0786)," August 4, 2019, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
[117] The Maine Information and Analysis Center, "Situational Awareness (MIAC-2020-0712)," April 7, 2020, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;
[118] TransUnion, 0177-0181, undated.

completed, including a "TLO (Comprehensive and Social Media)" report, which most likely refers to the TransUnion TLOxp product.[119] The document also contains the report itself, which includes information on bankruptcies, liens, properties, corporate affiliations, and other information which is fully redacted and cannot be identified. It is unclear why information of this type would be relevant for investigating violent political speech on social media, which surfaces questions as to whether MIAC's use of commercial databases violates its own privacy policy by allowing it to acquire information that it cannot legally acquire by itself.

The heavily redacted nature of the documents makes it impossible to determine if the MIAC's use of commercial databases violates its own policy and/or Federal or State privacy laws. As with now strictly regulated facial recognition technology, these private data brokers raise existential threats to privacy and other basic rights. There is currently no oversight or transparency mechanisms that govern the MIAC's use of technology.

Investigative Techniques: MIAC's policy requires that any investigative techniques used be in compliance with 28 C.F.R. Part 23, Federal and state constitutional provisions, and Maine statutes and regulations. 28 C.F.R. Part 23 regulates criminal intelligence systems, providing clear limitations on the operation of such systems. MIAC is a criminal intelligence system subject to the regulations. 28 C.F.R. § 23.20(a) in particular requires that the MIAC "shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." The Cellebrite case discussed below provides clear evidence that the MIAC is in violation of 28 C.F.R. § 23.20(a), because it has acquired and maintained information which is in no way "relevant to the identification of and the criminal activity engaged in by an individual who . . . is reasonably suspected of involvement in criminal activity," and there is no indication that the MIAC has made efforts to permanently delete this information from its records, in accordance with both the regulation and with its own stated policy.[120]

Destruction of Information: The limitations outlined in Figure 3 also restrict MIAC's ability to retain information; thus, unless the MIAC can justify ongoing retention of information under one of the bases outlined in Figure 3, it must destroy the information. Although MIAC's Privacy Policy indicates that MIAC "may retain information that is based on a level of suspicion that is less than 'reasonable suspicion,' such as tips and leads or [Suspicious Activity Report] information," such retention is prohibited by 28 C.F.R. § 23.20(a) as discussed above. Documents released by BlueLeaks show that MIAC has failed to destroy information in accordance with its policy. Loder's whistleblower complaint filed against the MIAC alleges that:

> MIAC routinely monitors social media accounts and/or conducts background checks on individuals associated with lawful public protests, frequently citing a pretextual criminal offense (subjects may litter during the protest, for example) to

[119]Reporting has revealed that TransUnion's TLO product is used by intelligence fusion centers, although BlueLeaks may be the first public confirmation of MIAC's use of TransUnion products. American Friends Service Committee, "Transunion," Investigate.afsc.org, September 8, 2021, https://investigate.afsc.org/company/transunion

[120] Maine Information and Analysis Center, *Privacy Policy*, Maine State Police, March 20, 2019, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Policy_0.pd, 30.

justify the collection. MIAC then retains all the data collected even after finding no indication of a threat, hazard, or criminal activity.[121]

Additionally, the Cellebrite case discussed below provides further evidence that MIAC is violating its own policy and Federal regulation by failing to discern between criminal intelligence information and other information and subsequently failing to remove information that is not relevant to the identification of criminal activity.

MIAC's own Advisory Board has recognized that the MIAC is not doing enough to ensure the destruction of information where relevant. The MIAC Privacy/Civil Liberties/Civil Rights Audit Report for the first half of 2020, released in Dec. 2020, indicates that the audit team surfaced issues related to the "length of retention of information," especially that concerning Juveniles, for further discussion by the Advisory Board.[122] The Audit Report for the second half of 2020 specifically asked the question of "[w]hether, once a First Amendment-protected has occurred, and if no criminal activity occurred during the event, ascertained information about the event should be deleted from the Activity Report" as one of the "Points of Discussion for Further Discussion with the Advisory Board."[123] In the October 2021 Advisory Board meeting, the MIAC Privacy Officer introduced a concern around the retention of information for longer than is necessary, and while some board members agreed, others indicated that the MIAC should maintain all records, however minor, in archives–a practice which would certainly violate MIAC's privacy policy.[124]

Although information retention has surfaced as an issue during both audits and Advisory Board meetings, it is not clear from the publicly-released files that the MIAC has established clear guidelines. The absence of clear guidelines for information destruction and disposition violates MIAC's Privacy Policy, 28 C.F.R. § 23, Maine State law, and the federal Privacy Act, 5 U.S.C. § 552a.[125]

---

[121] Complaint and Demand for Jury Trial, *supra* note 1, ¶ 59.
[122] Maine Information and Analysis Center, *Privacy/Civil Liberties/Civil Rights Audit Report for the Period 15 01 January 2020 - 15 July 2020*, Maine State Police, December 2, 2020, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20Privacy%20Audit%202020%20Part%201.pdf, 3.
[123]Maine Information and Analysis Center, *Privacy/Civil Liberties/Civil Rights Audit Report for the Period 15 Jul 2020 - 31 Dec 2020*, Maine State Police, undated, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/210708%20%20Fourth%20MIAC%20PCLCR%20Audit%20Full%20Report%20%2B%20Attachments.pdf, 3.
[124] Maine Information and Analysis Center Advisory Board Meeting Minutes, October 4, 2020, Maine State Police, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/2021%20Oct%20Minutes%20MIAC%20Advisory%20Board%20Meeting%20Minutes%20Final.docx.pdf
[125] Complaint and Demand for Jury Trial, *supra* note 1, ¶¶ 137, 144, 153-55

Figure 3 - Limitations on when the MIAC can seek, acquire, retain or share information

Based on criminal predicate or possible threat to public safety	**OR**	Based on reasonable suspicion that an identifiable individual or organization has committed or is planning criminal conduct and the information is relevant to such conduct	**OR**	Relevant to investigation and prosecution of suspected criminal incidents, the justice system response or enforcement orders, or the prevention of crime	**OR**	Is useful in a crime analysis or in the administration of criminal justice and public safety
AND	The source of the information is **reliable and verifiable**, or limitations on the quality of the information are identified					
AND	The information was collected in a fair and lawful manner					

Deficiencies in MIAC's Privacy Audit Practices

MIAC's Privacy Audit Policy, last amended in December 2020, governs the processes for auditing the MIAC.[126] To date, the MIAC has adopted a practice of performing the Audit two times per year using six-month periods. When work on this report began, only the audits for 2019 and 2020 were posted on the MIAC website. Audits from 2021 are now available.[127] Although MIAC's Privacy Audit practices are regularly evolving, they continue to suffer from numerous deficiencies, which have prevented the MIAC from identifying all of the likely privacy policy violations outlined in the prior section. This section explores these deficiencies in detail.

Absence of Independent Oversight: The audit team is composed of the MIAC Director, the MIAC Compliance Officer, a Public Member of the MIAC Advisory Board, and another board member selected by the board's chair, although the inclusion of the public member is not mandatory.[128] There are no truly independent audit team members, as the "public member," whose inclusion is not required, is a member of the MIAC Advisory Board and therefore affiliated with the MIAC. Further, as discussed above, neither of the current Public Members of the MIAC Advisory Board are experts in Privacy or Intelligence issues.

