

SURVEILLANCE TECHNOLOGY IMPACT REPORT

Department:	Executive
Division or Unit (if applicable):	Communications Office
Submitted by:	Jeremy Warnick
Date:	4/9/26
Surveillance Technology:	SMS Non-Emergency Alert Notifications

1. Describe how the proposed Surveillance Technology will work, including how it will collect Surveillance Data.

A mass notification system can enable the City to create and issue strategic communications to residents and distribute them for consumption based on residents' preferences. We are looking to explore platforms that would allow the City -- via the Communications and Community Engagement Office -- the ability to conduct outreach via SMS/text messaging.

The Communications and Community Engagement Office currently has no way of conducting SMS outreach for non-emergency related communications. It is reliant on CodeRed, Tip411 and other public safety-related tools.

Adding SMS/text messaging for non-emergency situations could serve as a critical tool and complement the City's existing digital, print, and in-person outreach.

The Communications and Community Engagement Office is interested in conducting a no-cost pilot to measure the effectiveness of this tool. If proven effective, the Office would look to extend the service agreement.

The platform functions as a managed communications delivery service — not a surveillance, analytics, or data aggregation system. The system operator would not independently collect, track, or harvest constituent data (e.g. no location data, no device metadata, no behavioral tracking, no passive data collection). The platform operates exclusively on information that users voluntarily provide through City and system-operator hosted webforms (e.g. name, email and/or mobile phone number, communications preferences). The system operator would not sell, share, or use

constituent data for any purpose beyond delivering the contracted communications services.

2. What is the purpose of the Surveillance Technology?

- Analyzing and managing communications service delivery;
- Targeting communications to verified residents and responding to any questions, issues or concerns sent via the system (e.g. resident seeks additional details on a road closure or extended event notice);
- Amplifying and optimizing communication with community members, particularly at a hyper-targeted level. Ideally, this would help the Communications and Community Engagement Office test potential impact (both the application and notifications at a broader scale) by leveraging a platform for targeted outreach in some defined areas where there are issues or opportunities (e.g. residents whose preference is not email or social media; with residents where there was low parking ban compliance during the Snow Emergency Parking Ban).

3. Where will the Surveillance Technology be deployed? When?

The web application would initially be housed on three accounts in the Communications and Community Engagement Office. It could be downloaded to other accounts in the Communications and Community Engagement Office with Department head approval. A pilot could be available for use anytime in the first half of 2026 following onboarding and training sessions.

4. What privacy impact will the Surveillance Technology have?

The web application will initially include resident phone/SMS contact data that is sourced by the web application company and then layered on top of publicly available voter registration data in Cambridge.

While residents are initially opted in to receive the SMS/text message for the pilot and any extended service agreements, they would have the option to opt-out from any future SMS/text messages sent by the City at any time.

This meets the [Telephone Consumer Protection Act](#) (TCPA), passed by Congress in 1991, which protects consumers from unwanted marketing calls and text messages¹. Furthermore, it also meets the Cellular Telecommunications Industry Association (CTIA) messaging guidelines used by mobile carriers.

Any other data would be associated with inbound communications from users who respond to messages from the City (e.g. mobile phone number from which a reply was sent, text content of the reply message, and a timestamp of a reply). The Communications and Community Engagement Office would address these privacy impacts by limiting access to designated employees in the office. Access would be password protected, and the employees would receive detailed training on best practices for protecting personal information.

5. What are the fiscal costs of the Surveillance Technology, including initial costs, ongoing maintenance and personnel costs, and source of funds?

- Initial costs - 10,000 text credits would be provided for free for the pilot.
- Ongoing maintenance - If the Communications and Community Engagement Office were to extend service after the pilot following analysis of its effectiveness, the City could have access to unlimited text credits each year for \$9,500.
- Source of funds – If extended, the initial annual cost would be addressed under E-Gov and then integrated into the Communications and Community Engagement Office's Operating costs thereafter, if evaluations prove its value as anticipated.

¹ Under TCPA rules, companies must respect a person's request to stop receiving marketing texts.