METRO NASHVILLE COMMUNITY OVERSIGHT

FUSUS Informational Report

Prepared by the Metro Nashville Community Oversight Board

An informational report on FUSUS, a new surveillance technology utilized by the Metro Nashville Police Department.

Introduction

On September 15th, 2022, the Metro Nashville Police Department (MNPD) entered a contract with FUSUS, a law enforcement surveillance technology company. Despite falling under the purview of surveillance technology, MNPD entered a $175,000 sole source contract[1] with FUSUS, a price point below the $250,000 benchmark[2] that would require Metro Council approval. MNPD acquired 58 FUSUS devices with the original contract, eight for public use and 50 for private use to disperse to businesses and residents. Currently, there are over 900 FUSUS-linked cameras in Nashville.

FUSUS allows MNPD to integrate public and private cameras across Nashville into a "Real-Time Intelligence Ecosystem[3]," as advertised on FUSUS's website. Essentially, all FUSUS-linked cameras collect and enable MNPD to analyze visual and audio data through the FUSUS hardware installed in the cameras, which encrypts the data and compiles it into a cloud-based surveillance dashboard. Once compiled, MNPD can view the locations of registered cameras and the data and real-time footage of integrated cameras, all in one place. Any type of camera can be linked to FUSUS, from public cameras (like city-owned cameras, public school cameras, and license plate readers), to private cameras like security cameras, CCTVs, and Ring doorbell cameras[4]. Linking a camera to FUSUS involves the option of registering the camera with MNPD, and/or granting them real-time access. FUSUS-linked cameras can be accessed by sanctioned MNPD personnel even from their mobile devices[5]. Now that MNPD has been approved for a full LPR program, there is now a large network of police surveillance cameras for FUSUS integration in Nashville.

FUSUS came to the attention of MNCO staff in August 2023, as MNPD attempted to procure an additional $175,000 worth of the FUSUS technology. However, rather than entering a second $175,000 contract with FUSUS, Resolution RS2023-2380[6] aimed to amend MNPD's original contract to $350,000 and extend the contract 12 months, which required the purchase to be voted on by Metro Council. RS2023-2380 was brought before Metro Council by Councilmembers Kevin Rhoten and Jeff Syracuse on August 15th, 2023, but was deferred indefinitely in both the Budget and Finance and Public Health and Safety subcommittees prior to the 8/15/23 Metro Council meeting.

The withdrawal of the resolution caused the original contract to expire on September 14th, 2023, though it is unclear what will happen to existing FUSUS technology now that the contract has lapsed. This question is especially salient given that FUSUS is more than just a tool purchased by MNPD and is

[1] https://documents.nashville.gov/Request/Open/756940ef-a433-4dda-86ad-4a508092b399_Contracts-20181129_58232_1
[2] https://nashville.legistar.com/View.ashx?M=E2&ID=1116527&GUID=4AB96F3B-86E0-4ECD-B124-B25C74BE077A
[3] https://www.fusus.com/
[4] For more information on the linkage of Ring and FUSUS, see Bridges, Lauren. "Infrastructural obfuscation: Unpacking the Carceral Logics of the Ring Surveillant Assemblage." Information, Communication & Society 24.6 (2021): 830-849.
[5] https://www.documentcloud.org/documents/23795974-fusus-ops-use-redacted
[6] https://nashville.legistar.com/LegislationDetail.aspx?ID=6311977&GUID=1695E844-FF60-4714-A806-5C258246C619

still on the market for the Nashville public. To this end, MNPD still has a FUSUS-operated website[7] where the public can purchase FUSUS devices allowing them to link their own cameras to MNPD's FUSUS network. When making this purchase, members of the public can opt into which level of integration they want to have with MNPD. According to MNPD's FUSUS website, there are two main "levels", 1) registering cameras and 2) integrating cameras, which are outlined further below.

Registration and Integration

Members of the public can choose at what level they want to link their cameras with MNPD. The first level, camera registration, provides MNPD with the precise location of the camera. This enables MNPD to create a registry of every FUSUS-linked camera in Nashville, so that MNPD knows the locations of all the cameras across Nashville that opt into the program. Per correspondence with Deputy Chief Gregory Blair, the locations of all the FUSUS cameras are integrated into MNPD's Geographic Information System (GIS) mapping databases[8]. This level is designed for the public to notify MNPD that they have cameras and where those cameras are located, which enables MNPD to map their locations.

An overlay of a FUSUS network. Source: https://www.fusus.com/about-us/working-with-us

FUSUS's second level is camera integration. Camera integration gives MNPD live-stream access to integrated cameras. This allows MNPD to create a "Real-Time Crime Center in the Cloud[9]," effectively creating a centralized database where MNPD can access cameras anywhere across Nashville in real time, regardless of if they are in the public or private sphere. Owners of the cameras can opt to give MNPD full access to their cameras, or partial access and limit the data sharing to certain times of the day or with permission. Beyond just camera access, the data from integrated cameras could potentially be

[7] https://connectmetronashville.org/
[8] MNCO reached out MNPD Deputy Chief Gregory Blair via email correspondence on 8/15/23.
[9] https://www.fusus.com/rtc3-products/fusus-real-time-crime-center-in-the-cloud

linked with other MNPD technology[10] as well, including but not limited to license plate readers, body-worn cameras, and even MNPD's drones. These forms of existing surveillance technology are all compiled into one central hub for MNPD personnel to access. Alongside other police technology, this enables MNPD to view events in real time, compare data across databases, and dispatch officers to where they can view live footage.