Independent audits are not a panacea for identifying and addressing privacy, civil rights, and civil liberties issues posed by agencies like MIAC; however, they are a necessary starting point. Experience shows that independent audits of law enforcement agencies can surface significant problems in a transparent way that is more likely to reassure the public that good governance is a real priority.

---

[126] Maine State Police, Maine Information & Analysis Center, "MIAC Privacy/Civil Liberties/Civil Rights (P/CL/CR) Audit Policy," December 12, 2020, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20PCRCL%20Audit%20Policy%20.pdf

[127] About the MIAC, Maine State Police, 2019, https://www.maine.gov/dps/msp/specialty-units/MIAC/About

[128] Maine State Police, Maine Information & Analysis Center, "MIAC Privacy/Civil Liberties/Civil Rights (P/CL/CR) Audit Policy," December 12, 2020, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/MIAC%20PCRCL%20Audit%20Policy%20.pdf

For example, the Chicago Police Department gave the RAND Corporation "extraordinary access" to evaluate the department's controversial "Strategic Subject List" or "Heat List," an algorithmically generated list of people deemed most likely to be involved in a shooting. The "Heat List" was billed as a tool to pre-empt crime by identifying and delivering services, such as counseling, to at-risk individuals. In practice, it became a way to identify suspects.[129] The RAND analysts conducted a regression analysis comparing individuals on the "heat list" to a control group. They found that individuals on the heat list were not more or less likely to be a victim of homicide or shooting than the control group. They were, however, more likely to get arrested. Through interviews with officers and observations of their activities, it became clear that this finding reflected the fact the "heat list" was being used as a "wanted list" and not a tool to pre-empt violence.[130]

Note the contrast between the MIAC's Advisory Board's self-policing and independent oversight by a third party. The former is narrowly focused on elevating a small area. The latter is a broad effort that develops its own momentum and identifies issues of concern. The MIAC's self-policing, now enshrined as public oversight through LD 12, is not meaningful accountability. If the legislature wants oversight, they should follow the example of Chicago, bring in an independent third party and provide them"extraordinary access" to the MIAC records, personnel, and information systems.

Record Selection Should Be Entirely Risk-Based, and Review Should Be Risk-Prioritized

The MIAC's 2019 audits selected records for audit through a purely randomized approach. After filtering for only those MIAC activity reports from the time period of the audit, the audit team then selected three percent of the activity reports at random, plus all SARs that were entered into the Federal eGuardian system. In 2020, however, a slight change to the record selection process appears to have coincided with the addition of the two public members from the Advisory Board to the audit team. The audit for the first half of 2020, for example, combined activity reports which were randomly selected with a few "handpicked entries" chosen by the public board members; however, the report does not indicate how the handpicked entries were chosen, how many handpicked entries were included and does not specify which MIAC record identifiers correspond to the handpicked entries.

An analysis of the first half (1H) 2020 audit highlights the importance of a risk-based approach to audit record selection rather than a randomized approach. Figure 4 provides an overview of all "Record Evaluation Forms" contained in the 1H 2020 Audit. The questions from the Record Evaluation Form can be found in the Annex, which contains a Record Evaluation Form from the most recently published audit from the second half (2H) of 2021.[131] It is important to note that many of the questions are very high-level and generic, which makes a thorough analysis of MIAC's audit practices difficult. However, even a high-level analysis based on the very limited information contained within the audit report produces evidence that the MIAC's

[129] Matt Stroud, "Chicago's predictive policing tool just failed a major test," *The Verge*, August 19, 2016, https://www.theverge.com/2016/8/19/12552384/chicago-heat-list-tool-failed-rand-test

[130]Jessica Saunders, Priscillia Hunt, and John S. Hollywood. "Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot." *Journal of Experimental Criminology* 12, no. 3 (2016).

[131] The two audit reports from 2021 were posted immediately prior to the release of this report; the sample is drawn from the most recent audit report in order to reflect the current list of audit questions, but this report's analysis relied on the audit reports that were available at the time the analysis was performed.

audit practices are failing to capture the MIAC records, which pose the greatest risk of privacy, civil liberties, and civil rights violations. For example, of the 58 records shown in Figure 4, only seven relate to suspicious E-guardian entries, SARs, social media, or civil unrest, the categories where the risk of violating individuals' privacy, civil rights, or civil liberties is high given the absence of clear criminal activity. As shown in Figure 5, more than 40% of the records evaluated contain neither personally identifying information, first amendment-protected activity, nor religious terminology or language, despite these three categories being some of the most sensitive areas for privacy, civil rights, and civil liberties violations. Many of the records, on the other hand, involve either administrative reports or summaries that contain little or no personal information or requests from other agencies related directly to criminal activity. The inclusion of low-risk records in the audit is an ineffective use of the audit team's time and efforts and distracts focus from the areas in which oversight is most critical.

Subsequent audit reports and Advisory Board Meeting minutes show that the audit team has identified the problem that audit efforts are not targeted at the MIAC activities, which pose the greatest risk to privacy, civil rights, and civil liberties. For the 2H 2020 audit, for example, the record selection process included five "handpicked records" selected by the board members serving on the audit team; however, it is unclear if the handpicked records were chosen blindly or if they were chosen with knowledge of the records' contents.[132] The 1H 2021 audit report is not posted on the MIAC website[133]; however, in the October 2022 Advisory Board Meeting minutes, a note indicates that the team "[p]icked 10 MIAC reports at random, each Board member picked 10."[134]

In order for the audit to more effectively assess and mitigate the risk of privacy violations, the record selection process should be risk-based, and the review should be risk-prioritized. This would entail using the pre-existing record categorization mechanism, or establishing a new mechanism if one does not exist, to filter out the record categories which pose the greatest risk of privacy violations. The records for the audit would then be drawn from this smaller set of high-risk records. Once the set of records is chosen, the team should prioritize the records which pose the greatest risk of violations. A risk-based and risk-prioritized audit infrastructure and approach would allow the MIAC to more efficiently and effectively identify and address the risks that its practices pose to privacy, civil rights, and civil liberties.

---

[132] Maine Information and Analysis Center, *Privacy/Civil Liberties/Civil Rights Audit Report for the Period 15 Jul 2020 - 31 Dec 2020*, Maine State Police, undated, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/210708%20%20Fourth%20MIAC%20PCLCR%20Audit%20Full%20Report%20%2B%20Attachments.pdf,

[133] The two audit reports from 2021, as well as the minutes from the March, 2022 MIAC Advisory Board Meeting, were posted to the MIAC website immediately prior to the release of this report and therefore were not able to be incorporated into the report's analysis

[134] Maine Information and Analysis Center Advisory Board Meeting Minutes, October 4, 2020, Maine State Police, https://www.maine.gov/dps/msp/sites/maine.gov.dps.msp/files/inline-files/2021%20Oct%20Minutes%20MIAC%20Advisory%20Board%20Meeting%20Minutes%20Final.docx.pdf, 3.

