

SUNSHINE ORDINANCE TASK FORCE  
AGENDA PACKET CONTENTS LISTComplaint CommitteeDate: March 21, 2023

<input checked="" type="checkbox"/>	Petition/Complaint
<input checked="" type="checkbox"/>	Respondent's Response
<input type="checkbox"/>	Petitioner/Complainant Rebuttal
<input type="checkbox"/>	Memorandum - Deputy City Attorney
<input type="checkbox"/>	Petitioner/Complainant
<input type="checkbox"/>	Supporting Documents
<input type="checkbox"/>	Respondent Supporting Documents
<input type="checkbox"/>	Public Correspondence
<input type="checkbox"/>	Order of Determination
<input type="checkbox"/>	Minutes
<input type="checkbox"/>	Administrator's Report
<input type="checkbox"/>	No Attachments

Petition/Complaint	Page: <u>917</u>
Respondent's Response	Page: <u>1089</u>
Petitioner/Complainant Rebuttal	Page: _____
Memorandum - Deputy City Attorney	Page: _____
Petitioner/Complainant	Page: _____
Supporting Documents	Page: _____
Respondent Supporting Documents	Page: _____
Public Correspondence	Page: _____
Order of Determination	Page: _____
Minutes	Page: _____
Administrator's Report	Page: _____
No Attachments	Page: _____

**OTHER**

<input type="checkbox"/>	_____

Page

Completed by: C. Leger Date 3/16/23

\* An asterisked item represents the cover sheet to a document that exceeds 25 pages.  
The complete document is in the file on a disk

**Sunshine Ordinance Task Force  
Complaint Summary**

File No. 23013 A-E

Chris Ward Kline v Department of Public Health (A)

Chris Ward Kline v Office of the Sheriff (B)

Chris Ward Kline v Mayors Office (C)

Chris Ward Kline v Department of Emergency Management (D)

Chris Ward Kline v SF Police Department (E)

Date filed with SOTF: 1/28/2023

Contact information:

Chris Kline ([ckblueaqua@gmail.com](mailto:ckblueaqua@gmail.com)) Complainant

Deirdre Hussey ([deirdre.hussey@sfdph.org](mailto:deirdre.hussey@sfdph.org)) Public Health; Paul Miyamoto

([paul.miymoto@sfgov.org](mailto:paul.miymoto@sfgov.org)) Sheriff's Office; Victor Lim ([victor.lim@sfgov.org](mailto:victor.lim@sfgov.org)) Dept. of Emergency Management; Lt. William Toomey ([william.toomey@sfgov.org](mailto:william.toomey@sfgov.org)) Police Dept. (Respondents)

---

**File No. 23013 A** Complaint filed by Chris Ward Kline against Department of Public Health (A) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013 B** Complaint filed by Chris Ward Kline against Office of the Sheriff (B) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013 C** Complaint filed by Chris Ward Kline against Mayors Office (C) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013 D** Complaint filed by Chris Ward Kline against Department of Emergency Management (D) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013 E** Complaint filed by Chris Ward Kline against A-E SF Police Department (E) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

---

**File No. 23013 A** Complaint filed by Chris Ward Kline against Department of Public Health (A) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

Request for all communications between Public and Chris Ward Kline that deal with the app Once Systems and Bitfocus, as well as any and all APPS.

DPH response stated that they conducted a search and the only result were emails send by Mr. Ward Kline himself.

**File No. 23013 B** Complaint filed by Chris Ward Kline against Office of the Sheriff (B) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

Request for all public records to include epidemiology, behavioral health surveillance to include communications from county to and from Chris Ward Kline. See file for additional details.

**File No. 23013 C** Complaint filed by Chris Ward Kline against Mayors Office (C) for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

It is unclear as to the exact nature of the request for records. There is a email sent to various departments requesting records but it is not clear what was requested from the submitted documents. The request is most likely for the following:

Electronic surveillance, Microphone Surveillance, Physical Surveillance and Technical Surveillance for both main files records and cross references.

**File No. 23013 D** Complaint filed by Chris Ward Kline against Department of Emergency Management (D for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

Electronic surveillance, Microphone Surveillance, Physical Surveillance and Technical Surveillance for both main files records and cross references.

**File No. 23013 E** Complaint filed by Chris Ward Kline against A-E SF Police Department (E) e for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

It is unclear as to the exact nature of the request for records. There is an email sent to various departments requesting records but it is not clear what was requested from the submitted documents. The request is most likely for the following:

Electronic surveillance, Microphone Surveillance, Physical Surveillance and Technical Surveillance for both main files records and cross references.

# Petition/Complaint



RECEIVED  
BOARD OF SUPERVISORS  
SAN FRANCISCO  
2023 FEB 13 AM 8:42

BY QJR

SUNSHINE ORDINANCE TASK FORCE

1 Dr. Carlton B. Goodlett Place, Room 244, San Francisco CA 94102

Tel. (415) 554-7724; Fax (415) 554-7854

<http://www.sfgov.org/sunshine>

SUNSHINE ORDINANCE COMPLAINT FORM

Complainant Name (Optional)

Date of Request:

Please identify the City Official(s) and/or Employee(s) against whom the complaint is being made:

Please identify the Officials' and/or Employees' Board, Commission, Task Force, Department or other type of agency.

Name of the Custodian of Records tasked with providing the requested information:

Alleged violation of public records access  
 Alleged failure to provide information in a timely manner in accordance with the provisions of the Sunshine Ordinance  
 Alleged violation of a public meeting  
Please indicate date of meeting if known

Sunshine Ordinance Section(s)

67.21; 67.24 (B) (0); 67.25

(If known, please cite specific provision(s) being violated)

Please describe the alleged violation. Use additional paper if needed. Please attach any relevant documentation which supports your complaint.

See ATTACHED WORD DOCUMENTS FOR SPECIFIC DETAILS.

Are you requesting a public hearing before the Sunshine Ordinance Task Force?<sup>1</sup>

yes  no

If yes, please provide 1 or more preferred method(s) of contact:

Phone: 415 513-9334  Mailing Address: 250 Kearny St Apt 618  
 Fax: \_\_\_\_\_ San Francisco, CA 94108  
 Email: CKBluequadrangle@gmail.com  Other: \_\_\_\_\_

Signature: Chris Ward Kline

Date: 1/28/2023

<sup>1</sup> NOTICE: PERSONAL INFORMATION THAT IS PROVIDED WHEN ADDRESSING A PUBLIC POLICY BODY IS SUBJECT TO DISCLOSURE UNDER THE CALIFORNIA PUBLIC RECORDS ACT AND THE SUNSHINE ORDINANCE. MEMBERS OF THE PUBLIC ARE NOT REQUIRED TO PROVIDE PERSONAL IDENTIFYING INFORMATION, AND COMPLAINANTS MAY REMAIN ANONYMOUS. HOWEVER, FOR PROPER NOTICING AND PROCESSING OF A HEARING REQUEST, A RELIABLE MEANS OF CONTACT IS RECOMMENDED. PLEASE NOTE THAT THE SOTF ADMINISTRATOR WILL NOT REDACT ANY INFORMATION PROVIDED IN THESE SUBMISSIONS.



Sunshine Ordinance Task Force  
1 Dr. Carlton B. Goodlett Place, Room 244, San Francisco CA 94102  
Tel. (415) 554-7724; Fax (415) 554-7854  
<http://www.sfgov.org/sunshine>

Thank you for your interest in the implementation of the San Francisco Sunshine Ordinance.

The Sunshine Ordinance adopted by the citizens of the City & County of San Francisco declares that:

- (a) Government's duty is to serve the public, reaching its decisions in full view of the public.
- (b) Commissions, boards, councils and other agencies of the City and County exist to conduct the people's business. This Ordinance will assure that their deliberations are conducted before the people and that City operations are open to the people's review.

The role of the Sunshine Ordinance Task Force is to advise the Board of Supervisors and provide information to other City departments on appropriate ways in which to implement the Ordinance. The Task Force is responsible for developing appropriate goals to ensure the practical and timely implementation of the Ordinance and to report to the Board on practical or policy problems encountered in the administration of the Ordinance.

If you have encountered problems regarding compliance with the Ordinance, the Public Records Act or the Ralph M. Brown (Public Meetings) Act, we ask that you fill out the attached complaint form. Please deliver the form to: Administrator of the Sunshine Ordinance Task Force, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102-4689.

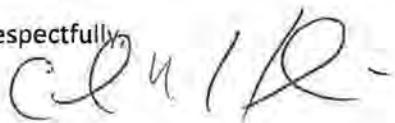
We attempt to resolve complaints informally where possible, through the affected departments and the City Attorney's office. Matters, which cannot be adequately resolved, or matters that involve substantial policy considerations, may be set for a hearing at a Task Force meeting. The Task Force meets the first Wednesday of each month at 4:00 p.m. at City Hall, Room 408.

**NOTICE: PERSONAL INFORMATION THAT IS PROVIDED WHEN ADDRESSING A PUBLIC POLICY BODY IS SUBJECT TO DISCLOSURE UNDER THE CALIFORNIA PUBLIC RECORDS ACT AND THE SUNSHINE ORDINANCE. MEMBERS OF THE PUBLIC ARE NOT REQUIRED TO PROVIDE PERSONAL IDENTIFYING INFORMATION, AND COMPLAINTANTS MAY REMAIN ANONYMOUS. HOWEVER, FOR PROPER NOTICING AND PROCESSING OF A HEARING REQUEST, A RELIABLE MEANS OF CONTACT IS RECOMMENDED. PLEASE NOTE THAT THE SOTF ADMINISTRATOR WILL NOT REDACT ANY INFORMATION PROVIDED IN THESE SUBMISSIONS.**

SUNSHINE ORDINANCE COMPLAINT FORM ALLEGED VIOLATION

- 1) Numerous request with SFDPH, SFPD, DEM and Sheriff's Department for public records for my person with most recent request dated December 13, 2022 – see that specific enclosed request for the entirety of request, specifics to include all surveillance, health surveillance, HIV surveillance and all audio/video surveillance. Pg 3-5
- 2) Please note on pg 5 "You will receive the Sheriff's office response no later than January 6, 2023" signed by Alison Lambert, Legal Assistant, San Francisco Sheriff's Office, Central Records and Warrants Unit.
- 3) Please note on pg 2, as on January 27, 2023 that request aforementioned in 1) and 2) is still listed as 'in progress' and I have not been notified via any other communications. These records have been delayed for over 8 plus months now.
- 4) All other pages in this request are a sampling and not all request sent to SFDPH, DEM, SFPD and Sheriff's Department. I have notified the Mayor, SFPD, Sheriff and Director Colfax several times of these attempts and it is obvious that there is stalling, and hesitancy to turn over the documents in the city/county possession.
- 5) The city and county utilizes an app called One System, which offers a variety of surveillance type tools to include GPS/GPRS, tracking documents and tracking individuals. Due to the GPS abilities; all data would eventually be stored within the Sheriff's Department and/or Department of Emergency Management. Just with One System, there would be records concerning myself. I'm asking for all records not just with One System, but all notes, files, surveillance, request, etc.
- 6) HIPPA Law does state that it is not required to turn over 'audio files' in protective health records; however, that a typed or otherwise printed format of the transcript is required for review by the person's health record it pertains too. The aforementioned agencies are refusing to turn over any records stating federal protection which is not valid nor true. Surveillance 'supremacy laws' lie within the city and county and are reviewable records and can be challenged in the court of law. For example, if a person was on HIV or Health Surveillance for Public Health to guide a patient to healthcare by audio means, a complete transcript of the interaction between 'operator and patient' shall be made available for review.
- 7) I'm in the process of amending my medical records with the Veterans Affairs and Kaiser. Records already received clearly would show that San Francisco has records that I'm requesting to review, challenge and potentially challenge in the court of law.
- 8) It is my desire to work with the city and county outside the court of law in resolving disputes, access to the records and their assistance with amending my records.

