
Government of the District of Columbia



Metropolitan Police Department

Testimony of
Cathy L. Lanier
Chief of Police

***The Encryption of
Metropolitan Police Department Radios***

Committee on the Judiciary
Phil Mendelson, Chair
Council of the District of Columbia
November 4, 2011

John A. Wilson Building, Room 412
1350 Pennsylvania Avenue, NW
Washington, DC 20004

Good afternoon, Councilmember Mendelson, members of the Committee, and guests. There has been a great deal of media attention devoted to the issue of the Metropolitan Police Department's (MPD) encryption of its radio communication, and I would like to brief you on why this move has become imperative for public safety. I am also glad to have an opportunity to stress my commitment to maintaining our strong partnership with the media, which plays a vital role in public safety in the District.

Beginning in September, MPD moved to fully encrypt radio transmissions to ensure that law enforcement is not broadcasting information that would endanger the safety and privacy of victims, witnesses, officers, and the public at large. In order for police to do our jobs, we need to communicate vital information immediately and without hesitation. However, as anyone who has listened to police radio communications knows, this may include detailed and sensitive information about victims, witnesses, or suspects. Encryption can help to:

- **Deter crime:** Criminals have used scanners to track police activity to plan and then ultimately commit crimes. This is especially easy to do now with Smartphone technology.
- **Apprehend criminals:** Wanted offenders have used scanners to elude police and to destroy evidence before the police arrive.
- **Promote officer safety:** Encryption helps officers to stay one-step ahead of the criminal, rather than the criminal knowing an officer's next move.
- **Prevent identity theft:** Names, birthdates, addresses, and other private information are routinely transmitted over police radios for records checks and other purposes. This is often all that criminals need to steal one's identity.
- **Protect witness and victim information:** Some witnesses will not call police if they know that their name will be broadcast on a radio. Victim identities need to be protected to allow for proper notifications to relatives. Other sensitive information, such as the physical and mental health of involved parties, should not be broadcast for everyone with a scanner to hear.
- **Promote national security:** Terrorists will use all technology available, including scanners, to plan an attack and target first responders. Encryption will make the District a harder target for terrorists to attack.

We have long been concerned about these issues, and have often found scanners in criminals' homes or businesses. However this has become a more critical threat to public safety because of advances in technology. Last year, with Capitol Hill plagued by a rash of carjackings, we began to suspect that the perpetrators were listening to our communications because even when we had deployed all available resources, they were still eluding capture. Only after we changed our techniques to not broadcast over the radio were we able to capture these dangerous criminals. Whereas listeners used to be tied to stationary scanners, new technology has allowed people – and especially criminals – to listen to police communications on a Smartphone from anywhere. When a potential criminal can ask how they can evade capture and learn, “There's an app for that!” it's time to change practices. The number of cases where we have seen this is growing. The most alarming include:

- In the Seventh District, a sergeant began to suspect that individuals selling drugs at a local laundromat were somehow monitoring communication. He tested this theory by going over the air to instruct units to meet him at the location, and then watched the subjects immediately clear the building.

- In the Second District, 13 burglaries were committed by a group of five offenders who would listen to radio communications on their Smartphones and leave the scene before police arrived. Fortunately we eventually caught them, and they are now serving sentences of five to 12 years, but not before they had victimized 13 homeowners. A similar scenario happened in Fairfax and Loudon Counties, except the burglars hit 29 homes before being caught.
- In Ohio, a man convicted of a misdemeanor tax violation plotted to toss pipe bombs into the homes of the judge, mayor, police chief and prosecutor before his sentencing. He planned to strike at 2:00 a.m., carrying a police scanner and a firearm, in case he was caught. The bombs were to have a one minute fuse so that the target would have time to come check on the noise and then be killed by the bomb.¹
- The worst case that we know of did not happen in the District, but should be a wake-up call for police and the public everywhere. During a home invasion, the offender shot, but did not kill, a person in the home. While he was in another part of the house fatally shooting another victim, the first victim called 911. The offender heard the police communications over a portable scanner, and came back to fatally shoot the first victim.

We do not want to wait for the same tragic outcome to happen in the District before we take action. And contrary to what some believe, MPD is not the only agency moving to full encryption. Other United States cities or counties include Jacksonville, Florida, Santa Monica, California, and Nassau County, New York. Locally, the Federal Bureau of Investigation and the Drug Enforcement Administration are both encrypted. The US Capitol Police will be encrypted in 2013. Internationally, law enforcement communications in the United Kingdom and Ireland are fully encrypted, as well as major cities in Canada. And many US jurisdictions are moving towards full encryption, including the Los Angeles Sheriff's Department. As the problem of criminals listening to police communications on mobile communications devices grows, other jurisdictions will continue to move to this. A survey of major police departments revealed that cost was the primary factor preventing more jurisdictions from moving to full encryption.