Figure 4 - Summary of 1H 2020 Audit Record Evaluation Forms by Type of Record

Type of Record	
Requests from other agencies	14
Activity Reports (weekly meetings, administrative items)	8
HIDTA Drug Arrest Notifications	8
E-Guardian Records	7
- Criminal	5
- Suspicious	2
Summary	6
Bulletin	3
Suspicious Activity Report/Tip	2
Information from Social Media	2
Information regarding Civil Unrest	1
Other	7
Total Number of Records Evaluated	58

Figure 5 - 1H 2020 Audit Record Form Summary by Audit Risk Factors

Total Number of Records Evaluated	58 (100%)
Records which contain neither: - Personally Identifying Information (Q6) - First Amendment-protected activity (Q14) - Religious terminology or references (Q12, Q13)	24 (41%)

What We Still Do Not Know about the MIAC

For years, fusion centers operated in the dark. The MIAC is no exception. As recently as February 2020, when the *Portland Press Herald* published a feature story on police surveillance in Maine, DPS refused to provide any information about the MIAC's technological capabilities, budget, or any documents from the Advisory Board, including privacy audits.[135] As a result of the whistleblower complaint, BlueLeaks, and resultant debate over Maine's fusion center, there is now more information in the public record than ever about the MIAC. We now know the basics of the MIAC's staffing and organization. The reporting and research that followed the BlueLeaks disclosures provided further insight into the MIAC's operations and intelligence output, raising concerns about the MIAC's focus on property and drug crimes at the expense of public safety concerns and political bias in its intelligence reporting.

This increased scrutiny, however, has not produced a complete picture of the MIAC. There is still much we do not know about Maine's fusion center. The courts dismissed the allegations concerning surveillance and illegation data retention in the whistleblower complaint on a technicality and, as such, this litigation will only address their factual basis if the case is appealed. The details of the MIAC's information systems and the analytic capabilities are still unclear. We do not know what information the MIAC can access and what tools it can use to analyze it. BlueLeaks provided an unredacted archive of MIAC intelligence bulletins and revealed that many caught in the MIAC's dragnet are some of the most vulnerable people in the state. We know the MIAC monitors people with mental illness, unhoused people, and people with substance abuse disorder, but we do not know the effects of this surveillance.

*We know the MIAC monitors people with mental illness, unhoused people, and people with substance abuse disorder, but **we do not know the effects of this surveillance.***

Official secrecy makes these questions difficult to answer. Almost all of the nominally public records created by fusion centers are not easily accessible by the public. To see these documents, members of the public need to request them under Maine's Freedom of Access Act (FOAA). Requesting a document, of course, is no guarantee that it will be released. There are over 300 exemptions to the FOAA, including broad exemptions for "intelligence and investigative" information and "security records." When records are released, they are often redacted, partial records. Finally, the public agency or officials may charge processing fees.[136]

The FOAA alone cannot ensure government transparency, as our efforts to research the MIAC and write this report attest. After the whistleblower complaint made headlines, Brendan McQuade filed thirteen FOAA requests for twenty items. The Maine State Police filled most of

[135] Randy Billings, "Maine State Police may be spying on you," *Portland Press Herald*, February 10, 2020, https://www.pressherald.com/2020/02/09/maine-state-police-may-be-spying-on-you/
[136] Sigmund Schutz, "Maine: Open Government Guide," *Reporters Committee for Freedom of the Press*, undated. https://www.rcfp.org/open-government-guide/maine/#ii-exemptions-and-other-legal-limitations

these requests, and many of the documents are cited in the report and have been shared with legislators who had, for years, been unable to get basic information from the MIAC about its budget and staffing, and journalists, both within Maine and across the country, that were covering the controversies that engulfed the MIAC in 2020.

However, an important request was effectively denied with an onerous processing fee. In response to a request for "All invoices, payment vouchers, canceled checks or other such documents that reflected the expenditure of funds from 2006 to present for expenses arising from or related to the MIAC," the Maine State Police required an estimated $1,000 processing fee. Here, it is important to note that McQuade, a professor at a public university in Maine and nationally recognized expert on fusion centers, had a strong claim for a fee waiver under §408-A subsection 11 B, which states, "The agency or official considers release of the public record requested to be in the public interest because doing so is likely to contribute significantly to public understanding of the operations or activities of government and is not primarily in the commercial interest of the requester."[137] If filled, this request would provide the documentation necessary to evaluate how the MIAC spends its budget, including the purchase of private data brokers and software systems for data analysis.

In another instance, the Maine State Police opens records officer responded to FOAA requests with bad faith denials until confronted with potential litigation and, under that pressure, released the documents. In November 2021, and in preparation for this report, McQuade filed another request for more recent email access logs, which would have enabled another network analysis of the MIAC intelligence sharing. Along with the request, McQuade attached an example of the MIAC email access logs made public with the publication of BlueLeaks. The open records officer's initial response was, "Our agency does not have records responsive to your request."[138] McQuade then rewrote the request and asked for 'Records detailing the emails sent by the MIAC and whether they were downloaded by the recipients. Please include the dates emails were sent, subject headings, names of attachments, and email addresses that opened the emails." In response to this request, the open records officer could find responsive documents but again charged an onerous processing fee estimated to be between $4,100 and $8,212.50. At this point, McQuade informed the public records officer he had hired a lawyer, who was preparing to appeal the FOAA response. Under threat of litigation, the processing fee dropped to $390.25, which McQuade agreed to pay.[139] A similar bad faith denial and reversal under the pressure of litigation occurred in response to another request regarding a request for information sent to the MIAC, which we discuss later in this report.

In other cases, redactions limit the usefulness of the released documents. In December 2021, Maxine Secskas submitted three FOAA requests for MIAC intelligence bulletins related to drugs and civil unrest. In February 2022, the Maine State Police open records officer released 137 pages of heavily redacted MIAC intelligence bulletins, which included two "Civil Unrest Situation Reports" related to the Million Militia March in Washington DC and related protests at

[137]Freedom of Access Act, Maine Revised Statutes, §408-A. Public records available for inspection and copying (2021), https://www.mainelegislature.org/legis/statutes/1/title1sec408-A.html

[138] Chrisopher Parr, email message to Brendan McQuade, "FOAA Request: MIAC Access log," November 8, 2021.

[139] The open records officer released these reports in early March. Some of them are cited in the report. However, the records were not released soon enough to give the research team enough time to review the MIAC's privacy audit using redacted versions of the documents reviewed by the Advisory Board.

state capitol's across the country, including two in Augusta, ME. As with the "Civil Unrest Reports" on the 2020 Black Lives Matter protests published in BlueLeaks, these documents include sections titled "(U//FOUO) National Informational" and (U//FOUO Related Products)."[140] This acronym stands for "For Official Use Only," a category which has been criticized as a needless "pseudo-classification" for "sensitive but unclassified information" that relegates access to public records "to a nether world-governed neither by the FOIA or Privacy Act."[141] In the "Civil Unrest Situation Reports released to Secskas under the FOAA, the entirety of these sections is redacted. What is hiding in the "nether" regions of these documents? The precedent set by unredacted versions of these documents published in BlueLeaks suggests that the redactions could be covering scandal and controversy. These sections of "Civil Unrest Reports" on the 2020 Black Lives Matter protests included the poorly sourced and easily debunked claims of pre-staged bricks and paid protesters.