Nashville Context

According to the MNPD FUSUS website[11], there are currently 940 registered cameras and 202 integrated cameras. This suggests that MNPD has access to the locations of those 940 cameras, and real-time data access to 202 cameras. While the first level (camera registration) is the most advertised option for most police departments, many cities are using both levels of integration. While FUSUS is relatively new to the Nashville scene, Atlanta, Georgia, a peer city to Nashville, has a similar FUSUS-run website[12]. Atlanta first implemented cameras in the fall of 2021[13], and now there are currently more than 18,000 FUSUS-registered cameras as well as 16,000 FUSUS-integrated cameras in Atlanta, which indicates the potential scope of this technology. While FUSUS is a relatively new technology, it has the capability to expand fast in the cities it is implemented in.

FUSUS comes at a crucial turning point for police surveillance in Nashville, as the much-debated license plate reader (LPR) program was approved for full implementation on August 15, 2023. LPRs are automatic cameras that take a picture of every license plate that passes through them, cross checks them with the National Crime and Information Center (NCIC) law enforcement database and identifies any license plates that are in the database as a "hit." MNPD is notified of all hits, and then will physically verify the hit before sending the verified hit to dispatch for law enforcement action. The LPR program gives MNPD the authority to place and use LPR cameras in public rights-of-way across Nashville. Based on one of MNPD's reports[14] to Metro Council on the LPR pilot program, there will be an estimated 117 LPRs across the city once there is full deployment of the technology. MNPD can retain the data from LPRs up to 10 days, after which it must be deleted unless it is part of active or ongoing investigation or has written exemption.

In MNCO's Full LPR Pilot Program report[15], we found that LPRs were overwhelmingly placed in non-white and low-income areas. These disparately distributed LPRs provide a general surveillance technology foundation that FUSUS can integrate into and build upon: LPRs provide a network of cameras for FUSUS to connect to, since LPRs have the capacity to integrate with FUSUS[16]. Additionally, FUSUS allows police departments to create and edit their own license place hotlists. This could provide MNPD with the opportunity to use more than just the NCIC law enforcement database, as FUSUS also includes other, independently chosen LPR hotlists within FUSUS. The creation of custom hotlists could

[10] https://www.fusus.com/security-operations/fusus-security-operations-center-in-the-cloud
[11] https://connectmetronashville.org/
[12] https://connectatlanta.org/
[13] https://www.ajc.com/news/a-game-changer-atlanta-police-hope-new-camera-network-will-help-solve-reduce-crime/NOQQDEYMXNAERARZACITEBHBKU/
[14] https://www.nashville.gov/sites/default/files/2023-07/LPR-Council-Report-3.pdf?ct=1689087910
[15] https://www.nashville.gov/sites/default/files/2023-08/MNCO-Full-LPR-Pilot-Program-Report.pdf?ct=1691418108
[16] https://www.documentcloud.org/documents/23795975-fusus-hotlist-editing-redacted

allow police departments to sidestep exclusively using the NCIC database, which is heavily controlled, and create targeted lists based on the areas in which LPRs are placed.

FUSUS creates more than just a platform to compile data, as it also creates a foundation to add more surveillance technology. Beyond just LPRs, FUSUS can integrate with gun-shot detection technology like ShotSpotter (recently rebranded as SoundThinking). MNPD has made multiple attempts to acquire ShotSpotter since 2018. Per MNCO's previous ShotSpotter report[17], MNPD included line items in Nashville's Capital Improvement Budget for $800,000 worth of the technology in FY2023-24, indicating that the technology remains relevant to MNPD. However, Metro Council has yet to approve the technology, which may be a prudent decision amongst concerns about its efficacy[17]. The fact that FUSUS can provide a platform that is ready to integrate ShotSpotter into might provide further motivation for MNPD to make another push to Metro Council for its approval.

Given the prevalence of school shootings across America, including the Covenant School shooting in Nashville in March 2023, FUSUS has advertised[18] their devices' ability to be integrated into schools to provide more surveillance, real-time viewing, and potentially faster response times. In fact, MNPD and MNPS already have a memorandum of understanding (MOU) regarding the integration of FUSUS into MNPS schools[19]. The MOU allows for MNPD to have "24 by 7 by 365" access to MNPS security camera systems, video management systems, and security software. However, MNPD can only access these cameras in the event of a "Health or Safety Emergency," including but not limited to active shootings and bomb threats. MNPD is limited in the number of officers who have access to MNPS cameras, and any time MNPD accesses MNPS cameras there must be written documentation, which includes an incident report, documentation outlining when the cameras where accessed, who within MNPD accessed the cameras, what the reason for accessing the cameras was, what actions were taken by MNPD, and what school and cameras were accessed. The MOU also establishes that the use of FUSUS does not waive the constitutional rights of its employees or students. Finally, the MOU establishes that any data gathered from MNPS cameras may not be used for law enforcement purposes[20], may not violate FERPA (the Family Educational Rights and Privacy Act), or be disseminated to third parties.