Respectfully,



Chris Ward Kline

1/28/2023



ADDITIONAL DOCUMENTATION CONCERNING ONE SYSTEM

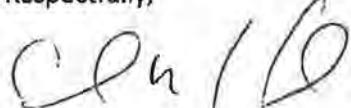
The last several pages are a list of SF Agencies and non-profits that utilize the app One System that information is stored within the Department of Emergency Management, within the Public Health/Safety Infrastructure Communications.

ALL SAN FRANCISCO DEPARTMENTS UTILIZE THIS APP, HOWEVER, SENIOR OFFICIALS ATTEMPT TO NOT LIST PUBLIC HEALTH, SHERIFF'S DEPARTMENT, SAN FRANCISCO POLICE DEPARTMENT, ETC IN AN ATTEMPT TO RESTRICT INFORMATION ON SURVEILLANCE EQUIPMENT ON CITIZENS OF SAN FRANCISCO.

IT SHOULD BE NOTED THAT THIS IS NOT LISTED ON ANY SURVEILLANCE TECHNOLOGY REQUIRED RELEASE TO THE PUBLIC. IT IS ONLY BECAUSE IT IS OVERUSED AND USED ILLEGALLY AND UNCONSTITUTIONALLY BY A FEW WITHIN SAN FRANCISCO.

With this information, which is reviewable and able to be challenged in the courts, it will show that a few in San Francisco have acted in violation of the Sunshine Act and obstructed in investigations regarding, Chris Ward Kline.

Respectfully,

A handwritten signature in black ink, appearing to read "Chris Ward Kline".

Chris Ward Kline

2/10/2023





San Francisco  
Sheriff's Office

MENU

## Records Menu

### FAQs

See All FAQs

What types of records are available?

Are there fees for public records requests?

What records are exempt from public requests?

When will I receive records for my public request?

If a records does not exist, can the agency create a record in response to my request?

Public Records Request about a month ago

P001596-121322

Public Records Request

**Status :** Received

Chris Kline

In Progress

[View File\(s\)](#) [Details](#)

Public Records Request 3 months ago

P001470-101922

Public Records Request

**Status :** Partial Release

Chris Kline

Completed

[View File\(s\)](#) [Details](#)

Subpoena Duces Tecum about a year ago

S000127-070521

Completed

All public health records to include epidemiology, behavioral health surveillance to include communication from county to and from Chris Ward Kline. Information should include all communication transmitted through Public Broadcast, Emergency Broadcast and Public Health Communication and any additional surveillance networks within San Francisco County via voice synthesizers and utilization of text to voice/speech and voice/speech to text during all periods from 9/2001 through July 4, 2021. It should be noted that plaintiff was not in prison nor affiliated with a gang; however, Plaintiff is requesting electronic surveillance listed above but also any

Powered by  
**GovQA**





Chris K. &lt;ckblueaqua@gmail.com&gt;

**[Records Center] Public Records Request :: P001596-121322**

1 message

San Francisco County Sheriff <sfsheriff@govqa.us>  
To: "ckblueaqua@gmail.com" <ckblueaqua@gmail.com>

Fri, Dec 23, 2022 at 11:26 AM

— Please respond above this line —



RE: Public Records Request of December 13, 2022, Reference # P001596-121322

Dear Chris Kline,

On December 13, 2022, the San Francisco Sheriff's office received your request for records pursuant to the California Public Records Act (CPRA) wherein you requested the following:

*See original request and additional items. I'm also looking for encrypted files of Interoperable Communication, text-to-voice/voice to text and for these files to be decrypted and turned over within a reasonable amount of time. It is how public health and safety uses technology. For example, it picks up code words such as 'what is the speed limit? and the technology is supposed to inform me with computers and devices talking to me the individual. It is not classified nor confidential. It is the same devices and equipment that churches use, Federal Prisons, jails and protective housing folks as well as folks with HIV. It is also used to protect politicians inside city hall and outside during events in which SFPD and Sheriff's places on large swaths of people during these events and with the equipment atop the County Library and Asian Art Museum.*

*I know these records exist as they exist in all approximately 3,030 counties across the United States. This is not an abnormal request, just all files related to me and interaction with former and current employees.*

*I understand the legal issues and the facts that some former and possible current deputies have went to fall with their surveillance duties. The office of the Sheriff is to uphold the law with the upmost integrity.*

*I can if needed request this information from the District of Columbia Public Safety as that is where the Interface for the entire system that wraps up to federal agencies such of Commerce, Labor, DOJ, HHS, AND multiple others. It is also available at the FCC.*

*I'm also requesting all information from the Sheriff's Department on any investigation conducted by current and former employees using this equipment. I have also submitted an*



*Internal Affairs request and have submitted over 60 pages of documentation. There would have been notes added to my file and those are public records.*

*Besides One System which I have 100% proof that Department of Emergency Management and the Sheriff's Department uses, amongst others, but to also include the following:*

*1) body worn cameras, 2) Inmate phone call recording, 3) CCTV Cameras, 4) Fiber Optic Cameras and Under door cameras, 5) GPS Tracking devices, 6) HNT Throw Phone/Camera, 7) any stingray or related technology, 8) Recon Scout, 9) Constant Contact, 10) Google Web Analytic, 11) drones, 12) RFID Scanner, 13) Vehicle and Mobile Command Cameras, 14) SCRAM Ankle Bracelet, 15) Dataworks Plus Digital Photo, 16) Cellbrite, 17) Lil Ears Microphone, 18) Irobot, 19) Vetmax Camera, 20) Wolstenholme Hazprobe, 20) Andros Robotics with Camera, 21) under vehicle Camera, and all other apps, devices and technology.*

*As a portion of this has been answered already, please disregard the portions already answered by your office such as P.R.E.P.*

*All records within the Sheriff's Department, the Department of Emergency Management and other agencies to include the Sheriff Department Community Programs and Engagement Programs to include but not limited too: Current and valid P.R.E.P. certification from the California Department of Health and for all other records that are known to exist on a variety of incidents, issues, surveillance to include: interviewing gang members, interviewing homeless people, interacting with people on the app*

*One System, public health surveillance and safety equipment to include and not limited too: All Central Records Systems to include but not limited to Electronic/Microphone/Physical and Technical Surveillances for both main file records and cross reference files. These records are known to exist as all apps that utilize GPS and GPRS data, with One System and all other apps such as public health, public safety and political surveillance to include any and all surveys and messages sent to any and devices specific to Chris Ward Kline. a previous request for records was denied by Retired Deputy James Wilson which would be misconduct of a public official since the records do exist. --- Clarification response: --- I was asked for follow up on two specific parts of my records request: 1) P.R.E.P. is the Post Release Education Program, certification #380083BN expired 5/31/2017. It is required by state law as the Sheriff conducts outpatient Alcohol and/or other Drug Services. California Department of Health Care Services issues the certification. 2) the App One System was purchased by the city and county of San Francisco from Bitfocus, Inc. and is used in all agencies within the city and county of San Francisco to multiple day to day functions, monitors SIGINT, is assigned a FCC channel, and used for Protection for elected officials, gang surveillance, public health day to day operations, public safety day to day operations. With it, you can program signals to go to peoples homes, cell phones, police vehicles, fire trucks, etc. and it is being used illegally by a few in San Francisco to influence people for various personal and political reasons. Simply put, I want all information that applies to me, impacted me, etc that was used on that FCC channel. You can contact this person's email shonie.vasudevan@sfgov.org who has the certification which expires in the year 2030. SFIA COMMUNICATIONS DEPT SAN FRANCISCO, SAN MATEO, SAN FRANCISCO, CA P: (650)821-3644 SY - Trunked Public Safety 700 MHz WQMR423 - Call Sign 90.523(A) - GOVERNMENT AGENCIES SAN FRANCISCO INTERNATIONAL AIRPORT PUBLIC SAFETY RADIO SYSTEM City Agency HSH is the largest agency in the city and county. It uses the app and issues credentials to agencies and individuals to, when done legally, to guide people to healthy decisions. When it is being done illegally, it can force people to move that they don't like, that don't vote for a specific person, or donate to a specific person or cause. Please let me know if there is additional information needed.*

*I'm also concerned that at least one record was removed from this service request system in*



*which the Legal Office stated that they needed two more weeks to review my claim asking for my knowledge of P.R.E.P. and One System.*

*I'm also looking for all credentials that were given out to any citizen, former and current employee and purpose of allowing them credentials. Within San Francisco, over 50 agencies utilize One System, from churches, non profit, Department of Emergency Management, Public Health, and politicians use to send out MailChimp, SurveyMonkey, SurveyGizmo, etc.*

*If the Sheriff was not able to monitor this system, a person could at any time, send an email, text, call with the aforementioned apps, to inmates or visitors entering into City Hall. It sends bots and malware that turn on a persons phone, and then can be a live operator, program, questionnaire, etc to cause violence within areas that are protected by the Sheriff's Department.*

***IT WOULD BE IMPOSSIBLE FOR THE SHERIFF NOT TO HAVE ANY DOCUMENTATION CONCERNING THIS, LET ALONG SOMEONE THAT HAS VISITED SAN FRANCISCO, FREQUENTED SAN FRANCISCO, SPOKE AT CITY HALL, ETC.***

*I'm also including multiple dates and times in which current and former Sheriff's employees were using surveillance on me at various times and the obstruction that occurred.*

The Sheriff's Office responds to your public records request as follows: The Sheriff's office is conducting an extensive review to locate and review responsive records in order to respond to your public records request. Please be advised that because of the need to consult with another unit in our department, the Sheriff's office is hereby invoking an extension of time of 14 days under Gov. Code section 6253(c). On or before January 06, 2023, the Sheriff's office will notify you if we locate any records that are responsive and not exempt from disclosure to your request, in addition to providing a date that non exempt records will be provided to you.

You will receive the Sheriff's office response no later than January 06, 2023.

Sincerely,

Alison Lambert  
Legal Assistant  
San Francisco Sheriff's Office  
Central Records & Warrants Unit

To monitor the progress or update this request please log into the Records Request System





## Records Menu

### FAQs

[See All FAQs](#) 

What types of records are available?