In short, the FOAA, like the MIAC's privacy audits, is not a sufficient tool to provide transparency or accountability. If oversight and accountability are the policy goals, the Maine State Legislature must rise to the occasion, exercise their oversight powers, and investigate the MIAC. In addition to the allegations of the whistleblower complaint, there are two major problem areas that need to be addressed: the MIAC's information systems and analytic capabilities and the MIAC's impact on vulnerable populations. We detail each of these in turn before closing with specific recommendations for an independent investigation of the MIAC.

Information Systems and Analytic Capabilities

The scope of the MIAC's information systems is still unclear. The whistleblower complaint notes that the "MIAC maintains an 'index pointer' type of Multi Jurisdictional Criminal Intelligence Database," which includes "Personal Identifying Information."[142] The complaint also alleges that the "MIAC conducts electronic surveillance of people's social media and other accounts and permanently retains personal and private information on those individuals because they engaged in constitutionally protected activity such as participating in a lawful protest or purchasing a firearm."[143] Currently, these allegations cannot be confirmed or refuted. The hacks behind BlueLeaks did not compromise the MIAC's databases, only its email systems.

We have similarly limited knowledge of the MIAC's analytic capabilities. In a July 3, 2020 open house attended by members of the media, state legislature, and the public, MIAC

---

[140] Maine Information and Analysis Center, "Civil Unrest Situation Report," January 15, 2021; Maine Information and Analysis Center, "Civil Unrest Situation Report," January 19, 2021.

[141] Lotte E Feinberg, "FOIA, federal information policy, and information availability in a post-9/11 world." *Government Information Quarterly* 21, no. 4 (2004): 439. See also the 2007 hearings of the House Subcommittee on Intelligence, Information Sharing and Terrorist Risk Assesment held on "over-classification and pseudo-classification." The prevailing concern of the hearings was that the proliferation of such pseudo-classifications was impeding the information sharing mission of fusion centers. Despite these concerns that "over-classification and pseudo-classification" was preventing meaningful accountability and impeding the mission of fusion centers, the use "sensitive but unclassified" categories stands today as a common label applied to bulletins and other information produced and shared by fusion centers. US Congress, House of Representatives, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, 110th Congress, First Session, March 22, 2007, April 26, 2007, and June 28, 2007. https://www.govinfo.gov/content/pkg/CHRG-110hhrg35279/pdf/CHRG-110hhrg35279.pdf.

[142] Complaint and Demand for Jury Trial, *supra* note 1, ¶ 37

[143] Complaint and Demand for Jury Trial, *supra* note 1, ¶ 63

leadership disclosed that they have a subscription to i2 Analyst's Notebook, a data analytics platform produced and sold by IBM. This software provides police with the capability to analyze telephony metadata and produce pattern of life and social network analyses, but they declined to explain how often the software is used and for what purposes.[144]

We also learned from email correspondence related to FOAA requests that the MIAC once had a subscription to Geofeedia, the social media intelligence platform, which allows users to search social media content for a specific location.[145] In 2018, for example, the ACLU of Massachusetts obtained thousands of records regarding the use of Geofeedia by the Boston metro fusion center, the Boston Regional Intelligence Center. Their analysis of these documents showed that "police in Boston were using Geofeedia's automated surveillance capabilities to conduct surveillance on entire communities and to monitor First Amendment protected speech and association, not to fight crime."[146] The MIAC discontinued its use in December 2016. By that time, however, bad press and the resultant backlash caused Geofeedia to lose access to data from Facebook, Instagram, and Twitter, dramatically reducing the usefulness of the platform for social media monitoring.[147] This begs the question: How did the MIAC use Geofeedia? Has the MIAC since purchased a different software package for social media monitoring?

We do not know the full scope of the data that the MIAC can access or the tools it can put to work to analyze them. However, in the BlueLeaks documents, we uncovered a case that provides insight into the intrusive surveillance capabilities leveraged by police organizations in Maine and the lack of care in securing personal identifying information.

Cellebrite and MIAC's Analytic Capabilities

Through our search of the BlueLeaks information pertaining to Maine residents, we were able to uncover records of two cell phones being accessed using a passcode and encryption circumvention device called Cellebrite UFED Touch 2.[148] Cellebrite is an Israeli digital intelligence company that provides a product called UFED (Universal Forensics Extraction Device), which is used for the extraction and analysis of data from mobile devices. Physical possession of the target mobile device is required to use the Cellebrite UFED hardware. Cellebrite forensics devices and training have been provided to human rights-violating countries the world over, including Turkey, United Arab Emirates, Russia, Saudi Arabia. Federal, state,

---

[144] See this promotional "solution brief" for summary of capabilities of Analyst's Notebook. IBM Security, IBM Analyst's Notebook. IBM, 2017, https://www.ibm.com/downloads/cas/QNGO6RNA.

[145] Chrisopher Parr, email message to Brendan McQuade, "[**Your recent FOAA request/requests]," July 21, 2020..

[146] Nasser Eledroos and Kade Crockford, "Social Media Monitoring in Boston: Free Speech in the Crosshairs," *Privacy SOS,* 2018, https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/

[147] Lora Kolodny, "Facebook, Twitter cut off data access for Geofeedia, a social media surveillance startup," *Tech Crunch*, OCtober 11, 2016, https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/.

[148]Tim Dalton, "Extraction Report, Apple iPhone" May 16, 2019, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Tim Dalton, "Extraction Report, LG LG-SP200 Tribute Dynasty" May 16, 2019, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

and local law enforcement and private corporations in the United States are also known to use Cellebrite.[149]

One Cellebrite record was from an android device in February 2019, and the other record was from an Apple iPhone SE in May of 2019. The iPhone, presumably running up to date iOS 12 at the time, would have been both encrypted and passcode protected by default. Encryption is a way of securing digital data using mathematical techniques so that it can only be decrypted and read when a valid key is provided. The iPhone would have been protecting against brute force guessing, which is the attempt to exhaustively guess passwords to unlock the device.

The records showed that the Cellebrite UFED forensics extraction device circumvented the encryption and password protections and revealed the data on the iPhone. The extracted data includes user accounts and passwords belonging to healthcare records, social media, internet search history, text messages, call logs, and contact information, among other data points. These records were available in BlueLeaks because, after extraction of all of this information from the target device, the whole of the record was presumably stored unencrypted and without password protection on the MIAC email servers.