According to the FUSUS MOU that exists between MNPD and MNPS, all FUSUS data will be housed at MNPD's Community Safety Center (SCS) when it is built. The CSC is being funded through a $3,000,000 grant based around reducing crime rates across Nashville[21]. Through FUSUS, authorized users at the SCS will be able to view real-time FUSUS data around the clock. The CSC alongside FUSUS will allow MNPD to have all its technology and data linked in one place digitally and physically. Since the SCS will be the technological hub for MNPD, it may provide MNPD and Council with additional justification for more surveillance technology given the large investment already made in the SCS and other such tech.

[17] https://www.nashville.gov/sites/default/files/2022-10/ShotSpotter-Informational-Report.pdf?ct=1666884022
[18] https://www.fusus.com/security-operations/fusus-educational-institutions
[19] MNCO received a copy of the MOU via email correspondence with MNPS on
[20] This most likely means that MNPD cannot use FUSUS footage as the basis of questioning, investigating, or apprehending a student or MNPS employee in matter unrelated to a "Health or Safety Emergency." However, until a situation like that plays out, it is only speculation as the MOU does not go into greater detail.
[21] https://www.wkrn.com/news/local-news/nashville/mnpd-applies-for-3-million-grant-to-combat-violent-crime-in-nashville/

A visual representation of a FUSUS-integrated system. Source: https://vimeo.com/529039664

It is also worth noting that Nashville is getting a smart streetlight[22] overhaul next year. While this might seem inconsequential, some smart streetlights have cameras. In other cities that use FUSUS, like Cleveland, OH, they have been able integrate streetlight cameras with FUSUS, turning every streetlight into potential surveillance technology. It is unclear whether Nashville's smart streetlights will have cameras as well, but the Mayor's Office of Cleveland has stated that their LPRs are FUSUS-linked, indicating the potential for the technology[23]. Additionally, both Cleveland State University and the Cleveland Metropolitan School District are FUSUS-linked.

MNPD FUSUS Policy

Currently, MNPD does not have any FUSUS-specific policies, draft policies, or Standardized Operating Procedures (SOPs)[24]. MNPD has several sections of their policy that deal broadly with surveillance technology that would encompass FUSUS usage, but these sections are not specific to FUSUS itself. This deviates from other specific police surveillance devices such as LPRs or Body-Worn Cameras (BWCs) that have specific policy written for them. MNPD's usage of FUSUS falls under MNPD Department Manual[25] Section 12.10: Security and Disposition of Law Enforcement Records and Files; and Section 12.30: Management and Utilization of Automated System.

Section 12.10 covers any document stored in or displayed on any electronic file or storage medium. It prohibits MNPD personnel from sharing, or profiting off, any electronic data. While MNPD-

[22] https://wpln.org/post/nashville-streetlights-are-getting-a-makeover-and-thats-possibly-good-news-for-stargazers/
[23] https://mayor.clevelandohio.gov/news/city-expanding-safe-smart-cle-camera-sharing-program-mayor-calls-community-participation
[24] Private communication from Deputy Chief Greg Blair indicates that there is no SOP for FUSUS.
[25] https://www.nashville.gov/sites/default/files/2023-07/MNPD-Manual.pdf?ct=1689616240

original documents are managed by the Records Division, it is uncertain who would oversee management of FUSUS data. Additionally, it appears most of the provisions regarding data deletion and retention pertain specifically to MNPD-original documents, so it is unclear how long FUSUS data would be kept by the Department. Section 12.30 covers the management and use of automated systems, which includes any hardware, software, programs, and applications, and reinforces Nashville's Security management Policy (ISM Policy) from Executive Order 038[26], which establishes protections for the confidentiality, integrity, and availability of data for Metro Nashville Departments. Section 12.30 also mandates that MNPD personnel must adhere to the licensing of software, including the terms and conditions. However, the rest of Section 12.30 mostly pertains to individual personnel technology use rather than the maintenance and use of general surveillance hardware, software, and data.

While no concrete policy exists regarding how MNPD can use FUSUS, there is a "terms and conditions[27]" page of FUSUS's MNPD website, which is also listed in the original and amended FUSUS contracts listed in Resolution RS2023-2380[28]. FUSUS terms and conditions identify two main actors: the "Partner," (members of the public who install FUSUS in their private cameras) and the "Agency" (MNPD). The terms and conditions grant MNPD the locations of all the FUSUS-registered cameras of members of the public, and video access for all the FUSUS-integrated cameras of the public. Regarding the real-time 24 by 7 by 365 access mentioned in the MNPS MOU, the FUSUS terms and conditions for private partners only state "it is not the intention or expectation that the public's cameras will be routinely monitored in real-time by MNPD." Members of the public still own camera footage that is not real-time, and MNPD must make digital requests to gain video access. Once videos are transferred onto the FUSUS cloud, it adheres to FBI Criminal Justice Information Services, or CJIS, standards and complies with applicable laws governing the storage, access, and dissemination of evidentiary data. Finally, it also prevents MNPD from sharing the camera locations or videos with any member of the public, or anyone outside of MNPD, without prior consent from the private partner.

