

Now hear this: Emergency agencies turn off radio encryption

October 11 2016, by Dave Collins



In this Thursday, Oct. 6, 2016 photo, a radio in a police cruiser sits between the front seats in Naugatuck, Conn. While many police departments around the country are concealing their dispatch communications through encryption, Naugatuck, among others, has decided to keep theirs open to the public. Some police chiefs have said their officers may not be able to communicate on encrypted systems with first-responders in neighboring towns. (AP Photo/Dave Collins)

Some police and fire departments are bucking a trend to conceal dispatch communications from the public, acknowledging that radio encryption has the potential to backfire and put first responders in danger.

Agencies with digital radio systems have turned off the encryption to their main dispatching channels and others have decided not to turn it on. They say their officers and firefighters may not be heard during emergencies by responders at neighboring departments with radio systems that either don't have access to their encrypted channels or aren't advanced enough to have encryption capability.

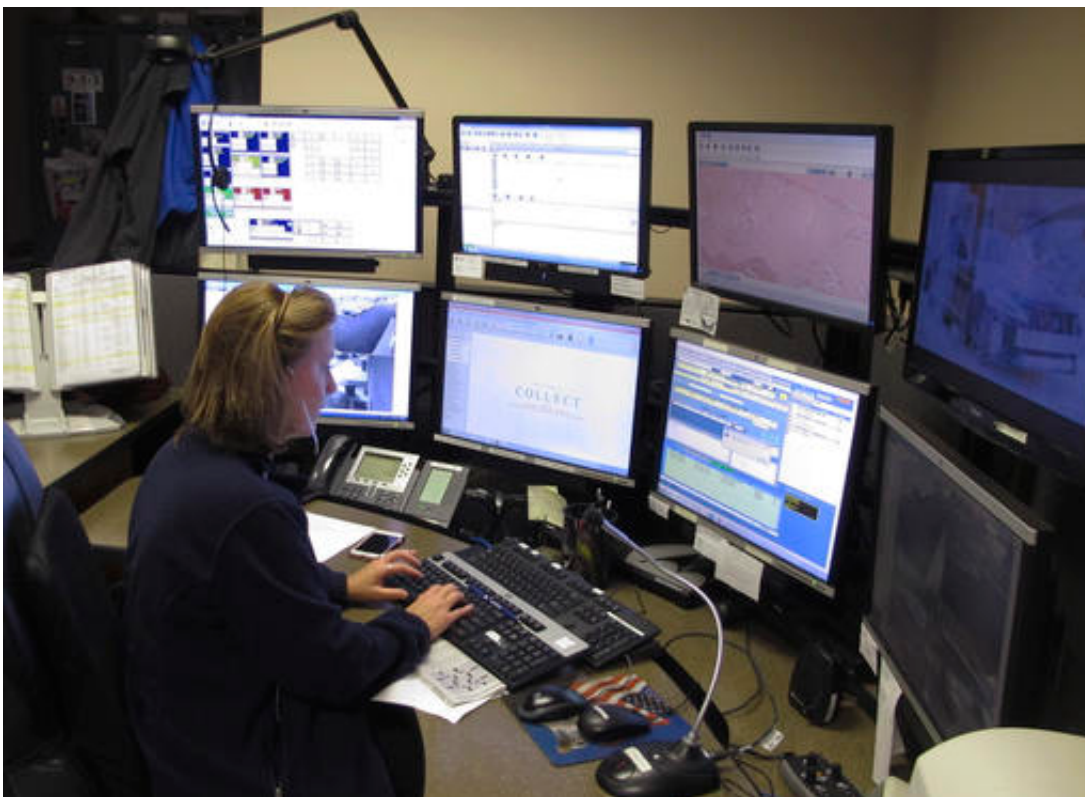
Officials also say they are addressing concerns from critics who argue encryption decreases police transparency at a time when it is needed, especially in the wake of shootings of unarmed black people by police officers.

"The overwhelming opinion of encryption is that it works great for preplanned tactical environments like SWAT teams staging a situation," said Eddie Reyes, deputy chief of Amtrak police and chairman of the International Association of Chiefs of Police communications and technology committee.