These data extracted from the phones were sent to the MIAC by a Scarborough Police officer. In addition to the extracted data from the phones, BlueLeaks also included a spreadsheet of the requests for information (RFI) received by the MIAC. We linked the Cellebrite extraction reports to a May 16, 2019, RFI sent to the MIAC concerning an overdose death case. The officer wanted the MIAC to create a timeline of calls and text messages between a suspected drug dealer and the individual who died of an overdose. The Maine Drug Enforcement Agency was apparently involved. Although the domain of the officer's email is @scarborourgh.maine.org, the spreadsheet lists his agency affiliation as "Scarborough Police/MDEA." For this reason, we cannot determine which agency, the Scarborough Police Department or the MDEA, owns the Cellebrite UFED forensics extraction device.[150]

In December 2021, we filed FOAA request records "detailing the MIAC's response to a May 16, 2019 request for information" and attached the RFI spreadsheet. We filed this request to get a better understanding of the MIAC's analytic capabilities. Our request was initially fully rejected, but when confronted with potential litigation, we received a heavily redacted document that removed all mentions of Cellebrite, its use, and information on who it had been used to target. The State Police released the email exchange between the officer and the MIAC but not the timeline created using the data extracted from the phones. From this correspondence, it appears that a MIAC analyst used the software, Analyst's Notebook to create a timeline, which

[149] Joseph Cox, "Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests" *Vice*, January 12, 2017,
https://www.vice.com/en/article/aekqjj/cellebrite-sold-phone-hacking-tech-to-repressive-regimes-data-suggests; Mara Hvistendahl and Sam Biddle, "Use of Controversial Phone-Cracking Tool Is Spreading Across Federal Government," *The Intercept*, February 8, 2022,
https://theintercept.com/2022/02/08/cellebrite-phone-hacking-government-agencies/
[150] The Maine Information and Analysis Center, "RFI", June 14, 2020,
https://ddosecrets.com/wiki/BlueLeaks.

the officer then presented to the assistant attorney general as part of the case against the suspected drug dealer accused of murder in the overdose death.[151]

This example underscores the power of the tools available to law enforcement and the secrecy surrounding them–to say nothing of the difficulty asserting democratic control over whether and how they should be used. Cellebrite maintains a high level of secrecy regarding its usage as part of agreements made with its customers.[152] At this time, it is unknown if the most current versions of mobile devices are still vulnerable to attacks on the passwords and encryptions that Cellebrite uses to extract data.

It is also unknown what other types of intrusive surveillance technologies may also be in the arsenal of police agencies in Maine. The RFI spreadsheet published in BlueLeaks provides the details of 143 requests for information received by the MIAC between October 2017 and June 2020.[153] The Cellebrite data extraction reports included in the MIAC records allowed us to reconstruct this story, but we are left wondering what other tools are available, not just at the MIAC, but among other police agencies, and what is the MIAC's role in analyzing this data.

More narrowly, this case reveals the invasiveness of one surveillance product known to be available to law enforcement in Maine, Cellebrite's UFED forensics extraction device. It shows the failure of police to protect the very personal contents of the extracted data, including the data of a victim. All of this is evidence of the lack of care given to privacy by the MIAC program and Maine state police. When considered in relation to the many of the allegations and findings in this report–the claims of the whistleblower complaint, the abuse complaints against Minkowsky, the shoddy and biased intelligence shared about the 2020 BLM protests, and the repeated failures of the MIAC to follow its own privacy policy–it suggests that MIAC's work environment is characterized by unprofessionalism and carelessness.

The MIAC's Impact on Vulnerable Populations

In the last fifty years, as the United States has become the world leader in incarceration, the criminal legal system has become the social safety net of last resort. To critics, this situation is known as "mass incarceration" and is understood as "one of this country's key strategies for addressing problems of poverty, inequality, unemployment, racial conflict, citizenship, sexuality, and gender, as well as crime."[154] Jonathan Simon, a University of California-Berkeley law professor, describes this situation as "governing through crime."[155] The MIAC is caught up in this larger process of managing social problems with police and prisons. In addition to the previously discussed role of the MIAC in monitoring racial justice protests and the over-policing of the crimes of poverty, the MIAC records published with BlueLeaks include documents produced by

---

[151] [name redacted] email message to Timothy Dalton, "[redacted] Chart" June 19, 2019; Timothy Dalton email message to [name redacted] "Re: Chart Update," June 25, 2019.
[152] Kim Zetter, "When the FBI Has a Phone It Can't Crack, It Calls These Israeli Hackers," *The Intercept*, October 31, 2016,https://theintercept.com/2016/10/31/fbis-go-hackers/
[153] The Maine Information and Analysis Center, "RFI", June 14, 2020, https://ddosecrets.com/wiki/BlueLeaks.
[154] James Kilgore. *Understanding Mass Incarceration: The People's Guide to the Key Civil Rights Struggle of Our Time*, (New York: The New Press, 2009), 1.
[155] Jonathan Simon, *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear* (New York: Oxford University Press, 2009).

the MIAC and "passed through" from other agencies that concern unhoused people, undocumented people, and youths running away from home or the juvenile justice system.

The role of the criminal legal system in managing social problems is especially salient in the area of mental health: 37 percent of people in state and federal prisons and 44 percent of people in county jails have been diagnosed with mental illness.[156] Between a quarter and half of the victims of police-involved shootings are people with mental illness.[157] There are at least 89 MIAC bulletins published in BlueLeaks that report on people with suicidal feelings, mental health issues, disabilities, and/or chronic illness. Some bulletins detail what appear to be sympathetic tragedies. For example, a 2018 officer bulletin alerts officers to an "Armed…Maine (ME) resident living in the woods…reportedly suffering from mental health issues." The document explains that family members suspect that the individual suffers from Huntington's Disease. Two members of the individual's immediate family had already passed from the progressive and fatal genetic brain disorder that impairs the ability to reason, walk, and speak.[158] Other bulletins detail more ambiguous situations: people that also have troubling histories of violence and threatening behavior. Individually, the bulletins are snapshots of larger, incomplete stories. Taken together, they provide a dispiriting account of the punitive regulation of social problems, countless untold tragedies of structural victimization, and interpersonal harm: homelessness, addiction, mental illness, trauma, and abuse.

We do not know what happens to these individuals when they become subjects of the MIAC intelligence reports, but we do know at least one situation where an individual at risk of suicide featured in a MIAC intelligence bulletin shot himself during a confrontation with police. A 2019 "Attempt to Locate" MIAC release details the situation of Joshua Hussey, described as "a dangerous suspect involved in multiple criminal violations." Hussey violated a protection from abuse order filed by his ex-girlfriend. He vandalized her home and car. At the time the bulletin was issued, the Maine State Police had probable cause to arrest Hussey for domestic violence terrorizing and felony criminal mischief. The MIAC bulletin notes that the Hussey is a known runner from police and has made numerous suicide by cop statements to family and friends and that he would not be 'taken alive.'[159]" A subsequent *Lewiston Sun Journal* article noted that Hussey had previously been incarcerated and said in text messages that "I don't want anyone to be hurt, not even me…But I'm not going back to prison." Despite this intelligence, the Maine State Police sent their tactical team to bring the individual into custody in a 2 AM raid on the home of Hussey's mother. In the subsequent confrontation, Hussey shot himself in the head and eventually died from the wound.[160]

---

[156] Jennifer Bronson and Marcus Berzofsky, *Indicators of Mental Health Problems REported by Prisoners and Jail Inmates, 2011-2012*. The Bureau of Justice Statistics, 2017. https://bjs.ojp.gov/content/pub/pdf/imhprpji1112.pdf

[157] Doris Fuller, H. Richard Lamb, Micheal Biasotti and John Snook, *Overlook in the Undercounted: The Role of Mental Illness in Fatal Law Enforcement Encounters*. The Treatment Advocacy Center, 2015, https://www.treatmentadvocacycenter.org/storage/documents/overlooked-in-the-undercounted.pdf.