However, FUSUS terms and conditions alone do not hold the same legal standing as the law and come with clearly outlined limitations. Section VII of the FUSUS terms and conditions states one such limitation, the limitation of liability. The section states in all caps, "IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO LOST OF REVENUES, PROFITS, OR GOODWILL, FOR ANY MATTER ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OR NONPERFORMANCE OF THIS AGREEMENT." This appears to be based on "Consequential Damage Waiver" language[29]. While the terms and conditions provide guidelines, both parties are exempt from liability to the other party for any damages, regardless of whether one follows or breaks the terms and conditions. There are thus no established civil or legal consequences that either party can enforce on the other for not abiding with the terms and conditions. These guidelines do not specify any documented repercussions for violations of using FUSUS technology, which is concerning given the all-encompassing scope of the surveillance that FUSUS provides.

[26] https://www.nashville.gov/departments/metro-clerk/legal-resources/executive-orders/mayor-karl-dean/kd038
[27] https://connectmetronashville.org/terms-conditions/
[28] https://nashville.legistar.com/LegislationDetail.aspx?ID=6311977&GUID=1695E844-FF60-4714-A806-5C258246C619
[29] https://afterpattern.com/clauses/consequential-damages-waiver

Metro Code 13.08.080[30] also governs surveillance or electronic data gathering devices onto public rights-of-way, most notably LPRs. Metro Code 13.08.080 provides important guidelines MNPD must abide by for the LPR program, including limiting the retention period of data gathered by surveillance devices in public rights-of-way to 10 days, prohibits unlawful usages, and mandates equitable distribution of the devices. While FUSUS devices conduct surveillance in both public and private spaces, they are not specifically included in Metro Code 13.08.080, nor any other Metro code. This legislation could provide an important model for comparable FUSUS legislation. This is especially relevant as other cities polices specifically include FUSUS LPR-integration[31].

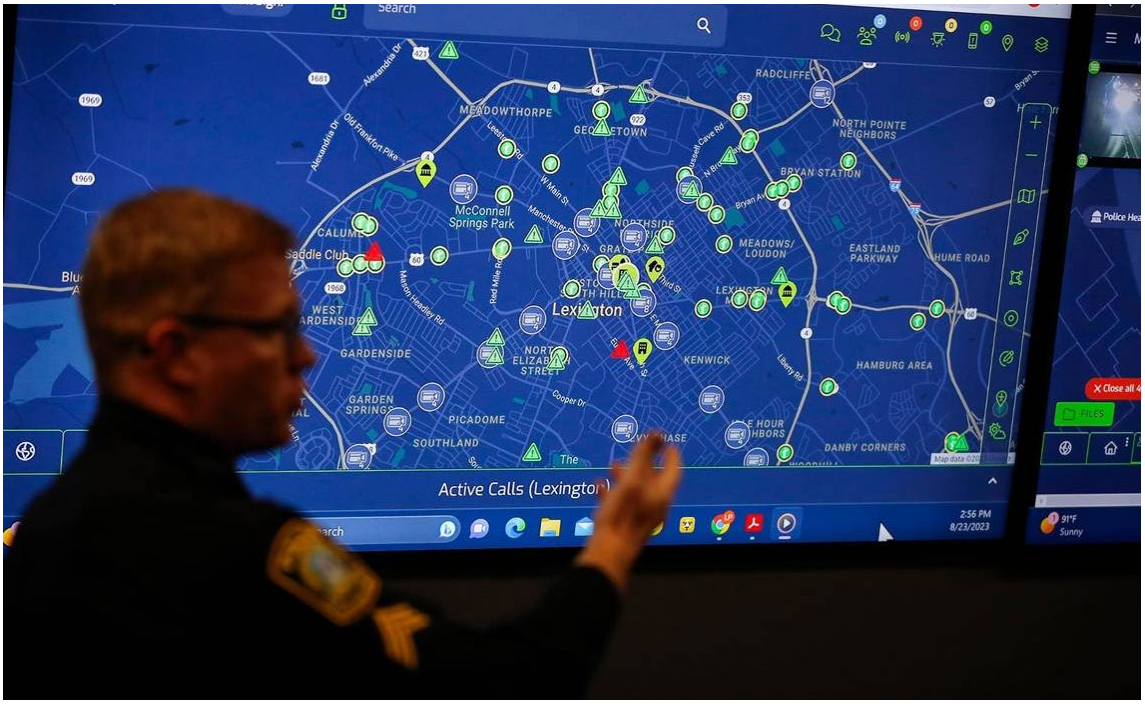
Existent FUSUS Policies

Currently, Nashville does not have any FUSUS specific policy, even though other cities, even smaller cities, and other cities in the South, have drafted and implemented FUSUS policies. Lexington, Kentucky, for example, has even brought civil rights advocacy groups in to help their police department create FUSUS policy[32]. The advocacy groups included the American Civil Liberty Union (ACLU) in Kentucky, the National Association for the Advancement of Colored People (NAACP) and the Lexington Human Rights Commission. With the advocacy groups' input the Lexington Police Department (LPD) incorporated important recommendations into their policy, including restrictions on accessing FUSUS data, adding retention schedules to the data, and including regular audits of the data. According to the Lexington herald-Leader, Kungu Njuguna, a policy strategist for the ACLU in Kentucky stated, "'For the most part they made the changes we requested,'" and "'It's kind of like if you're going to do a bad thing, at least you do it in the least bad way.'" In terms of restricting access to FUSUS data, the policy limits the number of users in the department who would have access to FUSUS, FUSUS data will only be available in LPD's Real-Time Crime Center, and LPD officers will only be able to utilize private cameras if they are within range of a call for service. In terms of retention schedules, data from traffic cameras will be held for 60 days, and footage from the city-owned cameras will only be held for 30 days. In addition, even the camera registration data will not be available to the LPD, only the owners of the cameras. Furthermore, the advocacy groups and the LPD stated that they looked at the issue of surveillance technology through a non-discriminatory lens, making sure to account for how FUSUS would impact citizens regardless of race, color, sex, religion, age, disability, and other protected classes.