Are there fees for public records requests?

What records are exempt from public requests?

When will I receive records for my public request?

If a records does not exist, can the agency create a record in response to my request?

[Request / Incident Summary](#)

Request Type:

Contact E-Mail:

Reference No.:

Status:

[Ticket Type](#)

[Contact Information](#)

[Reference No.](#)

[Status](#)

[Additional Information](#)

[Type of Requests](#)

[Incident Details](#)

[Incident Number](#)

X

[View Message](#)

The San Francisco Sheriff's Office received a public records request from you on December 13, 2022.

Your request mentioned the following: *See original request and additional items. I'm also looking for encrypted files of Interoperable Communication, text-to-voice/voice to text and for these files to be decrypted and turned over within a reasonable amount of time. It is how public health and safety uses technology. For example, it picks up code words such as 'what is the speed limit? and the technology is supposed to inform me with computers and devices talking to me the individual. It is not classified nor confidential. It is the same devices and equipment that churches use, Federal Prisons, jails and protective housing folks as well as folks with HIV. It is also used to protect politicians inside city hall and outside during events in which SFPD and Sheriff's places on large swarths of people during these events and with the equipment atop the County Library and Asian Art Museum. I know these records exist as they exist in all approximately 3,030 counties across the United States. This is not an abnormal request, just all files related to me and interaction with former and current employees. I understand the legal issues and the facts that some former and possible current deputies have went to fall with their surveillance duties. The office of the Sheriff is to uphold the law with the upmost integrity. I can if needed request this information from the District of Columbia Public Safety as that is where the Interface for the entire system that wraps up to federal agencies such of Commerce, Labor, DOJ, HHS, AND multiple others. It is also available at the FCC. I'm also requesting all information from the Sheriff's Department on any investigation conducted by current and former employees using this equipment. I have also submitted an Internal Affairs request and have submitted over 60 pages of documentation. There would have been notes added to my file and those are*



SAN FRANCISCO DEPARTMENT OF EMERGENCY MANAGEMENT

Custodian of Records

**Request for Dispatch Records**

(San Francisco Sunshine Ordinance, Administrative Code §67.1.seq.)

2022 SEP - 5 P. M. T.

Date of Request: September 4, 2022

**NOTE: No Same Day Service Available**

Requestor Name: Chris Ward Kline

Address: 237 Kearny St, PMB 114

City/State/Zip: San Francisco, CA 94108 Telephone:

Records Requested:  CAD Printout  Telephone Audio (\$35)  Radio Audio (\$35)

Other (specify): public health and public safety surveillance

CAD Number:

Case or Incident Number:

Date of Incident:

various

Time of Incident: various

Incident Location:

various

Other identifying information or details (be specific): Please conduct a search of the Central Records System, including

but not limited to the Electronic Surveillance (ELSUR) Indices, the Microphone Surveillance (MISUR +  
the Physical Surveillance (FISUR) indices, and the Technical Surveillance (TESUR) indices, for  
both main file records and cross references.

**Fee Schedule: (City / County employees - DO NOT USE THIS FORM )**

**Audio:** \$35.00 for phone audio for each CAD requested; \$35.00 for radio audio for each CAD requested.

**Print:** Printouts over 100 pages billed at \$0.10 per page.

*Payment is by cash, check or money order*

**When Requesting by Email:** Send the completed form to [dem.records@sfgov.org](mailto:dem.records@sfgov.org).

(If you are requesting audio files, please mail the request form with exact payment to avoid a delay in receipt of the records requested. We cannot process electronic payments.)

**Method of Delivery:** Please check an option below. **We cannot currently send records by email**

I would like to inspect records by mail. Please send the records to the address above. I understand I must pay any applicable fees before the Department will send the records.

I would like to inspect & pick up a copy of the records from the Department of Emergency Management. Please advise when the records are ready. I understand I must pay any applicable fees before the Department will release copies to me.

**For Office Use Only**

Date Completed:

Completed By:

Comments:





# Public Records Portal

MENU

## Public Records

### Menu

### FAQs

[See All Seven FAQs >](#)
[Obtain an Existing Police Report](#)
[Requesting Public Records from the Police Department](#)
[Public Records Policy & Procedures](#)
[FAQs for Public Records](#)
[Departmental Requests that are Subject to Disclosure](#)

### Public Records Request

[View File\(s\)](#)
[View Message\(s\)](#)
[Select Language ▼](#)
**Request Type:**

Public Records Request

**Description:**

Public records are defined as any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

**Contact E-Mail:**

CKBlueaqua@gmail.com

**Reference No:**

P084503-091622

**Status:**

Completed

## UPLOAD DATE


[DOWNLOAD ALL](#)

FILE	09/26/2022	P84503_-9.26.22_sfpd_response.p df
------	------------	---------------------------------------

**Describe the Record(s) Requested:**

From: Chris K.  
 <ckblueaqua@gmail.com> Sent:  
 Tuesday, September 13, 2022 4:15  
 PM To: Breed, Mayor London  
 (MYR)  
 <mayorlondonbreed@sfgov.org>  
 Colfax, Grant (DPH)  
 <grant.colfax@sfdph.org>;  
 Walton, Shamann (BOS)  
 <shamann.walton@sfgov.org>;  
 Peskin, Aaron (BOS)

<aaron.peskin@sfgov.org> Cc:  
SFPD, Chief (POL)  
<sfpdchief@sfgov.org>; Pojman,  
Natalie (DPH)  
<natalie.pojman@sfdph.org>;  
Varisto, Michaela (DPH)  
<michaela.varisto@sfdph.org>  
Subject: Department of  
Emergency Management  
Response This message is from  
outside the City email system. Do  
not open links or attachments  
from untrusted sources. Good  
evening, Department of  
Emergency Management  
Response denies and record  
within 72 hours or request. It  
should be noted that on a SF govt  
website, the partner agencies list  
wss changed by IT and an  
appropriate list of previous and  
new are recorded which points to  
obstruction. I will be asking for a  
complete list and once again, I  
respectfully request the  
documents from Public Health,  
and any/all agencies that have  
record that include but not limited  
to: 'Electronic Surveillance  
(ELSUR) indices, the Microphone  
Surveillance (MISUR) indices, the  
Physical Surveillance (FISUR)  
Indices, and the Technical  
Surveillance (TESUR) Indices, for  
both main file records and cross  
reference files'. Respectfully, Chris  
Ward Kline

**Incident Number:** *if known*

**Police Officer(s) Involved:** *if known*

**Time of Incident:** *specify AM or PM, if known*

**Date Range From:** *if applicable*

**Date Range To:** *if applicable*

**Preferred Method to Receive Records:** Electronic via Records Center

## Messages 3

 Print Messages (PDF)

✓✉ On 9/26/2022 2:26:10 PM, San Francisco Police Records Portal wrote:

**Subject:** Public Records Request :: P084503-091622

**Body:**

September 26, 2022

*Via email CKBlueaqua@gmail.com*

Chris Ward Kline  
237 Kearny Street Apt 104  
San Francisco, CA 94108

RE: Public Records Request, dated September 16, 2022, Reference # P084503-091622

Dear Chris Ward Kline:

In response to your request, please see attached document(s).

Sincerely,

Lieutenant Lynn Reilly #1141  
Officer in Charge  
Risk Management - Legal Division

✓✉ On 9/16/2022 12:51:13 PM, San Francisco Police Records Portal wrote:



Dear Chris Ward Kline:

Thank you for your interest in public records of the San Francisco Police Department ("SFPD").

The San Francisco Police Department ("SFPD") received your request, dated September 16, 2022 and given the reference number **P084503-091622** for tracking purposes.

Record(s) Requested: From: Chris K.  
Sent: Tuesday, September 13, 2022 4:19 PM  
To: Breed, Mayor London (MYR) ; Colfax, Grant (DPH) ; Walton, Shamann (BOS) ; Peskin, Aaron (BOS)  
Cc: SFPD, Chief (POL) ; Pojman, Natalie (DPH) ; Varisto, Michaela (DPH)  
Subject: Department of Emergency Management Response

*This message is from outside the City email system. Do not open links or attachments from untrusted sources.*

*Good evening,*

*Department of Emergency Management Response denies and record within 72 hours or request.*

*It should be noted that on a SF govt website, the partner agencies list was changed by IT and an appropriate list of previous and new are recorded which points to obstruction.*

*I will be asking for a complete list and once again, I respectfully request the documents from Public Health, and any/all agencies that have record that include but not limited too.*

*'Electronic Surveillance (ELSUR) indices, the Microphone Surveillance (MISUR) indices, the Physical Surveillance (FISUR) Indices, and the Technical Surveillance (TESUR) Indices, for both main file records and cross reference files'.*

*Respectfully,*

*Chris Ward Kline*

*Your request is being forwarded to the appropriate department(s) for processing and you will be notified once the request is complete.*

You can monitor request progress at the link below. Thank you for using the San Francisco Public Records Center.

San Francisco Police Department

To monitor the progress or update this request please log into the SFPD Public Records Center.

✓  On 9/16/2022 12:51:12 PM, San Francisco Police Records Portal wrote:

Request was created by staff

GovQA is an SFPD authorized third party vendor which facilitates incident report request services for CISU. SFPD accepts no liability for the accuracy of content on the linked GovQA webpages. Members of the public may still make requests using U.S. mail or email by using the Incident Report Request Form(s). Those requests will be manually entered and tracked in the Incident Report Request Portal by a member of CISU. An account on the Incident Report Request Portal can be created to track the request online.







## Department of Emergency Management

London Breed  
Mayor



Mary Ellen Carroll  
Executive Director

To: Chris Ward Klein  
237 Kearny St., PMB 114  
San Francisco, CA 94108

From: Custodian of Records

Date: September 7, 2022

Re: Records Request

---

We are in receipt of your request regarding:

***Electronic Surveillance (ELSUR) Indices, the  
Microphone Surveillance (MISUR), the Physical  
Surveillance (FISUR) Indices, and the Technical  
Surveillance (TESUR) Indices, for both main file records  
and cross references.***

The San Francisco Department of Emergency Management does not maintain such records.  
You may wish to contact the San Francisco Police Department for further.

**San Francisco Police Department  
Risk Management Office  
1245 3rd Street, 4th Floor  
San Francisco, CA 94158**

If you have any further questions, please feel free to contact our offices at 415-558-3826.