[158] The Maine Information and Analysis Center, "Situational Awareness," (MIAC-2018-1625), August 31, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks;

[159] The Maine Information and Analysis Center, "Attempt to Locate," (MIAC-2019-0523)," August 31, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeak

[160] Mark LaFlamme, "Green suspect remains in critical condition after shooting himself," *Lewiston Sun Journal*, March 19, 2019, https://www.sunjournal.com/2019/03/18/greene-man-remains-in-critical-condition/.

No doubt, many will struggle to find sympathy for Hussey, given his previous history, but we raise the case to challenge the mass criminalization and question whether surveillance and police raids are the appropriate response to interpersonal violence and threats of self-harm. Hussey's previous incarceration is worth considering. We know that imprisonment has adverse effects on mental health, including the development of "institutionalized personality traits" (like distrusting others, difficulty maintaining relationships, and problems making decisions), social-sensory disorientation (issues with spatial reasoning and difficulty with social interactions), and social and temporal alienation (the feeling of not belonging in social settings).[161]

Did this situation have to end with Hussey's death? What police and other intelligence and security professionals understand as an uncomplicated act of information sharing appears, from a different perspective, as the quotidian acts of administration that comprise a system of mass criminalization: the social construction of various harms as crime or disorder that portends future crimes. No doubt, Hussey's situation and those described in the 88 other similar documents involve real danger, usually the threat of self-harm or violence toward others. They detail real suffering, but they do so in a way that individualizes the problem as a criminal stigma. They reinforce the idea that "criminal" behavior is an uncomplicated "choice."

The antithesis of criminalization is humanization. What would it mean to treat Hussey and others featured in the 88 MIAC documents detailing the situations of people with suicidal feelings, mental health issues, disabilities, and/or chronic illness with dignity owed to all humans as a matter of course? Is a secretive police intelligence center issuing a "law enforcement sensitive" bulletin and a 2 AM police raid really the most effective and appropriate response?

The antithesis of criminalization is humanization. *What would it mean to treat Hussey and others featured in the 88 MIAC documents detailing the situations of people with suicidal feelings, mental health issues, disabilities, and/or chronic illness with dignity owed to all humans as a matter of course?* ***Is a secretive police intelligence center*** *issuing a "law enforcement sensitive" bulletin and a 2 AM police raid really* ***the most effective and appropriate response?***

[161] Marieke Liem and Maarten Kunst, "Is there a recognizable post-incarceration syndrome among released "lifers"?." *International Journal of Law and Psychiatry* 36, no. 3-4 (2013).

The MIAC's impact on the vulnerable populations also needs to be considered in relation to substance abuse. On this issue, the ground has shifted. In the summer of 2020, the Maine State Legislature came three Senate votes short of decriminalizing drug possession. If LD 967: An Act To Make Possession of Scheduled Drugs for Personal Use a Civil Penalty had become law, Maine would have followed Oregon to become the second state to decriminalize drug possession. Instead of arrest and incarceration, the state's response to the possession of illegal drugs would have been a health assessment or, if the individual refused, a fine for no more than $100.[162]

This nearly successful push for decriminalization reflects years of mobilization and organizing from harm reduction advocates. Harm reduction is a set of practical strategies and ideas aimed at reducing negative consequences associated with drug use. Harm Reduction is also a movement for social justice built on a belief in and respect for the rights of people who use drugs. Jesse Harvey was one of the best known and most influential in this community. He is also the subject of intelligence bulletins possessed by MIAC and now in the public records as a result of BlueLeaks. In 2016, Harvey founded Journey House Recovery, a non-profit that today operates four low barrier, peer-run recovery houses in Southern and Central Maine. In 2018, Harvey formed the Church of Safe Injection because "other churches… aren't interested in helping people who use drugs."[163] The church is a workaround and a protest. It is an attempt to find a loophole to distribute clean hypodermic needles and naloxone, the medication used to counteract opioid overdoses. It's also a political challenge to the criminalization of the opioid epidemic. Now with five branches in as many states, its success is further support for what the approximately 120 supervised injections sites operating across the world have already proven: harm reduction works.

To the police in Lewiston, Maine, however, the matter is different. Harvey was a person of interest. Three different Lewiston Police Department Bulletins issued between May 29 and June 5, 2020, include a description of Harvey in the "Officer Safety & Awareness" section. The bulletin alerted officers to Harvey's work "distributing hypodermic needles throughout Lewiston's downtown." They noted that "HARVEY is ***NOT*** affiliated with a needle exchange organization and therefore, it is not legal for HARVEY to be handing needles out." They cited his previous criminal history and instructed officers who may have encountered him to "remind him of the Governor's stay-at-home order and summons him (if he is in possession of needles)."[164]

Harvey died in early September in what police called a possible overdose. A tribute published in *Mainer* explained the circumstances leading to his death: constant police monitoring that disrupted his harm reduction work, relapses and continuing struggles with

---

[162]https://www.pressherald.com/2021/07/01/maine-senate-rejects-bill-that-would-make-drug-possession-for-personal-use-a-civil-violation/

[163] Jesse Harvey, "Church of Safe Injection treats drug users as Jesus would have done," *Portland Press Herald*, December 18, 2018, https://www.pressherald.com/2018/10/18/maine-voices-church-of-safe-injection-treats-addicts-as-jesus-would-have-done/

[164] Lewiston Police Department, "Lewiston Police Department Bulletin," May 29-June 1, 2020, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Lewiston Police Department, "Lewiston Police Department Bulletin," June 1-June 3, 2020, BlueLeaks, Distributed Denial of Secrets. https://ddosecrets.com/wiki/BlueLeaks; Lewiston Police Department, "Lewiston Police Department Bulletin," June 3-June 5, 2020, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

substance use, legal troubles, and stigmatizing press coverage, compounded, in the end, by the isolation and stress of the pandemic. Friends and colleagues concluded that "relentless police surveillance and harassment helped push Harvey over the edge."[165] A decent society would have supported Harvey's initiative and leadership in response to a public health crisis. Instead, his calling was criminalized, and he became another casualty of the war on drugs.

While we cannot confirm that the MIAC did anything with these bulletins other than receiving them from the Lewiston Police Department, the case of Jesse Harvey helps contextualize the MIAC's other intelligence reporting on drug use. The most in-depth and frequent intelligence report regularly produced by the MIAC is the "Maine Drug Monitoring Initiative," a project which seeks to "establish a multi-jurisdictional, drug-incident information sharing environment through the collection and analysis of drug seizures, overdoses, related criminal behavior, and healthcare-related services with a specific emphasis on heroin and opioids." The reports provide strategic intelligence. The reports are "not to provide analysis or dissemination of real-time or time-sensitive drug intelligence that may require an actionable response." Instead, they usually begin by highlighting one specific item related to drug markets or drug trafficking like "Counterfeit Oxycodone Pills Containing Fentanyl" or "Cocaine Concealed in Tylenol Capsules," before providing a statistical summary of suspected overdose and naloxone administrations and out of state arrests of Maine residents. The reports end with a list of attached bulletins from other police intelligence operations concerning drugs. [166]

Under present law enforcement operations, where opioid use and addiction are criminalized, the "Maine Drug Monitoring Initiative" has arguably some intelligence value to law enforcement. It provides information on issues in trends related to drug use, overdoses, and drug market dynamics. However, these reports evince some of the same shoddy and unprofessional work on display in the Civil Unrest Reports. An October 2017 Drug Monitoring Initiative report included a bulletin from the Oregon-Idaho High Intensity Drug Trafficking Area on "fentanyl-laced marijuana," a claim which Snopes, the fact-checking website, had debunked the previous month.[167] Similarly, a December 2017 Drug Monitoring Initiative report warns officers to "exercise extreme caution when handling suspected Oxycodone pills due to the risk of fentanyl residue."[168] In May of that year, a story about a police officer in Liverpool, Ohio, overdosing due to unintentional skin contact with fentanyl went viral. By the time of the MIAC report, however, toxicologists had debunked the claim.[169]

---

[165] Nathan Bernard, "The Crucifixion of Jesse Harvey," The Mainer, October 2, 2020, https://mainernews.com/the-crucifixion-of-jesse-harvey/

[166] Brendan McQuade, Lorax B. Horne, Zach Wehrwein, and Milo Z. Trujillo. "The secret of BlueLeaks: security, police, and the continuum of pacification." *Small Wars & Insurgencies* (2021), 21.