Collaborating with advocacy group has led to LPD having a robust final FUSUS policy[33]. The policy includes detailed sections on FUSUS procedures, access, usage, retention, release, and auditing. The policy even includes important definitions pertaining to which entities own the cameras, where FUSUS data can be stored, and even how archived data is different than normal data. Interestingly, compared to other cities, Lexington's FUSUS policy establishes clear data ownership rights, with private entities having full ownership over their FUSUS data. Private owners can terminate the agreement with LPD at any time and are not held to the same retention schedule that LPD is held to. However, if any data has evidentiary value, then LPD will collect it in accordance with established department practices

[30] https://www.nashville.gov/sites/default/files/2023-01/License-Plate-Reader-Pilot-Program-Ordinance.pdf?ct=1673289099#:~:text=1%20of%209-,13.08.,way%20requires%20metropolitan%20council%20approval.
[31] https://www.documentcloud.org/documents/23314068-cpd-draft-policy-for-fusus
[32] https://www.msn.com/en-us/news/us/some-civil-rights-groups-ok-with-lexington-s-new-police-camera-software-the-aclu-is-not/ar-AA1fMyyM
[33] https://www.lexingtonky.gov/sites/default/files/2023-08/GO%202023-01%20Video%20Management%20System.pdf

and legal requirements. In that vein, LPD FUSUS policy also places all FUSUS usage under the applicable local, state, and federal laws.



Lexington police are among the most recent departments to utilize FUSUS. Source: https://www.kentucky.com/news/local/counties/fayette-county/article278520934.html

In terms of mid-sized cities in other regions of the United States, The Minneapolis Police Department (MPD) also has FUSUS policy in their departmental handbook[34]. Minneapolis's FUSUS policy has similar protections to South Bend's policy including protecting civil liberties under the United States Constitution, and local, state, and federal law. It also includes protections against using real-time video footage to target or harass individuals or groups, and that collecting data will only be for legitimate law enforcement use and not for the arbitrary collection of video surveillance. The policy includes similar language establishing that FUSUS video shall only be saved for judicial, investigative, and training purposes. Furthermore, the policy includes having a list of verified users who are allowed to access the real-time crime center that will be monitored by a systems administrator. Like MNPD, it appears that FUSUS data will be saved at MPD's Strategic Information Center (SIC).

However, Minneapolis' FUSUS policy includes noticeable differences that other city policies lack. Minneapolis's FUSUS policy strictly prohibits the use of facial recognition software. In addition, a list of all the public areas in which Minneapolis is collecting video shall be released to the public. Releasing a list of the public spaces that have live video-feed, especially FUSUS-enabled ones, is an important step in increasing the transparency between police departments and the citizens of their city amidst widespread surveillance technology use. The FUSUS policy also includes detailed operational steps about how FUSUS technology will be used in real-life applications, including protocol for data transferring

[34] https://kstp.com/wp-content/uploads/2023/05/MPD-Policy-and-Procedure-Manual.pdf

between precincts, when MPD's Strategic Information Center (SID) would need access to the data, and when the Emergency Operations Center (EOC) would need access to the data.

MPD's FUSUS policy abides by the authority over data collection and sharing in the Minnesota Data Practices Act[35]. In the Minnesota Data Practices Act, Section 13.82 Subdivision 31 Covers the use of surveillance technology. It states that "the existence of all technology maintained by a law enforcement agency that may be used to electronically capture an audio, video, photographic, or other record of the activities of the general public, or of an individual or group of individuals, for purposes of conducting an investigation, responding to an incident or request for service, monitoring or maintaining public order and safety, or engaging in any other law enforcement function authorized by law is public data." Essentially, Subdivision 31 states that in Minnesota, any video, audio, or image law enforcement data that is gathered by public surveillance devices is by law public data. However, there are two notable exceptions, Section 13.82 Subdivision 25, and Section 13.37 Subdivision 2. Subdivision 25 covers the classification of deliberative processes and rules that data that utilizes deliberate processes or investigative techniques against individuals or incorporate non-public data is considered confidential. However, once a case is cleared by final opinion or justification for a decision, then that data will become public as well. Additionally, Section 13.37, Subdivision 2[36] covers classification of data and prohibits data from being public if it contains any information that the government considers "nonpublic" including security information, sealed ballot, trade, and labor relation information. Thus, all MPS's FUSUS data that does not contain confidential or active investigatory information is public data.

