



ADVISORY COMMISSION ON POLICING

October 13, 2025

The Honorable Kate Stewart, President
Montgomery County Council
100 Maryland Avenue
Rockville, MD 20850

Re: Police Radio Encryption

Dear President Stewart and Members of the County Council:

Pursuant to the charter of the Advisory Commission on Policing (ACP), this letter provides the ACP's advice regarding Montgomery County Police Department's (MCPD) encryption of its radio dispatch communications.

We urge the County Council to:

- 1) Require MCPD to establish a delayed feed mechanism that would allow the press, public advocates, and the public access to redacted police radio dispatch communications.
- 2) Provide the funding required to purchase the necessary equipment, tools, and staffing to redact health and personally identifiable information protected by law, as well as other information needed to protect witnesses and victims.
- 3) Work with MCPD and public advocates to develop redaction rules that adequately balance the public's need to know with the need to protect police operations and tactics, as well as protecting privacy, witnesses and victims.

This letter pertains only to the encryption of radio dispatch communications, as MCPD has already been encrypting for years multiple talk groups, including tactical talk groups. MCPD states that encrypting radio dispatch communications addresses compliance requirements with the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII), and recommendations of the Federal Partnership for Interoperable Communications (FPIC); privacy concerns of witnesses, victims, and

Advisory Commission on Policing

100 Maryland Avenue • 240-777-7900 • www.montgomerycountymd.gov

suspects; as well as preventing media and public interference, and bad actors from monitoring police responses during the planning and commission of crimes, including the ambush of police officers.¹

While some of these arguments do not strike us as persuasive, encryption of police radio dispatch calls could help protect witnesses and victims, prevent bad actors from taking advantage of open radio dispatch communications, and promote interoperability with other agencies that already encrypt, or will encrypt, their own communications.² However, we are concerned about the major loss of transparency resulting from the encryption of dispatch radio communications that used to be available to the press and the public through scanners or apps.

Unaddressed, this loss of transparency would run counter MCPD's stated commitment to Community Policing and willingness to promote transparency and hold itself accountable. It would also run counter the County government's reform efforts over the last half-decade to ensure a more effective and equitable policing for all. In short, it would be a significant step backwards in developing the kind of public safety that meets the aspirations of County residents.

Our concerns are not driven by community sensibilities alone, they are also driven by an interest in supporting MCPD and helping the police officers serving our community. Though MCPD sees itself in the best position to provide accurate information to the public on law enforcement matters, the lack of transparency generated by encryption cannot be remedied solely by a proactive Public Information Office (PIO) or by timely and complete responses to Maryland's Public Information Act (MPIA) requests. In placing itself in the position of being the source of information to the public, MCPD's intentions could backfire, generating unnecessary suspicion and distrust. In today's environment, rife with conspiracy theories, hard-earned efforts to build community trust over the years could be undone by a single unanticipated incident.

Our concerns are not unique. Colorado passed a law in 2021 that requires any police department that fully encrypts its communications system to adopt a "communications access policy" allowing media

¹ See p. 3, in Susan J. Farag, Response to Council Questions in Briefing: Police Radio Encryption, Staff Report for the July 7, 2005 Public Safety (PS) Committee work session on Police Radio Encryption.

https://montgomerycountymd.granicus.com/MetaViewer.php?view_id=169&event_id=16537&meta_id=198855

² Note: HIPAA specifically applies to "health care workers" and "health plans," and it is not clear to us whether this federal law also applies to MCPD communications. Similarly, we are not aware of any PII law applicable to MCPD radio dispatch communications. Regarding compliance with FPIC recommendations, the Cybersecurity and Infrastructure Security Agency (CISA) website notes that the "*Federal Partnership for Interoperable Communications (FPIC) as a body has been sunset in order to streamline efforts that support public safety communications. The removal of this material eliminates redundancy and enhances the mission critical role of SAFECOM as a principal coordination mechanism authorized in statute.*" See <https://www.cisa.gov/safecom/fpic-products>. Finally, MCPD has not provided any examples of interference with police operations by member of the press or of members of the public endangering themselves or escalating a situation because of access to police radio dispatch communications. These strike us as speculative scenarios.

access to primary dispatch channels via scanners or other technology and should include provisions like media credential verification and fees to cover costs of equipment access.³ New York state lawmakers have passed a bill to preserve media access to police radio feeds, requiring police departments to grant journalists access to their encrypted radio communications. Other jurisdictions, like Baltimore City, have entered an agreement with *Broadcastify*, an online scanner service, to delay its dispatch feeds for 15 minutes.⁴

We believe that public safety is not the sole responsibility of MCPD. Rather, it is a responsibility that we share with the community, county government and MCPD. We are also cognizant that general mandates, especially those that are unfunded, are ineffective. Moreover, mechanisms that allow members of the media to be credentialed and gain access through licensed equipment are too restrictive and pose an unreasonable burden on already strained local media organizations.

Therefore, we urge the Council to mandate and fund a mechanism to enable public access to redacted streaming of police radio dispatch communications on a time-delayed basis. The Council should, in consultation with MCPD and public advocates, develop rules governing what can and cannot be redacted. The additional financial and staffing resources needed to fund such a delayed streaming may be significant, especially in the current fiscal environment, but we believe they are essential to safeguarding the transparency of our police department.

We hope you find this letter useful. Please feel free to contact us if you have any questions regarding this matter.

Sincerely,

Rev. Brian Bellamy
Chair, Advisory Commission on Policing,

CC: Marc Yamada, Chief, MCPD
Dawn Luedtke, Chair, Criminal Justice Coordinating Commission
Bishop Paul L. Walker Sr., Chair, Police Accountability Board
Hon. William England, Chair, Commission on Human Rights

³ See McNeil, Zane, "Police Are Increasingly Encrypting Their Radios to Block Scrutiny by Journalists," in Truthout, <https://truthout.org/articles/police-are-increasingly-encrypting-their-radios-to-block-scrutiny-by-journalists/>

⁴ According to its website, *Broadcastify* has streaming agreements with eight law enforcement agencies in Maryland, including: Baltimore City Police, Carroll County Law Enforcement, Charles County Law Enforcement, Frederick County Sheriff, FCSO Dispatch, Frederick County Fire and EMS, State Police, Howard County Police, Fire and EMS, Maryland State Police Barracks I, Talbot County, Worcester County Fire and EMS, State Police and Highway. See: <https://www.broadcastify.com/listen/std/24>