[167]Maine Information and Analysis Center and New England HIDTA, "Maine Drug Monitoring Initiative October 2017 Bulletin," MIAC 2017-1989, November 2, 2017, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks; Alex Kaspark, "Is Fentanyl-Laced Marijuana Use on the Rise?" *Snopes*, September 26, 2017, https://www.snopes.com/fact-check/fentanyl-laced-marijuana-rise/

[168] Maine Information and Analysis Center and New England HIDTA, "Maine Drug Monitoring Initiative December 2017 Bulletin," MIAC 2018-0010, January 3, 2018, BlueLeaks, Distributed Denial of Secrets, https://ddosecrets.com/wiki/BlueLeaks.

[169] Jeremey Samuel Faust, "The Viral Story about the Cop Who Overdosed by Touching Fentanyl Is Nonsense," *Slate*, June 2017, https://slate.com/technology/2017/06/toxicologists-explain-the-medical-impossibility-of-overdosing-by-touching-opioids.html.

The quality of the Drug Monitoring Initiative reports notwithstanding, the 16 "Opioid Arrest Bulletins" also disclosed through BlueLeaks are examples of gratuitous criminalization. These monthly reports list everyone arrested for opioid trafficking. They include names and addresses but never any intelligence information that connects the arrested people to ongoing investigations. Moreover, most of the individuals shamed and stigmatized in these "intelligence" reports may not have been charged with criminal offenses if LD 967 had been state law at the time. In her testimony to the Maine State Legislature in support of the bill to close the MIAC, Whitney Parrish, the then-advocacy director of Maine Equity Alliance, concluded that the "discernable reason for these bulletins is to distribute this information to every law enforcement agency in the state, putting officers on notice with nothing short of a modern day rogue's gallery."[170] In correspondence related to FOAA requests, the Maine State Police open records officer divulged that the MIAC no longer produces "Opioid Arrest Bulletins." The given reason was "staffing shortages," but we must also wonder if the criticism of these products and shifting public sentiments around substance use and addiction also played a role.[171]

The time has come for a different approach to social problems like substance use and mental illness. Many Mainers recognize this need for change, as evinced in recent reform efforts. The MIAC should be closed, not just to protect privacy and other rights, but also to make way for a more humane and effective social policy response to issues like substance use, mental illness, and homelessness. The MIAC claims to be essential for public safety, but we know that criminalization kills, and there are better ways to address problems like mental illness and substance abuse disorder.

*The MIAC claims to be essential for public safety, but we know that **criminalization kills, and there are better ways** to address problems like mental illness and substance abuse disorder.*

As it stands, the response to controversies that surrounded the MIAC in 2020–the self-policing by the Advisory Board and a report issued to the State Legislature–do not address some of the most serious issues at stake. The MIAC's reporting on substance use needs to be questioned and investigated, especially as politicians, policymakers, and the public continue to debate and re-evaluate the best response to substance use, mental illness, and homelessness.

[170] Whitney Parrish, "Testimony of Whitney Parrish, LD 1278: Ought to Pass," April 12, 2021, https://www.youtube.com/watch?v=BEstS1vPIKU.
[171] Christopher Parr email to Maxine Secskas, "FOAA Request" January 4, 2022.

Investigate and Defund the MIAC

After nearly two years of controversy and debate around the Maine Information Analysis Center, there is a strong case to close the embattled spy center. The allegations of the whistleblower complaint, the abuse complaints against Minkowsky, the hyperfocus on the crimes of powerless and vulnerable populations, the shoddy and biased intelligence shared about the 2020 BLM protests, and the repeated failures of the MIAC to follow its own privacy policy set the issue in dramatic relief. The MIAC, like all fusion centers, is fundamentally flawed. The MIAC should be closed and can safely be closed without negatively impacting public safety. Moreover, there is reason to believe that the MIAC, as the nerve center of mass criminalization in Maine, is actually exacerbating social problems and negatively impacting public safety. Defund the MIAC!

However, the State Legislature did not vote to close the MIAC and, instead, passed a first-in-the-nation bill that requires a fusion center to report to legislative authorities. This measure, while well-intended, is insufficient. Self-policing by the MIAC's Advisory Board is an obvious conflict of interest. This is not a theoretical problem. Our analysis of the MIAC privacy policy and audits shows that the Maine fusion center regularly violates its own privacy policy. It also exposes the privacy audit as a perfunctory exercise that fails to meet the full scale or scope of the privacy risks posed by the MIAC. The audits only consider MIAC intelligence bulletins; they do not assess its information systems and analytic capabilities. Given the strict facial recognition regulations recently implemented in Maine, there is little doubt many Mainers would be equally concerned about private data brokers and software that can decrypt phones, analyze telephony metadata, and automatically monitor social media. This report proves that the MIAC uses some of the surveillance and intelligence systems or has used them in the past. What will we do in this present moment? Should this police surveillance and intelligence gathering continue in the future?

Even if the privacy audit was more rigorous, privacy protection is not the only issue posed by the MIAC's operation. The MIAC's monitoring of constitutionally protected speech and assembly needs to be thoroughly investigated, as do related questions regarding how the MIAC reviews the intelligence it disseminates and vets (or fails to vet) the claims made in those bulletins. Finally, the MIAC's impact on vulnerable populations needs to be investigated and questioned. Does the MIAC make a measurable and positive impact on public safety issues related to mental illness, substance abuse, and homelessness? Should a secretive police intelligence center originally set up for counterterrorism really be part of the public response to these social problems?

The State Legislature needs to rise to the occasion and exercise oversight powers over the executive branch. Once again: Defund the MIAC! If the political will to revisit closing the fusion center is lacking, then the situation demands a thorough, open, and independent investigation. The allegations of the whistleblower complaint have not been settled by the courts or by journalists and scholars working from the outside. We need an independent investigation. The State Legislature or a third party hired to investigate needs unrestricted access to all MIAC records. These materials should be made public to the greatest possible extent. The decisions of what to release cannot be the exclusive purview of the State Police open records officer. The MIAC personnel need to testify under oath and provide the public with definitive answers.

Specifically, we recommend an alternative privacy audit and identify a series of unanswered questions that an independent investigation of the MIAC should address.