"But for day-to-day operations where officers are going across borders in emergency pursuits or foot pursuits, that's where it tends to break down," he said. "A good number of agencies are still operating on antiquated systems and would not have the ability to accept encryption."

When Reyes was working for Arlington, Virginia, police in 2006, he said, an officer who fatally shot a teenager outside a restaurant inadvertently switched over to encryption mode on his portable radio. There was temporary chaos on the radio when officers en route couldn't communicate with the officer in the shooting because their radios

weren't in encryption mode, Reyes said.



In this Thursday, Oct. 6, 2016 photo, dispatcher Kelly Orsini works at her communications desk at the police department in Naugatuck, Conn. While many police departments around the country are concealing their dispatch communications through encryption, Naugatuck, among others, has decided to keep theirs open to the public. Some police chiefs have said their officers may not be able to communicate on encrypted systems with first-responders in neighboring towns. (AP Photo/Dave Collins)

A slow trend continues toward encryption, which has been around for years. It hides communications from public airwaves by modifying voice signals with coded algorithms, preventing people from listening via radio scanners, the internet and cellphone apps. Only people with encryption

"keys," the information needed to access the encrypted channels, can listen.

Open government advocates say the practice withholds crucial information about emergency situations from the public. Concerns also have been raised by news organizations, which say it cuts off journalists who monitor public safety broadcasts from being alerted to major events.

Police officials say they're worried about the safety of their officers, because criminals have been known to track officers' movements by listening to police communications. They also say they want to prevent the public broadcasting of people's personal information, including medical histories and juveniles' names.

They further cite violence against officers around the country over the past few months and the response to the Boston Marathon bombings in 2013, when people listening to police communications posted misleading and inaccurate information on social media.

Among police departments that have recently encrypted all communications are those in Anchorage, Alaska; Riverside, California; Manchester, New Hampshire; and Newtown, Connecticut.

"What happened this summer really culminated in making the decision," Newtown Police Chief James Viadero said, referring to violence against police. "I had a legitimate concern for my officers."



In this Thursday, Oct. 6, 2016 photo, Police Chief Christopher Edson points out the department's dispatching communications system in Naugatuck, Conn. While many police departments around the country are concealing their dispatch communications through encryption, Naugatuck, among others, has decided to keep theirs open to the public. Some police chiefs have said their officers may not be able to communicate on encrypted systems with first-responders in neighboring towns. (AP Photo/Dave Collins)

Other departments are taking the opposite approach. Police in New Orleans; Spokane, Washington; and other cities have vowed not to encrypt their main dispatch channels. Others that had encrypted their communications have turned it off.

Police in Mansfield, Massachusetts, turned off their encryption more than a year ago after officers expressed concern they couldn't talk with counterparts in some neighboring towns, Police Chief Ronald Sellon said. Mansfield is home to the 20,000-seat Xfinity Center outdoor

amphitheater, and there were worries about communications with other agencies if there was a mass casualty event at the theater.

Last year, Washington, D.C., officials switched off the encryption for fire communications. The move came after firefighters had problems using their radios in a subway tunnel during an emergency response. The tunnel filled with smoke because of an electrical malfunction, killing one person and sickening dozens more.

The Metro transit agency, which had a radio system in the subway that allowed below-ground communications by city firefighters, said the radio problems were the result of the fire department changing its own radio system, including adding encryption, without telling the transit agency. City officials denied encryption caused the problems.

Police in Naugatuck, Connecticut, like many departments, are keeping their main dispatch channel open to the public while maintaining encrypted channels to use during tactical operations.

Naugatuck Police Chief Christopher Edson cited the need to be able to communicate with other emergency responders, as well as the expense of [encryption](#), which can cost several hundred dollars per radio to implement. Another issue was not wanting to block out the public, he said.

"We also want to be transparent," he said, "during this particular climate in the country."

© 2016 The Associated Press. All rights reserved.

Citation: Now hear this: Emergency agencies turn off radio encryption (2016, October 11) retrieved 25 April 2024 from <https://phys.org/news/2016-10-emergency-agencies-radio-encryption.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.