MPD's FUSUS policy also adheres to the authority of the Minnesota's Public Safety Retention Schedule[37]. In Minnesota's Public Safety Retention Schedule, Code PBS-10-43 covers non-evidentiary public safety cameras for police departments across Minnesota. Essentially, this code covers routine surveillance of pedestrian and traffic that serves no investigatory, judicial, or punitive purpose, which pertains to most FUSUS-recorded data. According to the code, the records will be kept while in active use and until the capacity of the recorder is met, after which they will be overwritten. While the code does not have a set retention schedule written, the code lists the time frame as "typically 10 – 14 days" based on a 11/21/2005 estimate. However, if the recorded data is evidentiary, then it would fall under Code PBS-77-24, which covers mobile video recording (MVR) and public safety camera footage that is considered property and evidence. Code PBS-77-24 dictates that records will be kept while active and can be permanently kept if they contain any of the following: arrest, DUI, use of force, significant incident, or any record in which the city is on notice of an investigation or claim. However, if the footage is just for a traffic citation, then it will be kept for one year. It is unclear however, if overwriting the data in the cameras themselves, will affect the data that has been sent to the MPD by FUSUS.

Even much smaller cities, like South Bend, Indiana have full FUSUS policies[38]. The policy includes crucial safeguards to FUSUS technology including not using FUSUS-linked cameras in areas where reasonable expectations of privacy exist, not using FUSUS to harass, intimidate, or discriminate individuals or groups, and not using FUSUS-linked cameras in an unequal or discriminatory way based on

[35] https://www.revisor.mn.gov/statutes/cite/13.82
[36] https://www.revisor.mn.gov/statutes/cite/13.37#stat.13.37.2
[37] https://www.minneapolismn.gov/media/-www-content-assets/documents/Public-Safety-Retention-Schedule.pdf
[38] http://docs.southbendin.gov/WebLink/0/edoc/362101/Policy334_PublicSafetyVideoSystem.pdf

actual or perceived characteristics including race, color, religion, sex, age, national origin or ancestry, disability, gender identity or sexual orientation. The policy mentions conducting video surveillance in public areas in a legal and ethical manner, while "recognizing and protecting constitutional standards of privacy," and commitment to the "protection of individual rights as governed by the United States Constitution, the Indiana Constitution, and Federal, State and local law." Notably, the policy also states that public and private video streams are "never for the arbitrary collection of video surveillance." Breaking these restrictions will subject employees to administrative disciplinary action and even criminal penalties.

South Bend's FUSUS policy also contains operational guidelines regarding which areas FUSUS cameras are allowed to operate. Those areas include public areas and activities where no reasonable expectation of privacy exists as well as public areas owned by private entities where the property owners have given permission for real-time monitoring. In the latter, the policy establishes that in private spaces where property owners have given police real-time access to the cameras, no reasonable expectation of privacy will exist in those areas. Interestingly, regarding where FUSUS-linked cameras are allowed to operate, South Bend's policy focuses on the strategic placement of cameras throughout the city through approval by the South Bend Chief of Police and the Mayor of South Bend, or their designees, indicating that there is acknowledgeable intentionality in where public FUSUS-linked cameras are located.

Additionally, South Bend's FUSUS policy includes requirements for those who are authorized to view real-time footage, which includes understanding of the policy, training on system use and security, being Criminal Justice Information Services (CJIS) certified, and the monitoring of all system access. It also establishes that any FUSUS footage that is saved shall only be used for judiciary, investigative, or training purposes, and falls under the same classification as digital evidence. South Bend's policy lists all the different technology vendors that FUSUS pulls together from and incorporates into one single real-time crime center (i.e. CommandCentral, Milestone, Necam, Utility, ADSI, and FLOCK). FLOCK is important because MNPD has announced its intent to partner with them for the full implementation of their LPR program. South Bend's FUSUS policy also includes an MOU for businesses to agree to for partnership. The MOU is almost verbatim the FUSUS terms and conditions document. Finally, South Bend's policy includes a section about a video surveillance audit. This audit is to be conducted annually. The review should include any concerns arisen from the public, significant prosecutions, and any systemic operational or administrative issues. Importantly, this audit section includes language about either the Chief of Police or an authorized designee, or other applicable advisory bodies conducting the audit, which includes community oversight boards and community review boards.

While not all cities have full FUSUS policies, some cities have draft policies in the works. The draft policy for Columbia, Missouri[31], for example, includes provisions like ensuring the constitutional rights of individuals, providing transparency regarding use of FUSUS to the public, and putting FUSUS use under the jurisdiction of local, state, and federal law. Importantly, the draft policy prohibits live-stream access from cameras associated with personal residences. It also establishes that the private partner is the owner of FUSUS hardware, and thus all the video footage compiled from it. Additionally, the policy limits the number of personnel who can access the FUSUS cloud to only officers trained on its

usage, and who have specific and identifiable needs for investigations. Personnel will further be required to get supervisory approval before accessing the live-stream video features. The draft policy also includes information on including periodic audits of the technology and use. Finally, the draft policy includes a provision to educate the community on the "nature, scope, and protocols" of FUSUS.

Finally, while not all cities that use FUSUS technology have full or drafted FUSUS-specific policy, other police departments across the country have comprehensive criminal intelligence policies that are based on Commission on Accreditation for Law Enforcement Agencies (CALEA) policies. CALEA policies are considered the gold standard of law enforcement policy and accreditation, largely because it ensures that police departments are meeting a national accreditation standard, which is crucial when dealing with surveillance technology that could potentially infringe on constitutional freedoms. CALEA helps ensure that police departments have baseline polices in place that can address new technological developments (i.e., FUSUS) in the time before they have a more specific policy in place. Three notable cities that have CALEA-based policies that govern FUSUS use are Providence, Rhode Island[39], Greenville, North Carolina[40], and Miami, Ohio[41]. The vast majority of these cities' FUSUS policies center around two main CALEA sections, 40.2.1 which covers "Criminal Intelligence Data Collection", and 40.2.3 which covers "Criminal Intelligence Procedures." MNPD is a CALEA-certified police department, yet the sections of their policy that cover FUSUS are not CALEA-based.