Technology has changed how criminals operate, and we all need to change our operations as well in order to protect the public and our officers. Fortunately, technology is also providing solutions for continuing communications between police and public and media. The Department has more than 14,000 followers on our email groups, DC Alert, and Facebook. In October alone, 143 DC Alerts were sent related to serious crimes. Recently, we have also begun sending information out on Twitter. We began in August with 24 tweets, which grew to 120 in September, and to 534 in October. After just two full months in operation, the number of tweets has more than quadrupled, and we have more than 2,000 followers. This information is sent out from the Command Information Center (CIC), MPD's nerve center that processes tactical information 24 hours a day, seven days a week. As information on a critical incident comes in, the CIC first calls the Chief of Police and top command officials, then sends out an alert to the Department, and lastly sends out alerts to the public. Depending on how busy the CIC is at the time, these alerts may be virtually simultaneous. For example, on Halloween all of the shootings were sent out via DC Alert and Twitter, and there was no shortage of media coverage of the events. Moreover, for any crime for which medical attention is required, the Fire and Emergency Medical Services Department still broadcasts their radio communications.

¹ "Plot to Kill Judge Fails, But Leaves Aftershocks," *Benchmark*. Vol. 29, No. 2. Summer 2006.

In addition, there are many, many more ways to access information about crimes. I don't know of any other police agency that makes available as much information as MPD does. We have an interactive crime mapping application for the public (www.crimemap.dc.gov), annual reports, flyers, and community meetings. We have press conferences, briefings, on-scene radio and television interviews, Amber Alerts and press releases. Pursuant to District law, police reports are also available to the public and the media. Our Public Information Officer responds to questions from the media 24-hours a day. Even more importantly, members of the media call me and my command officials directly anytime, day or night, to get or confirm information.

As everyone testifying here today knows, police rely on the media to alert the public as much as the media relies on us to provide information. I am committed to continuing this strong partnership to ensure that we are serving the residents of and visitors to the District. I have discussed this issue directly with some of you here and others and I believe that together we can find good solutions. For instance, I am exploring having the CIC broadcast out on our Citywide One channel brief information as soon as it is confirmed. I have already gotten a better understanding of what you need from our conversations. For instance, if there is a traffic tie up, you, and the public, need to know not just what intersection to avoid, but the best route to travel around it. I know how important it is not just to receive intelligence, but to receive *actionable* intelligence. This is the same principal that we have been working on with federal agencies for years. It is very challenging to take in all the information that is available. I can't even monitor all seven patrol channels at a time. We can help alleviate this avalanche of information by broadcasting information as soon as it is confirmed and available, helping the media to avoid wild goose chases and focus their resources.

However, what we are not willing to do is to give the media radios or share the encryption key. The former would be expensive; the latter, contrary to the objective. The National Institute of Justice sums it up well: "Poor key management practices negates any benefits of voice encryption and may result in a comprised system."² The Department would have no way to ensure that members of the media would maintain the confidentiality of the keys or the radios. We could not discriminate between different media outlets without allegations of favoritism, at best, or of obstructing First Amendment rights. If a breach were discovered, it would require extensive and expensive efforts to reset the entire system, not just for the Department, but with our law enforcement partners with whom we would share the key. This proposal is illogical and non-negotiable.

In short, I hope it is absolutely clear that MPD is not trying to keep information from the media or the public. Not only are we stepping up other means of communication, but there is significant, detailed information contained in existing resources, such as the police reports that we are required by law to make public. I recognize that this may not be as instantaneous as radio communications, but the public expects that the priority for police is to protect them – not to sell newspapers. Indeed, our previous efforts to protect information in police reports about victims and witnesses of sex assaults and other violent crimes have failed because there is an explicit right in the law of the public to view this information. In many ways, there are more protections in the law for arrestees than for victims. But there is no right to listen to police communications in which we need to share far more information than that which is open or important to the public. Given this, I sincerely hope that we can work together with the media to ensure that all of us are truly protecting the best interests of the public.

² "Voice Encryption for Radios." US Department of Justice, Office of Justice Programs, National Institute of Justice. NCJ217103. March 2007.