Chris K. &lt;ckblueaqua@gmail.com&gt;

**[Records Center] Public Records Request :: P001470-101922**

1 message

**San Francisco County Sheriff** <sfsheriff@govqa.us>  
To: "ckblueaqua@gmail.com" <ckblueaqua@gmail.com>

Tue, Oct 25, 2022 at 12:07 PM

--- Please respond above this line ---



RE: Public Records Request of October 19, 2022, Reference # P001470-101922

Dear Chris Kline,

On *October 19, 2022*, the San Francisco Sheriff's office received your request for records pursuant to the California Public Records Act (CPRA) wherein you requested the following:

*All records within the Sheriff's Department, the Department of Emergency Management and other agencies to include the Sheriff Department Community Programs and Engagement Programs to include but not limited to:*

*Current and valid P.R.E.P. certification from the California Department of Health and for all other records that are known to exist on a variety of incidents, issues, surveillance to include: interviewing gang members, interviewing homeless people, interacting with people on the app One System, public health surveillance and to include and not limited to:*

*All Central Records Systems to include but not limited to Electronic/Microphone/Physical and Technical Surveillances for both main file records and cross reference files.*

*These records are known to exist as all apps that utilize GPS and GPRS data, with One System and all other apps such as public health, public safety and political surveillance to include any and all surveys and messages sent to any and devices specific to Chris Ward Kline.*

*a previous request for records was denied by Retired Deputy James Wilson which would be misconduct of a public official since the records do exist.*

Additional clarification is needed in order to fulfill your request:

- Define P.R.E.P certification
- Define App One System

A reply must be received within ten (10) calendar days of the date this email was sent or your request will be closed and a new request will be required. Please respond in writing via the Records Request System so that there is a record of your response.

Upon receipt of your response, the department will further respond to your request as required by law.

Sincerely,

Juliana Petani  
Legal Assistant  
*San Francisco Sheriff's Office*  
*Central Records & Warrants Unit*

To monitor the progress or update this request please log into the Records Request System





San Francisco  
Sheriff's Office

[MENU]

## Records Menu

[View Message\(s\)](#)

### FAQs

[See All FAQs](#)

What types of records are available?

Are there fees for public records requests?

What records are exempt from public requests?

When will I receive records for my public request?

If a records does not exist, can the agency create a record in response to my request?

Request / Incident Summary

**Request Type:**

Public Records Request

**Contact E-Mail:**

ckblueaqua@gmail.com

**Reference No:**

P000320-041221

**Status:**

No Records Exist

Additional Information

**Type of Record(s):**

Incident Related Records

Calls for Service

Policy and Procedures

Other (describe below)

**The Sheriff's Office is not the custodian of records of mugshots and arrest records. To obtain copies of your criminal history and mug shots, you must contact the San Francisco Police Department, ID Bureau, located at 850 Bryant St., Room 475, San Francisco, CA 94103. The SFPD ID Bureau is open Monday - Friday, 8:00 a.m. - 5:00 p.m., and their telephone number is (415) 553-1415. You should also bring a valid government issued ID.**

### Incident Details

**Incident Number:**

**Date of Incident:**

**Time of Incident:**

04/12/2021

1335

**Location/Address:**

Lake Merritt BART

*Please be as specific as possible including the exact address or landmark.*

**Date Range:**

Since 09/2000

*If Applicable*

Powered by  
**GovQA**

**Involved Party:**

Various members of SF County Public Safety

**Describe the Record(s) Requested:**

Date of Incident: 04/12/2021 Today at 1335 hrs, I received a call from number 628-227-3227 which was used to place a survey and surveillance on my phone 415-203-1662. The surveillance was and is illegal and there are no reasons for surveillance to be placed on me, friends or family. I'm requesting that these records are turned over to me immediately in order to file criminal charges and to start civil proceedings on all parties involved. The surveillance has been occurring regularly off and on since approximately 09/2000 and lately 24/7 from San Francisco Public Safety. I will be requesting similar documentation from Alameda County, the state of California, FBI and Health and Human Services. I will request a subpoena for these records as well. Respectfully, Chris Ward Kline

**As a default, all records are provided to the requester electronically through the online Records Request System. If you would like to receive your records in an alternative format please select the format below. Please note copy fees may apply for non-electronic delivery.**

**Alternate Method to Receive Records:**

Electronic Records

**If you have any documents that may assist in responding to your request, please attach here:**

[New Message](#)[Return to List](#)[Messages 3](#)[Print Messages \(PDF\)](#)

✉ On 4/13/2021 7:54:53 AM, San Francisco County Sheriff wrote:

**Subject:** [Records Center] Public Records Request :: P000320-041221

**Body:**

RE: Public Records Request of April 12, 2021, Reference # P000320-041221

Dear Chris Kline,

On April 12, 2021, the San Francisco Sheriff's Office received your request for records pursuant to the California Public Records Act (CPRA) wherein you requested the following:

*Today at 1335 hrs, I received a call from number 628-227-3227 which was used to place a survey and surveillance on my phone 415-203-1662. The surveillance was and is illegal and there are no reasons for surveillance to be placed on me, friends or family.*



## Records Menu

### FAQs

[See All FAQs](#)

What types of records are available?

Are there fees for public records requests?

What records are exempt from public requests?

When will I receive records for my public request?

If a records does not exist, can the agency create a record in response to my request?

**Subpoena Duces Tecum** about a year ago  
**P000127-070521** Completed  
All public health records to include epidemiology, behavioral health surveillance to include communication from county to and from Chris Ward Kline. Information should include all communication transmitted through Public Broadcast, Emergency Broadcast and Public Health Communication and any additional surveillance networks within San Francisco County via voice synthesizers and utilization of text to voice/speech and voice/speech to text during all periods from 9/2001 through July 4, 2021. It should be noted that plaintiff was not in prison nor affiliated with a gang; however, Plaintiff is requesting electronic surveillance listed above but also any involving communication with gang members and current and/or former prisoners. Respectfully, Chris Ward Kline 415-203-1662 p.s. please do not utilize my cell phone number or my email to place electronic surveillance based on this request.  
**Status :** No Records Exist

Chris Kline

[View File\(s\)](#)

[Details](#)

**Public Records Request** about a year ago  
**P000320-041221** Completed  
Public Records Request  
**Status :** No Records Exist

Chris Kline

[Details](#)



*The surveillance has been occurring regularly off and on since approximately 09/2000 and lately 24/7 from San Francisco Public Safety.*

*I will be requesting similar documentation from Alameda County, the state of California, FBI and Health and Human Services.*

*I will request a subpoena for these records as well.*

*Respectfully,*

*Chris Ward Kline*

The Sheriff's Office has performed a diligent search and determined that no such record exists. The Sheriff's Office has no duty to create a record that does not exist at the time of the request. *Sander v. State Bar of California (2013) 58 Cal.4th 300.*

This completes the Sheriff's office response to your request under the California Public Records Act. If you would like to make a new public records request of the Sheriff's Office, please make your request at the Records Request System.

*Sincerely,*

*James Wilson  
Retired Deputy #1093  
San Francisco Sheriff's Office  
Central Records & Warrants Unit*

➤✉ On 4/12/2021 4:31:09 PM, San Francisco County Sheriff wrote:

➤✉ On 4/12/2021 4:31:08 PM, Chris Kline wrote:





**Department of Emergency Management**  
1011 Turk Street, San Francisco, CA 94102

London N Breed  
Mayor

Phone: (415) 558-3826  
Fax: (415) 558-3869



Mary Ellen Carroll  
Executive Director

**CUSTODIAN OF RECORDS**  
**REQUEST FOR DISPATCH RECORDS INSTRUCTIONS**  
(San Francisco Sunshine Ordinance, Administrative Code §67.2.seq.)

Dear Requestor:

Fill out each line as applicable. Specifically identify the information you are attempting to obtain.

The following information must be supplied to ensure your request is accepted:

- ✓ **Date of your request**
- ✓ **Name, address and contact telephone number**
- ✓ **CAD or police case number (if available)**
- ✓ **Date of the incident**
- ✓ **Location of the incident – if requesting address history, please list the date range**
- ✓ **Any other identifying information (i.e. requests for all calls to a particular location)**

If you do not have all of the above required information, please fill out the form to the greatest extent possible.  
*Incomplete requests may delay our ability to process the request in a timely manner or at all.*

We can use a police case number to locate your CAD record; however, **we do not have access to San Francisco Police reports**. For copies of a police report, contact SFPD – Record Management via their web portal at [www.sanfranciscopolice.org](http://www.sanfranciscopolice.org). You may also call 415.575.7232 or email them at [sfpd.cisu.reports@sfgov.org](mailto:sfpd.cisu.reports@sfgov.org).

If your request requires a payment, we currently accept cash, check, or money order. To avoid delays in receipt of your request, please include payment in the exact amount due with the request form.

**WE CANNOT PROVIDE RUSH SERVICE.** Requests are processed in the order received. While we process requests as quickly as possible, we have up to 10 calendar days to accept or deny the request. It is not necessary to call for the status of your request.

**You may submit a completed form via US mail, in person, fax, or email.**

In person: There is a secure drop box in our lobby along with additional blank forms for your convenience.

Fax: You may fax us at 415.558.3869.

Email: [dem.records@sfgov.org](mailto:dem.records@sfgov.org) – Printouts only

**We cannot return records by email at this time. You must choose whether to pick up the responsive records in person, or have them mailed to you via the return address you include on the form.**

Mail: Department of Emergency Management

Attn: Custodian of Records  
1011 Turk St  
San Francisco CA 94102



## SAN FRANCISCO DEPARTMENT OF EMERGENCY MANAGEMENT

Custodian of Records

## Request for Dispatch Records

(San Francisco Sunshine Ordinance, Administrative Code §67.1.seq.)

Date of Request:

October 19, 2022 **NOTE: No Same Day Service Available**

Requestor Name:

Chris Ward Kline

Address:

237 Kearny ST PMB 114

City/State/Zip:

San Francisco, CA Telephone: 415-513-9334

Records Requested:

 CAD Printout  Telephone Audio (\$35)  Radio Audio (\$35) Other (specify): All Surveillance - See

CAD Number:

All

Case or Incident Number:

All Attached

Date of Incident:

All

Time of Incident:

All

Incident Location:

All

Other identifying information or details (be specific):

See Attached emailSent to Sheriff Dept. I want their records  
and All stored with DEM.**Fee Schedule: (City / County employees - DO NOT USE THIS FORM )****Audio:** \$35.00 for phone audio for each CAD requested; \$35.00 for radio audio for each CAD requested.**Print:** Printouts over 100 pages billed at \$0.10 per page.**Payment is by cash, check or money order****When Requesting by Email:** Send the completed form to [dem.records@sfgov.org](mailto:dem.records@sfgov.org).

(If you are requesting audio files, please mail the request form with exact payment to avoid a delay in receipt of the records requested. We cannot process electronic payments.)

**Method of Delivery:** Please check an option below. **We cannot currently send records by email**I would like to inspect records by mail. Please send the records to the address above. I understand I must pay any applicable fees before the Department will send the records.I would like to inspect & pick up a copy of the records from the Department of Emergency Management. Please advise when the records are ready. I understand I must pay any applicable fees before the Department will release copies to me.**For Office Use Only**

Date Completed:

Completed By:

Comments:



Chris K. &lt;ckblueaqua@gmail.com&gt;

**RE: Request for One System, Bitfocus App and Network Communication**

2 messages

**DPH Sunshine** <dph.sunshine@sfdph.org>  
To: "Chris K." <ckblueaqua@gmail.com>  
Cc: DPH Sunshine <dph.sunshine@sfdph.org>

Tue, Sep 20, 2022 at 12:39 PM

Requester,

DPH IT conducted an email search of the records you request below. The only results were emails you have sent to DPH yourself; however, copies of those communications are attached here as PDFs.

