ASPEN POLICY ACADEMY
aspen institute

Development and Implementation of City Owned API Wrapper System

Evîn Cheikosman

OBJECTIVE

To implement a city controlled API wrapper system to protect sensitive reproductive and gender affirming healthcare data from unauthorized access during reverse warrant requests. This system would ensure that only necessary and sanitized data are shared with law enforcement, thereby upholding the privacy rights of San Francisco residents.

OPERATIONAL OVERVIEW

The API wrapper would act as an intermediary between tech companies and law enforcement, processing data requests under reverse warrants to ensure that sensitive healthcare information is encrypted, de-identified, and stored securely before any data are transmitted.

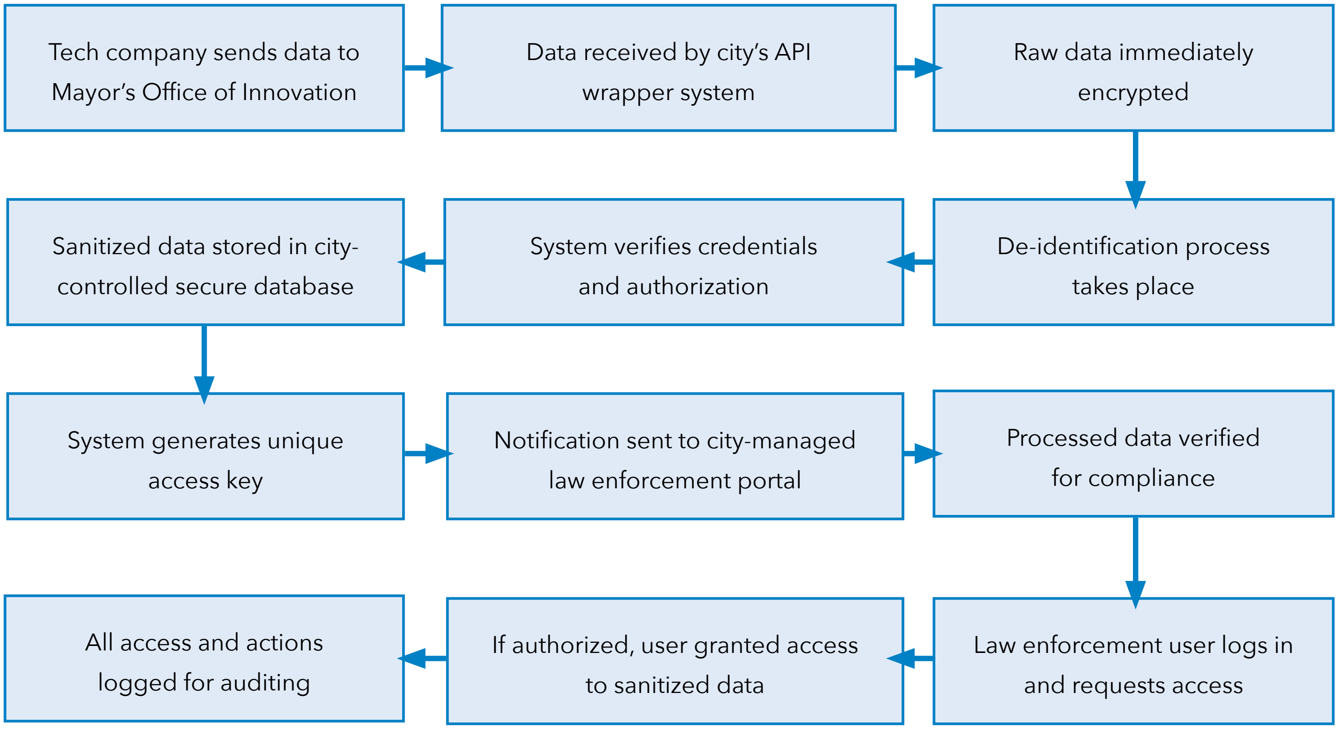
Tech company sends data to Mayor's Office of Innovation
Data received by city's API wrapper system
Raw data immediately encrypted
De-identification process takes place
System verifies credentials and authorization
Sanitized data stored in city-controlled secure database
System generates unique access key
Notification sent to city-managed law enforcement portal
Processed data verified for compliance
Law enforcement user logs in and requests access
If authorized, user granted access to sanitized data
All access and actions logged for auditing

Figure. Beginning at top left, this image illustrates the flow of data for the proposed API wrapper.

This system would leverage the existing DataSF platform, integrating with multiple tech company APIs while ensuring secure data processing and storage.