A meaningful privacy audit must be independent. MIAC personnel need to cooperate in providing documents and answering questions, but the auditing should be conducted by independent subject matter experts. The audit should prioritize MIAC activities that pose the greatest risk to privacy, civil rights, and civil liberties, and should consider the scale and scope of these risks as compared to MIAC's core mission. The audit should not be limited to information disseminated by MIAC, but should also cover MIAC's information gathering and processing systems and MIAC's operational procedures, following the example of the LAPD Inspector General, all SARs processed by the MIAC. The audit should also cover MIAC's record retention and information destruction procedures and documentation of any past record destruction efforts to ensure that they align with the MIAC's privacy policy and/or best practices for similar situated organizations.

There are also a series of unanswered questions that need to be addressed. There is much the public still does not know about the MIAC. Some of these questions would be answered in an independent investigation and privacy audit.

- *What data can the MIAC access*? Answering this question requires investigating the following: the information-sharing agreements the MIAC has with other agencies, the databases that personnel assigned to the MIAC can access, any subscriptions to private data brokers that the MIAC has purchased, and any in-house databases the MIAC has developed.
- *What are the MIAC's analytic capabilities*? We know that the MIAC can use i2 Analyst Notebook to analyze telephony metadata, and we know that they previously had a subscription to GeoFeedia, the controversial social media monitoring platform. However, we do not know the full extent of the fusion center's capabilities.
- *What other data analysis platforms are available to the MIAC*? A meaningful independent audit would produce a complete list of MIAC's inventory of surveillance and analytic technologies, including social media monitoring, digital forensics, crime mapping and predictive analytics, specifying how long these technologies have been in use, identifying specific privacy protections in place for each technology, and auditing compliance with those policies.
- *The allegations of the whistleblower complaint also need to be addressed.* We cannot wait for an appeal that may never happen to find out if the MIAC does or did maintain an illegal database of gun owners, make agreements with other states to circumvent Maine law regarding retention of license plate reader data and surveil anti-CMP activists and Seeds of Peace counselors and campers. Settling these allegations also requires investigating the role of Bruce Lewis, CMP's director of security and former member of the MIAC Advisory Board. Did Lewis pass on information on anti-CMP activists to the utility? Why did he leave the Advisory Board when he did?
- *The shocking and shoddy work of the MIAC exposed by BlueLeaks also demands attention.* A thorough investigation of the MIAC must revisit the "Civil Unrest Daily Reports" on the 2020 BLM protests. What is the review process for these intelligence bulletins? How did documents with such dubious sourcing get approved? These

scandalous reports are not the only issue, however. The more routine violations of MIAC's privacy policy documented in this report also require attention and investigation.

- *These matters open up to further reaching questions regarding the MIAC's organization and mission: can there be meaningful accountability in a task force organization?* Here, again the allegations of the whistleblower complaint surface again in relation to the ambiguous position of Loder between two interagency task forces and the question of policy shopping as it relates to license plate readers. The James Minkowsky case is also relevant here. What are the pre-employment checks on MIAC personnel? How could they miss the abuse allegations against Minkowsky? How did the MIAC and DPS respond to the allegations?
- *The MIAC's mission also needs critical scrutiny: We know that the nebulous "all hazards" mission, in practice, translates into a hyperfocus on the crimes of the powerless but we do not know what is the MIAC's impact on these vulnerable populations?* What happens to people with mental illness, people that use drugs, and unhoused people that become the subject of MIAC bulletins? What we already know is not encouraging and raises more basic questions: should the MIAC be focusing on people that use drugs, people with mental illness, and unhoused people?

For some, these last questions are still open. For the authors of this report and the organizations endorsing it, the matter is already settled. There are better responses to these social problems. Investigate and defund the MIAC! Protect privacy and clear the way for more humane and effective policy responses to social problems.

Annex

Record Evaluation Form from Most Recent Published MIAC Audit

MAINE INFORMATION & ANALYSIS CENTER ("MIAC") PRIVACY AUDIT

RECORD EVALUATION FORM

Updated 2/18/2021

RECORD IDENTIFICATION NUMBER:	2021-1464

SUMMARY OF RECORD(S) EVALUATED*
**The content summary should be a de-identified information regarding each activity report that can lawfully be disseminated publicly in the interest of promoting transparency and clarity on MIAC's activities.*
Report from law enforcement agency of public gatherings/rallies/protests for situational awareness.

#	QUESTION	YES	NO	NA
1	Does the RECORD provide information that is consistent with the MIAC's mission?	X		
2	Was the RECORD disseminated by the MIAC to any agency or person?		X	
	A. If the RECORD was disseminated, is there documentation evidencing that it was reviewed and approved prior to its dissemination?			X
	B. If the RECORD was disseminated and it originated from another source (e.g., another law enforcement agency), did MIAC review and approve the RECORD in the same manner in which MIAC would review and approve its own RECORDs prior to their dissemination?			X
	C. If the RECORD was disseminated, was it repurposed or revised by MIAC for a new audience?			X
	(1) If so, was the RECORD appropriately re-labeled or labeled as necessary prior to MIAC's dissemination of the repurposed or revised RECORD?			X
3	Does the RECORD require labels or ratings relating to the confidence or reliability of the information in the RECORD?		X	
	A. If so, are such labels or ratings included in the RECORD?			X
4	Does the RECORD require any use or dissemination limitations or restrictions (legal or otherwise), given its content?	X		
	A. If so, are such limitations or restrictions expressly stated in the RECORD?	X		
5	Are any opinions of MIAC personnel stated in the RECORD?		X	
	A. If so, are the opinions expressly labeled or otherwise identified as such?			X
6	Does the RECORD contain personally identifying information ("PII")?		X	

1

	A. If so, was the inclusion of the PII necessary?			X
	B. If so, does the PII included in the RECORD relate to minors, victims of domestic violence, victims of sexual abuse, participants in substance abuse programs, or participants in mental health treatment programs?			X
	(1) If so, was the PII necessary to include in the RECORD, given the information being provided in the RECORD?			X
7	When it was originally reviewed, was the RECORD found to include erroneous data?		X	
	A. If so, was the RECORD amended or rescinded as a result?			X
8	Does the RECORD expressly identify the audience for whom the RECORD is intended?	X		
9	Does the RECORD expressly state when the RECORD should be disregarded or otherwise purged?		X	
10	Does the RECORD use broad, vague descriptors (e.g., "extremist," "radical," "far left," "far right," etc.) of persons and organizations?		X	
	A. If so, was the use of the descriptors appropriate given the purpose of the information provided in the RECORD?			X
	B. If the response to "A" is "NO," was the RECORD prepared by the MIAC?			X
11	Does the RECORD include demographic descriptors pertaining to one or more individual's race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity?		X	
	A. If so, were those descriptors appropriate to include, given the information being provided in the RECORD?			X
12	Does the record discuss or reference religion?		X	
	A. If so, is the discussion of or reference to religion neutral?			X
13	Does the RECORD relate to First Amendment-protected activity ("*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*")	X		
	A. If so, does the RECORD include any necessary and appropriate qualifiers or context regarding First Amendment-protected activities to which the RECORD relates?	X		
	B. If so, was there a compelling reason to create the RECORD?	X		
	C. If so, was the RECORD narrowly-tailored to achieve that purpose?	X		

NOTES/COMMENTS

No action taken by the MIAC.