This concludes your public records request.

**From:** Chris K. <ckblueaqua@gmail.com>  
**Sent:** Thursday, September 15, 2022 2:52 PM  
**To:** Varisto, Michaela (DPH) <michaela.varisto@sfdph.org>  
**Cc:** Colfax, Grant (DPH) <grant.colfax@sfdph.org>; Pojman, Natalie (DPH) <natalie.pojman@sfdph.org>; SFPD, Chief (POL) <sfpdchief@sfgov.org>; Breed, Mayor London (MYR) <mayorlondonbreed@sfgov.org>  
**Subject:** Request for One System, Bitfocus App and Network Communication

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Michaela Varisto,

I was reviewing my request and noticed your name on all the comments.

I'm now requesting all communications between Public Health and me, Chris Ward Kline that deal with the app One System and Bitfocus, as well as any and all APPS.

I have documentation that shows Public Health utilizes this app as well as other partner agencies within San Francisco.

I have reviewed all state and federal law as well as SF Public Health Manuals and have not seen any protections federally or within the state of California. It does show that these communications are reviewable and amendable with cause, which I have or can show. It also shows that these records can be challenged in state and federal court. It is my desire to resolve this within the county, collectively, amicably and timely.

I've been very patient with San Francisco in requesting these records. In fact, due to not receiving these timely requests, it cost me a civil judgment federally against H.H.S. I do believe SF has brought suit or is still involved with a suit with H.H.S. and it is my belief that H.H.S. is also accessing your One System with credentials it should not have.

If I need to request these records via another agency, please advise where to send the request.

Respectfully,

Chris Ward Kline

## Request Closed

Requester, it seems as though you are requesting your own protected health information. Please note medical record/health information requests are NOT public record requests. You may request medical records, in accordance with privacy protected law, by sending a fax to 628-206-8623 or visit the Medical Records Office at 1001 Potrero Ave, Building 5, 2nd Floor, Room 2B.

June 27, 2022, 4:00pm by Michaela Varisto

Public

## Department Assignment

Public Health: Other

June 27, 2022, 3:56pm by Michaela Varisto

### 3 attachments

 **Batch 1.pdf**  
853K

 **Batch 2.pdf**  
1511K

 **Request for One System, Bitfocus App and Network Communication.pdf**  
138K

**Chris K. <ckblueaqua@gmail.com>**

To: [grant.colfax@sfdph.org](mailto:grant.colfax@sfdph.org)

Cc: "Varisto, Michaela (DPH)" <[michaela.varisto@sfdph.org](mailto:michaela.varisto@sfdph.org)>, [natalie.pojman@sfdph.org](mailto:natalie.pojman@sfdph.org)

Bcc: "Breed, Mayor London (MYR)" <[MayorLondonBreed@sfgov.org](mailto:MayorLondonBreed@sfgov.org)>, [SFPDChief@sfgov.org](mailto:SFPDChief@sfgov.org), [Shamann.Walton@sfgov.org](mailto:Shamann.Walton@sfgov.org)

Tue, Sep 20, 2022 at 4:07 PM

Good afternoon Dr. Colfax,

I have sent you, as well as others, documented evidence that should be on my public health record with the city logo, Public Address on it.

I'm trying to resolve this without submitting to a city/county grand jury.

You certainly are not suggesting that these documents (that I submitted) are fraudulent, are you?

I know where the files are kept. Having send me only my emails will not suffice.

This would be best resolved without a grand jury convening or other legal means.

These documents have been produced in other counties, or should I say the county settled, because they did not want the files released.

I assure you, I have always wanted this resolved amicably; however, stalling, obstructing and not being straight forward, will potentially only backfire on city and county employees with potential civil and criminal penalties.

Having said that, I want to resolve this as soon as possible or I will discuss 'voices' as a byproduct of public health to guide people to healthy or unhealthy decisions. Voices are nothing more then public health and others to include politicians using for a host of issues.

It strongly appears that public health is protecting one or more politician, who acted outside of his scope.

This was filed with the FBI and DHS, as well as others.

Regards,

Chris Ward Kline

[Quoted text hidden]

---

### 3 attachments

 **Batch 1.pdf**  
853K

 **Batch 2.pdf**  
1511K

 **Request for One System, Bitfocus App and Network Communication.pdf**  
138K

**Sunshine Ordinance Complaint Process, Section A & B, “File a Complaint with the SOTF”** for how to present your complaint. Use of our complaint form, while optional, helps to ensure that you include the information we deem relevant for evaluating complaints.

2. You can email your complaint to [sotf@sfgov.org](mailto:sotf@sfgov.org) , fax it to 415-554-5163, or deliver it in person to the Administrator of the Sunshine Ordinance Task Force, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102-4683.
3. After you file a complaint, we will review it to determine whether we have jurisdiction over the matter as defined in the Sunshine Ordinance.
4. If we determine that we have jurisdiction, we may schedule a hearing before the full task force. If we determine that we do not have jurisdiction, you can request a reconsideration of this decision before the full task force.
5. Parties to a complaint can submit additional information to the Task Force up to 5 working days before a scheduled hearing. If either party submits material after this deadline, the Task Force may proceed without consideration of these materials. Alternatively, if new, relevant materials become available after the 5-day deadline, the complainant may incorporate this information into a new complaint or may ask to have the hearing postponed until the next Task Force meeting.
6. After a hearing, the Task Force will issue an Order of Determination stating the outcome of the proceeding and

Visit San Francisco's new website, [SF.gov](#)

## Sunshine Ordinance Task Force

### Filing a Complaint with the Sunshine Ordinance Task Force

If you believe that the City or County of San Francisco has not complied with the Sunshine Ordinance, the Public Records Act or the Ralph M. Brown (Public Meetings) Act, you may file a complaint with the Task Force. We attempt to resolve complaints informally among the parties involved whenever possible. Matters that cannot be resolved informally, or which implicate substantial policy considerations, may be set for hearing at a Task Force meeting. The Task Force meets the first Wednesday of each month at 4:00 p.m. at City Hall, Room 408. The meeting is accessible virtually at call-in phone number: 1-415-906-4659, Meeting ID: 127 497 534#.

- [How the Complaint Process Works](#)
- [Fax / Mail Complaint Form \(Pdf\)](#)
- [Submit a Complaint On-Line](#)

### Summary of the Complaint Process

1. You can access a complaint form at [sfgov.org/site/sunshine](https://sfgov.org/site/sunshine) or send us a letter detailing your complaint. Please see the

any decisions made regarding violations of public records or public meetings laws.

7. For further information, contact the Sunshine Ordinance Task Force Administrator, at (415) 554-7724.



MENU

## Participating Agencies

- 3rd Street Youth Center and Clinic
- Abode Services
- AIDS Housing Alliance
- Asian Women's Shelter
- At the Crossroads
- Bay View Hunters Point Multipurpose Senior Services
- Bayview Hunters Point Foundation for Community Improvement
- Bernal Heights Neighborhood Center
- Bridge Housing
- Brilliant Corners
- Caritas Management Corporation
- Catholic Charities CYO
- Center on Juvenile and Criminal Justice
- Chinatown Community Development Center
- Community Forward SF

Hello! — Anything I can do to help? Just let me know.

- Community Housing Partnership
- Compass Family Services
- Conard House
- Curry Senior Center
- Delivering Innovation in Supportive Housing (DISH)
- Department of Emergency Management (DEM) – Office of Housing Opportunities
- San Francisco Department of Homelessness and Supportive Housing
- Dolores Street Community Services
- Episcopal Community Services (ECS)
- Eviction Defense Collaborative
- First Place for Youth
- Five Keys Charter Schools & Programs
- Glide Community Housing
- GP/TODCO Inc.
- Hamilton Families
- Heluna Health
- Homeless Children's Network
- Homeless Prenatal Program
- Homeless Youth Alliance
- Hospitality House
- Huckleberry Youth Programs
- San Francisco Human Services Agency
- Institute on Aging
- John Stewart Company
- Larkin Street Youth Services
- LGBT Center
- Lutheran Social Services of Northern California
- Lyric
- Mary Elizabeth Inn
- Mercy Housing
- Metropolitan Fresh Start House
- Mission Hiring Hall
- Mission Housing Development Corporation
- Mission Neighborhood Health Center
- Positive Resource Center
- Providence Foundation
- Raphael House
- Reality House West
- SafeHouse

- ✓ Salvation Army
- ✓ San Francisco Housing Authority
- ✓ San Francisco Network Ministries
- ✓ Sequoia Living
- ✓ St. Anthony's
- ✓ St. Vincent de Paul Society
- ✓ Swords to Plowshares
- ✓ Tenderloin Housing Clinic
- ✓ Tenderloin Neighborhood Development Corporation (TNDC)
- ✓ United Council of Human Services
- ✓ UCSF Citywide
- ✓ Veterans Administration



The ONE System is an online database that enables organizations to collect data on the services they provide to people experiencing homelessness and people who are at risk of homelessness.

© 2003-2023 Bitfocus, Inc. All rights reserved.

System Administration provided by Bitfocus, Inc.  Bitfocus

**From:** Chris K. <ckblueaqua@gmail.com>  
**Sent:** Thursday, February 23, 2023 3:37 PM  
**To:** SOTF, (BOS)  
**Cc:** Lim, Victor (DEM)  
**Subject:** Re: SOTF - Complaint Filed with the Sunshine Ordinance Task Force - File No. 23013(D)  
**Attachments:** image001.png

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Good afternoon SOTF,

Victor Lim contacted me today to inquire about my request.

After speaking to Victor Lim, it is clear that Senior Officials are restricting access and documentation to his office, thus preventing him from being the ultimate record keeper of appropriate data within Department of Emergency Management.

That is one of my main arguments.

I believe with this information combined with what we learned yesterday from DPH, that this warrants a full committee hearing to discuss Record Management by all city/county agencies.

Respectfully,

Chris Ward Kline

On Wed, Feb 15, 2023, 4:12 PM SOTF, (BOS) <[sotf@sfgov.org](mailto:sotf@sfgov.org)> wrote:

Good Afternoon:

The Department of Emergency Management has been named as a Respondent in the attached complaint filed with the Sunshine Ordinance Task Force (SOTF). In an effort to provide the SOTF information in an easy to understand format the SOTF has prepared a revised request format for responding to complaints (attached). **The SOTF requests that you submit your response to our office the allegations including any and all supporting documents, recordings, electronic media, etc., to the Task Force within five (5) business days of receipt of this notice.** In developing and submitting your response, please use the attached instructions, "Preparing San Francisco Sunshine Ordinance Task Force Respondents Materials," to address your defense of this complaint. This is your opportunity to provide a detailed explanation to allow the Task Force to be fully informed in considering your response prior to the meeting.

