ASPEN POLICY ACADEMY
aspen institute

POLICY BRIEF

# A City Controlled Data Privacy System to Protect Sensitive Healthcare Data

Evîn Cheikosman

## EXECUTIVE SUMMARY

**The Mayor's Office of Innovation should implement a city controlled data privacy system to prevent unauthorized parties from accessing sensitive reproductive and gender affirming healthcare data collected during the execution of certain law enforcement activities.** This privacy system should use an API wrapper – a software tool that sits between 2 computer systems – as an intermediary to remove identifying details (in this case, sensitive healthcare data) before it is shared with law enforcement. Such a privacy system is particularly necessary in the context of reverse warrants, which allow law enforcement to compel tech companies to reveal the identities of people based on location or search history. The scale of this issue is significant; between 2018 and 2020, Google alone received over 5,700 reverse warrants from states with anti-abortion and anti-LGBTQI legislation. By leveraging the city's existing infrastructure, this solution can be swiftly implemented to address privacy violations posed by reverse warrants.

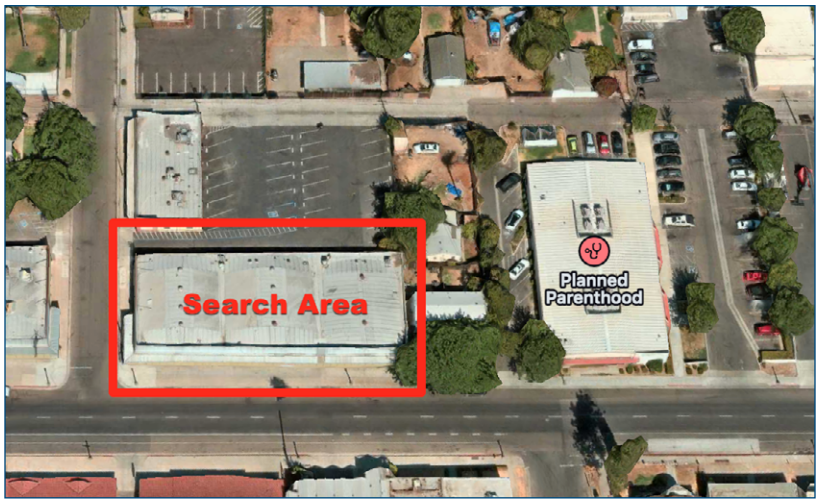
## BACKGROUND

Reverse warrants, including reverse keyword and reverse location (also known as geofence) warrants, compel tech companies to provide user data based on search terms or location. While these warrants may be useful for certain investigations, they also capture the information of countless innocent individuals. Google, a primary recipient of these warrants, received 11,554 such requests across the United States in 2020, a dramatic increase from 982 in 2018. Geofence warrants accounted for more than 25% of Google's total warrant requests in the United States, with California law enforcement submitting more reverse warrant requests than any other state.

To learn more about this project, please visit aspenpolicyacademy.org

aspen institute

Recent developments underscore the need for robust data protection. Despite Google's efforts to encrypt Android location history, studies show that the company continues to collect and retain sensitive location data, including visits to abortion clinics. This persistence of data collection highlights the ongoing privacy risks, particularly for those seeking sensitive healthcare services.




At the state level, AB 793, introduced by Assemblymember Mia Bonta, aims to prohibit reverse location and reverse keyword demands by government entities, reflecting California's commitment to protecting reproductive and LGBTQI rights and digital privacy.

Locally, the recently passed San Francisco Reproductive Freedom Act would focus on safeguarding access to abortions and protecting healthcare providers, but would not explicitly address privacy risks associated with reverse warrants in the context of reproductive and gender affirming care.

At the federal level, in August 2024, an appeals court ruled that geofence warrants are unconstitutional, marking a significant legal precedent against this surveillance technique. The 5th US Circuit Court of Appeals found that these warrants violate the 4th Amendment's protections against unreasonable searches. While this ruling does not cover California, it underscores the urgency and importance of implementing robust privacy protections at the local level, as proposed in this memo, to safeguard citizens' sensitive data even as the legal landscape continues to evolve.

## RECOMMENDATION

**The Mayor's Office of Innovation should develop and implement a city controlled data privacy system to protect sensitive healthcare information before it is shared with law enforcement during reverse warrant requests.** This system would use a software tool called an API wrapper to encrypt and remove identifying details from the data before they are made available to law enforcement. An API wrapper system is essential to protect the privacy of individuals seeking reproductive and gender-affirming healthcare. Reverse warrants can compel tech companies to disclose sensitive data, putting individuals at risk of privacy violations. Significant risks persist from reverse warrants and data breaches, particularly as other states enact laws targeting reproductive and LGBTQI+ rights. By implementing this system, San Francisco can control and secure the data before it is shared, aligning with the City's commitment to protecting digital privacy and healthcare access.

### API Wrapper Process

**Data Encryption:** Upon receiving a reverse warrant, tech companies would send the data to San Francisco's secure API wrapper system instead of directly to law enforcement. The API wrapper would immediately encrypt the raw data.

**Data Sanitization:** The system would use advanced techniques to remove or hide any sensitive healthcare information while preserving necessary details for legitimate investigations.

**Secure Storage and Access:** Sanitized data would be securely stored in a city managed database, accessible only through a secure portal with strong authentication. The entire process would be logged for full accountability.

### Data Retention and Third Party Vendor Security

**Retention Policies:** Data would be retained only for the minimum period required to fulfill legal obligations and would be permanently deleted thereafter.

**Vendor Security Standards:** Any third party vendors involved in the system would comply with stringent city privacy and security standards.

### Accountability and Remedial Actions

**Penalties for Violations:** Unauthorized access would result in penalties, including financial consequences and mandatory corrective actions.

**Remedial Actions:** In case of a breach, immediate remedial actions would be taken, including notifying affected individuals and enhancing security measures.

The success of this system would build upon the city's DataSF platform, which already securely manages and anonymizes data.

## IMPLEMENTATION

**Phase 1:** Analyze the DataSF framework to design a modular API wrapper system capable of encrypting, de-identifying, and securely storing data. Concurrently, establish legal agreements outlining data sharing protocols, privacy requirements, and vendor security standards.

**Phase 2:** Develop the core API wrapper components, focusing on secure data processing and integration. Create a secure portal for law enforcement with built-in authentication and logging features.

**Phase 3:** Conduct thorough testing, security audits, and performance evaluations. Roll out a pilot launch with selected tech companies, followed by full implementation and ongoing support.

## BUDGET CONSIDERATIONS

**Estimated cost:** $250,000 to $500,000, including system development, integration, legal compliance, testing, security audits, and first-year maintenance. This estimate is based on similar initiatives in other major cities and accounts for the complexity of secure API development and integration requirements. While the actual cost may vary based on specific implementation details, this range provides a realistic starting point for budgetary planning.

*Please see the following documents for more information:*
*Case Studies, a document presenting successful strategies for protecting sensitive data;*
*Data Sharing Agreement, a sample agreement between the City and County of San Francisco and a technology company;*
*One-Pager, a document defining reverse warrants;* ***and***
*Operational Plan, a plan to develop and implement an API wrapper system.*