> *"The true work of innovation is not coming up with something big and new, but instead recombining things that already exist."*
>
> *Erik Brynjolfsson and Andrew McAfee*

KEY COMPONENTS

API Wrapper Development

a. **Design and Architecture:**

   i. **Front end:** The API wrapper would be designed with a user friendly interface for managing and processing data requests. It would allow for seamless integration with tech company APIs and provide a secure portal for law enforcement access.

   ii. **Back end:** The backend would handle data encryption, de-identification, and secure storage. It would use robust encryption standards and flexible architecture to adapt to varying tech company data structures.

b. **Integration:** The wrapper would integrate with tech companies' APIs to intercept data before they reach law enforcement. It would process these data, ensuring that sensitive information is either removed or anonymized.

c. **Testing:** The system would undergo rigorous testing, including security audits and performance evaluations, to ensure that it meets the highest standards of data protection and operational efficiency.

Legal and Regulatory Framework

a. **Data Sharing Agreements:** The City Attorney's Office would draft and negotiate agreements with tech companies, outlining protocols for data sharing, encryption, and de-identification processes.

b. **Compliance:** The system would comply with all relevant state and federal privacy laws, including the California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), and, if passed, the San Francisco Reproductive Freedom Act.

System Deployment

a. **Pilot Phase:** A pilot launch would be conducted with 1 or a selected group of tech companies to test the system's functionality and effectiveness. Feedback from this phase would inform necessary adjustments before full deployment.

b. **Full Implementation:** The API wrapper would be fully deployed across all participating tech companies, with ongoing monitoring to ensure seamless operation and integration.

Security and Monitoring

a. **Encryption and De-identification:** All data processed through the API wrapper would be encrypted, and sensitive healthcare information would be de-identified before any data are shared with law enforcement.

b. **Logging and Accountability:** Every interaction with the system would be logged, ensuring full transparency and accountability. These logs would be regularly reviewed to detect and address any unauthorized access attempts.

c. **Security Audits:** Regular security audits would be conducted to ensure that the system remains secure against emerging threats.

Evaluation and Reporting

a. **Performance Metrics:** Key performance indicators such as response time, accuracy of data processing, and user satisfaction would be tracked to measure the system's effectiveness.

b. **Quarterly Reports:** The Mayor's Office of Innovation would submit quarterly reports to the Board of Supervisors detailing the system's performance, including any incidents, system updates, and recommendations for further improvements.

RECOMMENDED CONTACTS

As San Francisco implements this API wrapper system, it should consider partnering with Google, since it is the main target of reverse warrants.

Point of contact: Rebecca Prozan, Director of the West Region for Government Affairs and Public Policy, Google (rprozan@google.com).

ADDITIONAL RESOURCES

To support the implementation of the API wrapper system, the City of San Francisco can benefit from several valuable resources. The **National Institute of Standards and Technology (NIST)** provides comprehensive guidelines on encryption and data protection through its Special Publication 800-53, which can be accessed here: NIST SP 800-53.

For best practices in API security and management, the **Open Web Application Security Project (OWASP)** offers detailed resources, including its API Security Top 10, available at OWASP API Security.

EXAMPLES OF SUCCESSFUL CITY SPECIFIC API WRAPPER IMPLEMENTATIONS

- **Los Angeles GeoHub:** This platform integrates various city datasets while ensuring compliance with privacy regulations. It provides a secure interface for accessing city data, including public and sensitive information. More details at LA GeoHub.
    - Direct contact for more information: **Eva Pereira, Chief Data Officer for the City of Los Angeles, eva.pereira@lacity.org**
- **Chicago Data Portal:** This system offers access to a wide range of city datasets with built-in privacy protections. It manages sensitive municipal data and ensures compliance with local data privacy laws. Learn more at Chicago Data Portal.
- **New York City Open Data:** This portal provides access to city datasets with mechanisms to safeguard sensitive information. It serves as a model for integrating API wrappers with strong privacy controls. More information at NYC Open Data.

While specific city owned API wrapper systems like the one proposed for San Francisco might not have a direct precedent, the above examples illustrate that many cities have successfully implemented systems with similar functionalities — controlling data flow, protecting sensitive information, and ensuring compliance with privacy regulations. These implementations demonstrate the feasibility and effectiveness of such systems in a municipal context.

ABOUT THE POLICY ACADEMY

The Aspen Policy Academy offers innovative training programs to equip leaders across sectors – from tech to climate, science to social impact – with the practical policy skills to craft solutions for society's most pressing challenges.

ASPEN POLICY ACADEMY aspen institute

aspen institute