Please refer to the File Number 23013(D) when submitting any new information and/or supporting documents pertaining to this complaint.

Cheryl Leger

Assistant Clerk, Board of Supervisors

Tel: 415-554-7724



Click to complete a Board of Supervisors Customer Service Satisfaction form.

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*

**From:** Chris K. <ckblueaqua@gmail.com>  
**Sent:** Thursday, February 23, 2023 6:17 PM  
**To:** SOTF, (BOS)  
**Subject:** Respectively Request a Stay

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Good evening,

After most of the responses, I needed to ask your office to potentially ask for a stay of info collection and ask each agency, to follow up with their Senior Officials. If not, these agencies are outright lying and their bosses are setting them up to take the fall.

They are being led down a horrible path.

Let me explain:

Each agency uses technology to conduct surveys, questionnaires, programs, etc. It is done with computer technology that uses text-to-voice/voice-to-technology to gather information and data.

For example, a political party sends out these surveys to gather info, and agenda, etc. Another example would be emergency management training - once you attend, it is there to access at any time within your personal surveillance.

Some of the programs the city uses are MailChimp, SurveyMonkey, SurveyGizmo, etc. There are plenty others.

These programs are supposed to be automatic and computer only; however, a programmer or staff member could interject and alter the automatic program causing and altering outcomes.

These agencies are not even giving me the automatic, but simply stating nothing exist when that is impossible.

I will prove beyond a reasonable doubt, that these agencies have info on me, and not just a little info.

I do not want to embarrass this city and county.

Please ask these agencies and senior officials for the info and provide an additional five days (business days). If these responses stand as is, I will utilize in potential next steps.

Respectfully,

Chris Ward Kline

**From:** Chris K. <ckblueaqua@gmail.com>  
**Sent:** Thursday, March 9, 2023 2:40 PM  
**To:** SOTF, (BOS)  
**Cc:** Heckel, Hank (MYR); Hussey, Deirdre (DPH); Lim, Victor (DEM); Pojman, Natalie (DPH); Miyamoto, Paul (SHF); Toomey, William (POL); Young, Victor (BOS); Somera, Alisa (BOS); Calvillo, Angela (BOS)  
**Subject:** Re: SOTF - Notice of Complaint Committee hearing, March 21, 2023 - 5:30 PM; Room 408, City Hall  
**Attachments:** image001.png

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Good afternoon SOTF,

In reading the bylaws and to expedite File Number 23013 (A-E) and to prevent further delays and respondents denials of files, evidence, I make the following request for March 21, 2023 at 1730 hrs which is not covered by the bylaws.

I request at least 8 minutes (total and combined) to present evidence against each department. I can link the presentation to include each department acting in concert (either formally or informally) to not release files.

The only time stipulation listed on the bylaws is for five minutes in presenting 'new' evidence to reopen the claim.

I will submit all documentation five days prior to hearing, with no foreseen delays, weather permitting.

Respectfully,

Chris Ward Kline  
415-513-9334

On Fri, Mar 3, 2023, 3:32 PM SOTF, (BOS) <[sotf@sfgov.org](mailto:sotf@sfgov.org)> wrote:

Good Afternoon:

Notice is hereby given that the Complaint Committee of the Sunshine Ordinance Task Force (Task Force) shall hold hearings on complaints listed below to: 1) determine if the Task Force has jurisdiction; 2) review the merits of the complaints; and/or 3) issue a report and/or recommendation to the Task Force. ***Please confirm your attendance for this hearing.***

Date: March 21, 2023

Location: Room 408, City Hall

Time: 5:30 p.m.

Complainants: Your attendance is required for this meeting/hearing.

Respondents/Departments: Pursuant to Section 67.21 (e) of the Ordinance, the custodian of records or a representative of your department, who can speak to the matter, is required at the meeting/hearing.

**File No. 22134** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 22135** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 23013A** Complaint filed by Chris Ward Kline against Department of Public Health for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013B** Complaint filed by Chris Ward Kline against Office of the Sheriff for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013C** Complaint filed by Chris Ward Kline against Mayors Office for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013D** Complaint filed by Chris Ward Kline against Department of Emergency Management for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013E** Complaint filed by Chris Ward Kline against San Francisco Police Department (E) e for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**Documentation (evidence supporting/disputing complaint)**

For a document to be considered, it must be received at least five (5) working days before the hearing (see attached Public Complaint Procedure).

For inclusion in the agenda packet, supplemental/supporting documents must be received by **5:00 pm, March 15, 2023**.

Cheryl Leger

Assistant Clerk, Board of Supervisors

Tel: 415-554-7724



Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form.

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*

**Leger, Cheryl (BOS)**

---

**From:** Chris K. <ckblueaqua@gmail.com>  
**Sent:** Tuesday, March 14, 2023 4:43 PM  
**To:** SOTF, (BOS)  
**Cc:** Michael Petrelis; Heckel, Hank (MYR); Hussey, Deirdre (DPH); Lim, Victor (DEM); Pojman, Natalie (DPH); Miyamoto, Paul (SHF); Toomey, William (POL); Young, Victor (BOS); Somera, Alisa (BOS); Calvillo, Angela (BOS)  
**Subject:** Re: SOTF - Notice of Complaint Committee hearing, March 21, 2023 - 5:30 PM; Room 408, City Hall  
**Attachments:** 23013E.pdf; 23013D.pdf; 23013B.pdf; 23013A.pdf; MAINALL.pdf; 23013C.pdf

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Good evening all,

I broke the files and complaints down for each department. MAINALL is for everyone, then just add your specific document for your agency behind the main packet.

I have also included SEC. 19B.1. DEFINITIONS in which all agencies have not complied, not even close.

I may send some additional evidence by tomorrow's deadline.

Also, in response to the Mayor's Office, the entire packet refers to her office as she has a budget committee and multiple documents list the Mayor's Office and London Breed's name basically signing off on the budget, technology, etc.

I also included a few emails of a total 442 emails either sent, received or CC'd to the Mayor's office. She, without a doubt, knows the issues, complaints and has a very detailed understanding of the issues and complaints, sometimes supplied to me. In fact, she and her office actively monitors my emails, sometimes for ideas, complaints, and status, which I will share on 3/21/2023.

I would be more than happy to turn over these few, today and again on 3/21/2023, to have her office investigate. Her complaint is 23013C - I'm also requesting that the previous packet sent, be forwarded to the Mayor, as is as these directives and guidelines to prevent release came from the top and she has an understanding of each department and utilizes some of their equipment and technology.

Thank you in advance.

Respectfully,

Chris Ward Kline

On Fri, Mar 3, 2023 at 3:32 PM SOTF, (BOS) <[sotf@sfgov.org](mailto:sotf@sfgov.org)> wrote:

Good Afternoon:

Notice is hereby given that the Complaint Committee of the Sunshine Ordinance Task Force (Task Force) shall hold hearings on complaints listed below to: 1) determine if the Task Force has jurisdiction; 2) review the merits of the complaints; and/or 3) issue a report and/or recommendation to the Task Force. ***Please confirm your attendance for this hearing.***

Date: March 21, 2023

Location: Room 408, City Hall

Time: 5:30 p.m.

Complainants: Your attendance is required for this meeting/hearing.

Respondents/Departments: Pursuant to Section 67.21 (e) of the Ordinance, the custodian of records or a representative of your department, who can speak to the matter, is required at the meeting/hearing.

**File No. 22134** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 22135** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 23013A** Complaint filed by Chris Ward Kline against Department of Public Health for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013B** Complaint filed by Chris Ward Kline against Office of the Sheriff for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013C** Complaint filed by Chris Ward Kline against Mayors Office for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013D** Complaint filed by Chris Ward Kline against Department of Emergency Management for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013E** Complaint filed by Chris Ward Kline against San Francisco Police Department (E) e for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**Documentation (evidence supporting/disputing complaint)**

For a document to be considered, it must be received at least five (5) working days before the hearing (see attached Public Complaint Procedure).

For inclusion in the agenda packet, supplemental/supporting documents must be received by **5:00 pm, March 15, 2023**.

Cheryl Leger

Assistant Clerk, Board of Supervisors

Tel: 415-554-7724

 Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form.

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*

SEPTEMBER 15, 2022

eff.org



# San Francisco Police Must End Irresponsible Relationship with the Northern California Fusion Center

[ESPAÑOL](#)

In yet another failure to follow the rules, the San Francisco Police Department is collaborating with the regional fusion center with nothing in writing—no agreements, no contracts, *nothing*—governing the relationship, according to new records released to EFF in its ongoing complaint against the agency.

This means that there is no document in place that establishes the limits and responsibilities for sharing and handling criminal justice data or intelligence between SFPD and the fusion center and other law enforcement agencies who access sensitive information through its network.

SFPD must withdraw immediately from any cooperation with the Northern California Regional Information Center (NCRIC). Any moment longer it continues to collaborate with NCRIC puts sensitive data and the civil rights of Bay Area residents at severe risk.

Fusion centers were started in the wake of 9/11 as part of a Department of Homeland Security program to improve data sharing between local, state, tribal, and federal law enforcement agencies. There are 79 fusion centers across the United States, each with slightly different missions and responsibilities, ranging from generating open-source intelligence reports to monitoring camera networks. NCRIC historically has served as the Bay Area hub for sharing data across agencies from automated license plate readers (ALPRs), face recognition,

8/30

social media monitoring, drone operations, and "Suspicious Activity Reports" (SARS).

NCRIC requires all participating agencies to sign a data sharing agreement and non-disclosure agreement ("Safeguarding Sensitive But Unclassified Information"), which is consistent with federal guidelines for operating a fusion center. EFF has independently confirmed with NCRIC staff that SFPD has not signed such an agreement. This failure is even more surprising considering that SFPD has had two liaisons assigned to the fusion center and the police chief has served as chair of NCRIC's executive board.

In December 2020, EFF filed a public records request under the San Francisco Sunshine Ordinance, following a San Francisco Chronicle report suggesting that an SFPD officer had submitted a photo of a suspect to the fusion center's email list and received in response a match generated by face recognition, which would potentially violate San Francisco's face recognition ban. We sought records related to this particular case, but more generally, we sought communications related to other requests for photo identification submitted by SFPD, communications about face recognition, and any agreements between SFPD and NCRIC.

When SFPD failed to comply with our records request, we filed a complaint with the San Francisco Sunshine Ordinance Task Force, the citizen body assigned to oversee violations of open records and meetings laws. Many new documents were released and SFPD was found by the task force to have violated both the Sunshine Ordinance and the California Public Records Act. One document was missing though: the fusion center agreement.

New records released in the complaint now explain why: **no such agreements exist.** SFPD didn't sign any, according to multiple emails sent between staff.

SFPD can't simply solve this problem by signing the boilerplate agreement tomorrow. Any formal partnership or data-sharing relationship with NCRIC would have to go through the process required by the city's surveillance oversight ordinance, which requires public input into such agreements and the board of supervisors' approval. SFPD should expect public opposition to its involvement with the fusion center, just as there was opposition to its involvement in the FBI's Joint Terrorism Task Force.