Core traits of the CALEA-informed Criminal Intelligence Policies utilized by the above departments include detailing guidelines around the collection and assessment of data, the dissemination and storage of data, the sharing and acquisition of data, and training. Regarding the collection and assessment of data, CALEA-based policy includes preventing police departments from collecting general or targeted surveillance data against individuals or groups, placing criminal intelligence under the purview of local, state, and federal laws, and collecting information that matches the level of appropriate level of suspicion. All the policies specify that no information will be collected that contains political, religious, social views, the association, or activities of any individual, group association, corporation, business, partnership, or other organization, unless it is directly related to a criminal investigation, which is an important factor or preventing FUSUS-use for general surveillance.

The policy of Providence, Rhode Island for example, reinforces that routine reviews and audits should purge data that is outdated and no longer relevant. Greenville, North Carolina's policy includes specific procedures for the criminal intelligence analysist positions and differentiation between permanent and temporary datasets for their gang unit, which must be purged five and one years after their data of recording respectively. Miami, Ohio's policy includes both those aspects as well, in addition to including its own sections on what type of criminal intelligence may be recorded and what the retention schedules for different datasets are. Permanent records that include identifying information may be kept for five years after date of recording, temporary records that do not include identifying information may be kept for one year after date of recording, and working files that have not yet been verified by the criminal intelligence team may be kept for 20 days after recording. After the set amount

[39] https://www.providenceri.gov/wp-content/uploads/2020/03/360.06-Criminal-Intelligence.pdf
[40] https://public.powerdms.com/GPD19/documents/1797732
[41] https://www.miamitwpoh.gov/PDF/Police/Directives/40.2.pdf

of time is reached for each dataset respectively, the files are destroyed. Finally, all CALEA-based policies include annual audits and reviews as well.

To understand the elements of a strong FUSUS policy, MNCO staff have compiled all these policy provisions into a table for consideration for MNPD and the public. If a cell in the table is red, it does not contain a policy provision, and if it's green it does:

Table 1: FUSUS Policies Across Police Departments

Police Agency	FUSUS Policy?	CALEA-Based Policy?	Authorized Users?	Limited to Public Space?	Non-Discriminatory Usage?	Prohibits Facial Recognition?	Legal Framing?	Retention Schedules?	Routine Audits?	Consulted Advocacy Groups?
Nashville, TN	X	X	✓	X	X	X	X	X	X	X
Lexington, KY	✓	X	✓	X	✓	X	✓	✓	✓	✓
Minneapolis, MN	✓	X	✓	✓	✓	✓	✓	✓	✓	X
South Bend, IN	✓	X	✓	✓	✓	X	✓	X	✓	X
Columbia, MO	✓	X	✓	✓	X	X	✓	X	✓	X
Providence, RI	X	✓	X	X	✓	X	✓	X	✓	X
Greenville, NC	X	✓	X	X	✓	X	✓	✓	✓	X
Miami, OH	X	✓	X	X	✓	X	✓	✓	✓	X

Concerns

While FUSUS has been marketed to enhance public safety, there are many concerns surrounding the technology, especially on the grounds of privacy and data security. Consent, privacy, and civil liberties are jeopardized by constant surveillance and filming of individuals in both public and private spaces, as constant police surveillance jeopardizes the 1st and 4th Amendments of the Constitution according to the US Department of Justice. According to Jennifer Granholm, the former governor of Michigan who is now President Biden's Secretary of Energy, "electronic surveillance so alters the climate of community life that it constitutes an unwarranted invasion of privacy and chills free expression and association"[42]. Constant police surveillance jeopardizes the 1st Amendment because it can restrict freedoms of expression, speech, and movement, and jeopardizes the 4th Amendment because constant surveillance may be considered an unreasonable and unwarranted search. The risks to civil liberties and violations of Constitutional Rights are especially high for communities of color and low-income communities, who face higher rates of surveillance technology and police presence in their

[42] https://www.ojp.gov/ncjrs/virtual-library/abstracts/video-surveillance-public-streets-constitutionality-invisible#:~:text=First%2C%20the%20surveillance%20is%20an,freedom%20of%20expression%20and%20association.

communities[43]. These concerns are warranted particularly if the public is not aware of the level of police surveillance that FUSUS has provided to MNPD within Nashville. Private partners do not always know exactly what FUSUS is or does to its full extent, especially regarding the level of access MNPD has over data access, retention, and usage.