Even if that process were to move forward, the public must be involved in crafting the exact language of the agreement. For example, when the Bay Area Rapid

Transit (BART) Police Department pursued an agreement with NCRIC, the grassroots advocacy group Oakland Privacy (an Electronic Frontier Alliance member) helped negotiate an agreement with stronger considerations for civil liberties and privacy.

This isn't the first time SFPD has played fast and loose with data regulations. EFF is currently suing the department for accessing a live camera network to spy on protesters without first following the process required by the surveillance oversight ordinance. EFF has also filed a second Sunshine Ordinance complaint against SFPD for failing to produce a mandated ALPR report in response to a public records request.

This latest episode re-emphasizes that SFPD has not earned the trust of the people when it comes to its use of technology and data. SFPD should be cut off from NCRIC immediately, and the Board of Supervisors should treat any claim about accountability from SFPD with skepticism. SFPD has proven it doesn't believe rules matter, and that should always be a deal-breaker when it comes to surveillance.

#### RELATED CASES:

WILLIAMS V. SAN FRANCISCO

## JOIN EFF LISTS

### Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

905

**SUBMIT**

## RELATED UPDATES



DEEPLINKS BLOG BY JENNIFER LYNCH | OCTOBER 11, 2022

### **First Court in California Suppresses Evidence from Overbroad Geofence Warrant**



DEEPLINKS BLOG BY DAVE MAASS | OCTOBER 6, 2022

### **A National Lab Is Promoting a "Digital Police Officer" Fantasy for Law Enforcement and Border Control**

### **Ban Government Use of Face Recognition In the UK**



---

NEWS FIX

# Bay Area Police Departments Using 'StingRay' Surveillance Technology

By Tara Siler Mar 14, 2014

 [Save Article](#)*This article is more than 8 years old.*

This graphic illustrates how a StingRay works. Signals from cellphones within the device's radius are bounced to law enforcement. The information relayed may include names, phone numbers, locations, call records and even text messages. (Courtesy of News10)

Several law enforcement agencies around the Bay Area are using a controversial surveillance technology that can track people and collect data in real time.

StingRays as they're more commonly known- act like a kind of cell tower -- attracting all the surrounding wireless devices on the same network...and retrieving their data.

Police departments in San Francisco, Oakland, San Jose and Fremont are all using these devices, as is the Alameda County District Attorney's office. News 10 in Sacramento revealed

9/2  
970

the extensive use of this surveillance tool through a public records request.

KQED News interviewed Hanni Fakhoury is with the Electronic Frontier Foundation, which advocates for civil rights in the digital world.

**Can you start off by explaining more about what kind of information the StingRay can gather? Can it eavesdrop on actual conversations?**

Sponsored

It can capture conversation. There have been some assurances that these specific sorts of StingRays being used by local law enforcement aren't doing that, but we do know that they have the capability of doing so.

They also have the capability of capturing the metadata or the information about how you communicate. And in these specific instances of local law enforcement using them, they're using that information to pinpoint the person's location.

**It's my understanding that this technology is being used by some law enforcement without a warrant. An Oakland Police Department spokesperson told me in an email that prior to 2009 no warrant was required -- but that now, depending on how it's being used, a search warrant may or may not be required. What's your understanding of how often warrants are being obtained?**

---

**'These devices capture very rich, detailed and intimate information about a person's location and how they communicate and who they communicate with.'**

That's a big question mark because there's a lot of secrecy surrounding the use of these devices. I'm not quite sure why the shift in 2009, and I'm encouraged that they claim they are using search warrants today, but I will note that there has been some concern revealed through public records requests that the ACLU of Northern California did, that some federal court officials, some federal judges, were concerned that law enforcement requesting orders to use these devices weren't being completely forthright with the judges. That they were in fact using StingRays to get some of this information. And so, again, there's a lot of uncertainty

about it. They certainly should be using a search warrant, because these devices capture very rich, detailed and intimate information about a person's location and how they communicate and who they communicate with, and also have the capability to catch the actual content of conversation.

**The StingRays are coming from Homeland Security through federal grants -- does that mean they are supposed to be used to fight terrorism-- rather than more ordinary crime? Are there any guidelines regulating the use of this technology?**

Well you certainly see that with the requests made by local law enforcement agencies that purchase these devices. They are clearly trying to sell the city council or the mayor's office or whoever it may be, that these are devices that can be used really for two purposes: terrorism as well as emergency scenarios that require search and rescue. But the reality of what we are seeing on the ground is that these are being used in a garden variety of criminal cases. You mentioned the Oakland arrest statistics in the reports of the OPD, and if you look through the specific cases they've talked about, these are all garden variety kinds. Murder, robbery, kidnapping. I'm not trying to say those aren't serious crimes, and that they are awful things that should be investigated, but they are not national security concerns in quite the same way we tend to think of that term.

**Given your concern, and others at the ACLU, are we to expect some constitutional challenges to these devices?**

I would think so, and there's already been a little bit of litigation on the use of these devices in state and federal courts. And there's been a lot of litigation on just getting the information about the use of these devices that would be necessary to actually fully litigate the constitutional issues.

Oops, we couldn't find that track.

Privacy policy

94

## SAN FRANCISCO POLICE DEPARTMENT

## INCIDENT REPORT STATEMENT

page 51

INCIDENT NO.	220044404		
NAME (LAST, FIRST, MIDDLE) OF PERSON GIVING STATEMENT		DOB / AGE	RESIDENCE PHONE (DAY / NIGHT)
Kline, Chris WARD		12/25/69 (32)	415-203-1662
RESIDENCE ADDRESS / CITY IF NOT SAN FRANCISCO		ZIP CODE	BUSINESS ADDRESS / CITY IF NOT SAN FRANCISCO
237 Kearny St 114		94108	
DATE OF STATEMENT	TIME STARTED	TIME COMPLETED	LOCATION WHERE STATEMENT TAKEN
1/21/2022	1540	1605	AT SCENE <input type="checkbox"/> OTHER: Northern Station
STATEMENT TAKEN BY (NAME / STAR)		IN PRESENCE OF	
POA WONG 4798.			

I, Chris WARD Kline, was shoved and knocked unconscious at approximately 2015 hrs on 1/20/22 on Kearny outside the Veteran's Building. After waking up, I noticed my wallet and 2 Bass were missing and had abrasions on Right Knee, Above Both eyes and eyeglasses damaged. Prior to Altercation/Robbery, I was attending Post 448 American Legion January meeting.

The contents missing: (2) BANK of America cards, DMV CA license, Clipper Card, VA Health (420), Nordstrom (420), pair of glasses (\$850), (2) chargers (4100), court documents Federal Court, Mail Box Key, Storage Key, Safe Deposit Key (\$250), various clothing, NO cash and total value approximately \$1450. It should be noted that the BOA cards were attempted at Chevron on Kearny for gas but declined. Stephanie is the manager and works on Monday. At 0800.

It is believed that Regional Administrator Matthew Johns could have been involved or had someone take the items due to court proceedings in Federal Court and another related hearing on Monday. Johns works at HHS, 90th & 14th St, SF CA. Personal Info: Chris WARD Kline 12/25/69, 415-203-1662. 94102.

DECLARE, UNDER PENALTY OF PERJURY, THIS STATEMENT OF Chris WARD PAGES IS TRUE AND CORRECT, BASED ON MY PERSONAL KNOWLEDGE.

SIGNATURE OF PERSON GIVING STATEMENT

San Francisco Police Department  
INCIDENT REPORT

220046404

Report Type: Initial

<b>S U S P E C T</b>	Code S 1	Name (Last, First Middle) UNKNOWN, UNKNOWN				Alias				Email		
	Day Phone		Type	Home Address			City			State		Zip Code
	Night Phone		Type	Work Address			City			State		Zip Code
	DOB Unknown <input checked="" type="checkbox"/>		Date of Birth	Age	or age between and		Race U	Sex U	Height	Weight	Hair Color	Eye Color
	SFNO	J/D# (if Juvi)		ID Type/Jurisdiction/Number			ID Type/Jurisdiction/Number			ID Type/Jurisdiction/Number		
	Booking Charge(s)							Booking Location				
	Warrant #		Court#	Action#			Dept#		Enroute to			
	Warrant Violation(s)										Ball (\$)	
	Citation#		Violation(s)				Appear Date/Time		Location of Appearance			
	<input type="checkbox"/> CA Form Booked Copy Attached		Mirandized: Star <input type="checkbox"/>		Date Time		CWR Check 19.00 AM <i>(45)</i>		Star			
Book/Cite Approval		Star	Mass Arrest Code		M X-Rays <input type="checkbox"/>	School (if Juvenile)		Statement <input type="checkbox"/>				
Other Information: Citation/Warrant/Booking Charge(s)/Missing Person-Subject Description; Scars, Marks, Tattoos												
Interpreter Needed <input type="checkbox"/>		Language	Language Description(if Other)				Language Line Service/Interpreter ID#				Bilingual Ofc Star#	

<b>P R O P E R T Y</b>	Code/No EVD 1	Item Description PHOTOGRAPHS - PRINTED				Brand		Model		
	Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.		Quantity 3	Value	
	Seized by (Star) 4798		From Where 1125 FILMORE ST (NORTHERN POLICE STATION)							
	Additional Description/Identifying Numbers THREE PHOTOGRAPHS Submitted at: E - Northern									

<b>P R O P E R T Y</b>	Code/No EVD 2	Item Description STATEMENT				Brand		Model		
	Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.		Quantity 1	Value	
	Seized by (Star) 4798		From Where 1125 FILMORE ST (NORTHERN POLICE STATION)							
	Additional Description/Identifying Numbers ONE PAGE STATEMENT Submitted at: E - Northern									

<b>P R O P E R T Y</b>	Code/No STN 1	Item Description DRIVER LICENSE				Brand CALIFORNIA		Model		
	Serial No. D2876249		Gun Make	Caliber	Color	Narcotics Lab No.		Quantity 1	Value \$35.00 Total	
	Seized by (Star)		From Where							
	Additional Description/Identifying Numbers									

San Francisco Police Department  
INCIDENT REPORT

220046404

Report Type: Initial

P R O P E R T Y	S T N 2	Item Description GLASSES				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
								1	\$850.00 Total
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									
P R O P E R T Y	S T N 3	Item Description KEYS				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
								3	\$250.00 Total
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									
1-mail box key, 1-storage locker key, 1-safe deposit box key									
P R O P E R T Y	S T N 4	Item Description DOCUMENTS				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
								1	TBD
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									
Court documents for a Federal case.									
P R O P E R T Y	S T N 5	Item Description VARIOUS CARDS				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
								5	TBD
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									
2-Bank of America cards, 1-Nordstrom card, 1-Clipper card, 1-VA Health card3									
P R O P E R T Y	S T N 6	Item Description OTHER ITEMS				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
								6	\$350.00 Total
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									
1-phone chargers \$100, 5-clothing \$250.									
P R O P E R T Y	S T N 7	Item Description WALLET				Brand		Model	
		Serial No.		Gun Make	Caliber	Color	Narcotics Lab No.	Quantity	Value
						BLK		1	\$50.00 Total
		Seized by (Star)		From Where					
Additional Description/Identifying Numbers									

**NARRATIVE**

On 01/21/2022 at 1616 hours (R/V1) Chris Kline responded to the front counter of Northern Station to report a robbery and relayed to me the following. I took this report with the approval of Sergeant Smith #15.