FUSUS compiles surveillance data into one centralized hub, so data management protocols are crucial. In contrast, MNPD's data management protocols are concerningly ambiguous. FUSUS adds another level of ambiguity on top of the already growing list of external parties that are involved in surveilling Nashville citizens and collecting their data. Typically, public cameras have regulations as to how long they can keep data for, which is determined by the city. For LPRs in Nashville, Metro Code 13.08.080[44], limits the retention period of data gathered by surveillance devices in public rights-of-way to 10 days. However, a report[45] from the Electric Frontier Foundation emphasized that police departments do not have to follow the same retention protocols from private cameras since they do not fall under the same provisions as public cameras do. Depending on the type of FUSUS device installed, data can be archived for up to 30 days, which presents a potential conflict with MNPD's LPR data storage requirements. Additionally, FUSUS could potentially challenge other policies set forth for MNPD's LPR technology, as FUSUS has its own license plate reader hitlists pre-installed and allows users the ability to create and edit their own hitlists.

Additionally, regulating which staff have access to the data is another major concern. While MNPD's FUSUS website states that only authorized users within MNPD will have access to the FUSUS database, without specific policy or codes, it is impossible to know who and how many individuals within MNPD are authorized to view FUSUS data and what training they have on using it. This is especially crucial since the FUSUS database is easily accessible, even from just a smartphone. Furthermore, while FUSUS data is not automatically shared with other police departments and law enforcement agencies, it makes it much easier to share data police data with other entities, specifically those that are also using FUSUS technology. In contrast, Metro Code 13.08.080 limits the number of users that have access to LPR information, sets training requirements, and establishes securities around sharing the data with other users, entities, and even other law enforcement agencies. Since there is no defined FUSUS policy, it is unclear as to what the limits of sharing FUSUS data are, and if FUSUS data must comply with the same standards and regulations that MNPD has for their original data.

Lastly, FUSUS advertises the ability to use AI Technology to run video algorithms using its software. While FUSUS advertises that it does not use facial recognition software, that does not mean that the devices are incapable of facial recognition features. FUSUS states that it does not implement facial recognition features, but what police departments choose to do with the data is beyond FUSUS's terms and conditions. If police departments wanted to run their own facial recognition programs using additional third-party software, they easily could. In fact, while South Bend, Indiana has robust FUSUS

[43] https://www.aclu.org/report/community-control-over-police-surveillance-technology-101#:~:text=The%20proliferation%20in%20local%20police,color%20and%20low%2Dincome%20communities.
[44] https://www.nashville.gov/sites/default/files/2023-01/License-Plate-Reader-Pilot-Program-Ordinance.pdf?ct=1673289099#:~:text=1%20of%209-,13.08.,way%20requires%20metropolitan%20council%20approval.
[45] https://www.eff.org/deeplinks/2023/05/neighborhood-watch-out-cops-are-incorporating-private-cameras-their-real-time

policy, they are implementing facial recognition technology[46] alongside their FUSUS roll out. Considering South Bend has some of the strongest policy on FUSUS, the fact that even their policy makes no mention of facial recognition technology is worrisome given their plans to roll out facial recognition technology concurrently with FUSUS.

Conclusion

While a larger rollout of FUSUS cannot happen until the new Metro Council is sworn in, given that LPRs were put to vote before Metro Council three different times prior to their passage this session, it is likely that FUSUS will make a return before the Metro Council. In the meantime, it is still unclear what will happen to the FUSUS devices that MNPD and members of the public have already purchased. The FUSUS terms and conditions agreement provide some information, as it is effective for a period of five years upon signing and can only be terminated with written notice. Without termination, the agreement will automatically renew. Thus, any private partner in Nashville who has signed the FUSUS terms and agreements will likely still be included in the agreement unless MNPD's lapse in contract specifically terminates the terms and conditions.

The uncertainty around what will happen to the existing FUSUS devices poses another dilemma; the citizens of Nashville know very little about FUSUS, despite MNPD having a contract with them for nearly a year. There needs to be more transparency, communication, and trust with the community on what FUSUS is, especially since members of the public can buy into FUSUS from a FUSUS-run MNPD website. Private partners in Nashville must know what kind of deal they are entering with MNPD and FUSUS when purchasing the technology, and the Nashville community needs to know the full extent of the technology surveilling them, in both public and private spaces. Public forums that educate the citizens of Nashville about what FUSUS is and demonstrate what FUSUS integration and the real-time crime center look like from an operational standpoint would make a substantial difference in the public's knowledge and understanding of FUSUS. In addition, releasing a list of the locations that have FUSUS-linked cameras, and creating a plan that incorporates MNCO in the audit would make a substantial difference in improving public perceptions of safety and transparency with MNPD.

Most pressingly, expanding FUSUS without specific policy would be a concerning proposition; Nashville already has over 900 registered devices and 200 integrated devices, which significantly outnumber the estimated 117 LPR cameras that will be installed in the full roll out of MNPD's LPR program. While LPRs only capture license plates that drive through public rights-of-way, FUSUS-linked cameras have the potential to be a much more comprehensive surveillance technology that can capture data in both public and private spaces. While LPRs have had a draft policy even before the LPR pilot program started, FUSUS was rolled out in September of 2022, and does not even have a draft policy or SOP. The need for a policy is especially crucial as cities regardless of whether they have FUSUS-specific policies or not have exponentially increased the number of FUSUS-linked devices in just the span of a few years. A police surveillance apparatus at the scale of what FUSUS advertises without policy could

[46] https://www.southbendtribune.com/story/news/local/2022/12/29/south-bend-police-roll-out-real-time-crime-center-technology/69750223007/

lead to potential issues regarding constitutional protections, privacy erasure, and lack of community trust.