Kline stated that on 01/20/2022 at approximately 2015 hours he was standing on the sidewalk near the War Memorial Veterans Building at 401 Van Ness Ave. Kline stated that (S1) unknown approached him from an unknown direction, shoved or hit him with an unknown object causing him to fall onto the sidewalk and lose consciousness for an unspecified amount of time. Kline stated that after he regained consciousness, he noticed his (STN1-STN7) items stolen. Kline did not give anyone permission to take his items. Kline did not have any suspect information, any witnesses and did not note any surveillance cameras in the area. Kline stated that his Bank of America cards were fraudulently used at the Chevron gas station on Van Ness Ave, but the purchases were declined. Kline stated he sustained bruising and abrasion to his forehead, nose and right knee. I observed visible abrasions on Kline's nose and forehead, Kline declined all medical service at Northern Station and he would see his own doctor.

Kline wrote (EVD1) one page statement, which I seized, uploaded to this report, and booked as evidence at Northern Station.

Office Tano #2172 took (EVD2) three photographs of Kline's injuries, which I have uploaded to this report, and I booked the photographs as evidence at Northern Station.

I provided Kline a follow up form with the case number, a Victims of Crime card, a Marsy's Card and explained follow up instructions.

90  
98  
SFPD Crime Information Services (43518)  
Retrieved by 308150 on 1/14/21 11:11:04 AM

## San Francisco Police Department

## INCIDENT REPORT

220046404

Report Type: Initial

I	Incident Number 220-046-404	Occurrence From Date / Time 01/20/2022 20:15	Occurrence To Date / Time	Reported Date / Time 01/21/2022 16:16	CAD Number 220212315				
N	Type of incident ROBBERY, W/ FORCE 03074 THEFT, FROM PERSON, >\$950 (OTHER THAN PICKPOCKET) 06154								
C	Location of Occurrence: At Intersection wth/Premise Type 401 VAN NESS AVE SIDEWALK					District NORTHERN			
I	Confidential Report? <input type="checkbox"/>	Arrest Made? <input type="checkbox"/>	Suspect Known? <input type="checkbox"/>	Suspect Unknown? <input checked="" type="checkbox"/>	Non-Suspect Incident? <input type="checkbox"/>	Domestic Violence? <input type="checkbox"/>	(Type of Weapon Used)	Use of Force? <input type="checkbox"/>	Reporting Unit 3E00D
D	Location Sent / On View: At Intersection with 1125 FILLMORE ST					Reporting District NORTHERN			
E	Crime and Clearance Status 0	Reported to Bureau	Name Star	Date/ Time	Elder Victim <input type="checkbox"/>	Gang Related? <input type="checkbox"/>	Juvenile Subject? <input type="checkbox"/>	Prejudice Based? <input type="checkbox"/>	
Have you reviewed the attached list of procedures required by Department General Order (DGO) 7.04?									
O	I declare under penalty of perjury, this report of <u>4</u> pages is true and correct, based on my personal knowledge, or is based on information and belief following an investigation of the events and parties involved.								
F	PROF 115 CERTIFIED Post Training								
C	Reporting Officer (PSA) WONG, ANTHONY K	Star 4798	Station Northern Station	Watch 1500-0100	Date 01/21/22 22:00				
R	Reviewing Officer HUANG, EDMUND T	Star 2448	Station Northern Station	Watch 1500-0700	Date 01/21/22 23:16				
A	OIC HUANG, EDMUND T	Star 2448	Station Northern Station	Watch 1500-0700	Date 01/21/22 23:17				
I	Related Case -	Related Case -	Re-assigned to Copies to 5J200 3*300 3*300	Assigned to 5J200 Add'l Copies	Assigned by EH 2448				
N									

R	Code R/W 1	Name (Last, First Middle) KLINE, CHRIS WARD			Alias	Email							
V	Day Phone (415) 203-1662	Type Cell	Home Address 237 KEARNY ST, APT/A14			City SAN FRANCISCO	State CA	Zip Code 94108-					
I	Night Phone	Type	Work Address			City	State	Zip Code					
C	DOB 12/25/69	Age 52	DOB Unk. <input type="checkbox"/>	or age between and	Race W	Sex M	Height 5'11	Weight 175	Hair Color BLN	Eye Color BLU	ID Type	Jurisd.	ID No.
T	Confidential Person <input type="checkbox"/>	Violent Crime Notification <input checked="" type="checkbox"/>	293 PC Star Notification <input type="checkbox"/> 4798			Follow-up Form YES	Statement <input checked="" type="checkbox"/>	YES <input checked="" type="checkbox"/>	Relationship to Subject STRANGER/NONE				
I	School (If Juvenile)		Injury/Treatment			Other Information/If Interpreter Needed Specify Language							
M	Interpreter Needed <input type="checkbox"/>	Language			Language Description (If Other)		Language Line Service/Interpreter ID#			Bilingual Ofc Star#			

934

SFPD Crime

220046404

## SAN FRANCISCO POLICE DEPARTMENT INCIDENT REPORT

INCIDENT NUMBER: 226208769

## HEADING

TYPE OF INCIDENT 653M 19050	INITIAL SUPP <input checked="" type="checkbox"/>	TIME STARTED 01/24/2023 01:00	TIME ENDED 01/24/2023 08:00	LOCATION OF OCCURRENCE 237 KEARNY Street, 114, SAN FRANCISCO, CA
TIME REPORTED 01/24/2023 14:55	REPORTING UNIT 2F00 Internet	TYPE OF PREMISE Apartment	CAD NO.	RELATED CASE NUMBER 3CENTRAL300

## OFFICER DECLARATION

PREPARED BY	REVIEWED BY Q50 brandon McKelly 2343	OIC APPROVAL
-------------	---	--------------

## PERSON LISTINGS

CODE V	NAME (LAST, FIRST) KLINE,CHRIS	DOB **	RACE ***	SEX ***	DRIVERS LICENSE NO ***	LICENSING STATE ***
EMAIL CKBLUEAQUA@GMAIL.COM	RESIDENCE ADDRESS ***				PHONE ***	
EMPLOYER NAME	BUSINESS ADDRESS ***				PHONE ***	

## NARRATIVE

This is supplemental to report #22-6208769

I, Chris Ward Kline, have made arrangements to speak with an investigator concerning this incident. Due to safety and security of this conversation, I will not name the investigator or the agency being represented. The conversation was to take place week ending 1/29/2023.

After receiving an email conversation of this planned meeting, the cyberstalking intensified with more threats and duration. The last two mornings at approximately 0100 hrs, both on 1/23/2023 and 1/24/2023, the cyberstalking with the unwanted and unsolicited calls continued.

Again, this information is collected and saved within the Department of Emergency Management and Sheriff's Department. The app they are using is called One System and individuals were given credentials that have no reason to have these credentials. With these credentials, they would just need to have your email and/or phone number to cyberstalk a person(s).

I find it threatening, abusive, intimidating by these few. City and County Officials know who the individuals are and have not acted on bringing up criminal charges are indictments.

It is not known why city and county officials are protecting these few individuals. It is possible that the city and county officials received political donations to receive these credentials.

These facts are presented knowing the penalties of perjury.



Chris K. &lt;ckblueaqua@gmail.com&gt;

## Your Online Police Report T23002169 Has Been Submitted

1 message

CaSfPd@coplogic.com <CaSfPd@coplogic.com>  
Reply-To: sfpdonlinereports@sfgov.org  
To: CKBLUEAQUA@gmail.com

Tue, Jan 24, 2023 at 2:55 PM

THIS IS AN AUTOMATED RESPONSE -DO NOT REPLY TO THIS EMAIL

PLEASE READ THE FOLLOWING

Your online report has been successfully received.  
You will be notified via email if there are any problems with your report or if additional information is required. Once your report is approved, it will be issued a case number and you will receive a PDF copy as an attachment in your email within approximately ten business days.

If you do not receive a reply within the above time, you may contact the District Police Station where the incident occurred regarding the status of your online report. Provide your report T# when contacting the District Station. District Stations are listed here:

<http://sf-police.org/index.aspx?page=796>

DO NOT REPLY to this email to inquire about the status of your report.

If you have additional information regarding this report, you may submit it by filing a Supplemental Report online and referencing the T# you will receive via email. Once your report has been approved, you should use the 9-digit report number you will get that does not begin with a "T" to submit any Supplemental Reports.

DO NOT REPLY TO THIS EMAIL for this purpose.

THIS IS AN AUTOMATED RESPONSE -DO NOT REPLY TO THIS EMAIL

San Francisco Police Department

The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and/or work product and as such is privileged and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.

10/  
986



This incident has been reported to the  
San Francisco Police Department  
and is pending approval

San Francisco Police Department  
1245 3rd St - Crime Information Services Unit  
San Francisco, CA 94158  
415-575-7232

General Information

Incident Type: Harassing Phone Call  
Case Number: Pending  
Report Date: 01/24/2023 02:55 PM

Reporting Person Information

Name: KLINE, CHRIS  
Home Address: 253 KEARNY Street, 114, San Francisco, CA 94108, US  
Nighttime Phone: 415-513-9334  
Email: CKBLUEAQUA@GMAIL.COM  
Daytime Phone: 415-513-9334  
Race: White  
Sex: Male  
DOB: 12/25/1969  
Driver License No: D2876249  
Licensing State: CA

Incident Information

Incident Location: 237 KEARNY Street, 114, SAN FRANCISCO, CA 94108  
Incident Time (start): 01/24/2023 01:00 AM  
Incident Time (end): 01/24/2023 08:00 AM  
Location Type: Apartment

Narrative

This is supplemental to report #22-6208769.

I, Chris Ward Kline, have made arrangements to speak with an investigator concerning this incident. Due to safety and security of this conversation, I will not name the investigator or the agency being represented. The conversation was to take place week ending 1/29/2023.

After receiving an email conversation of this planned meeting, the cyberstalking intensified with more threats and duration. The last two mornings at approximately 0100 hrs, both on 1/23/2023 and 1/24/2023, the cyberstalking with the unwanted and unsolicited calls continued.

Incident Description

Again, this information is collected and saved within the Department of Emergency Management and Sheriff's Department. The app they are using is called One System and individuals were given credentials that have no reason to have these credentials. With these credentials, they would just need to have your email and/or phone number to cyberstalk a person(s).

I find it threatening, abusive, intimidating by these few. City and County Officials know who the individuals are and have not acted on bringing up criminal charges or indictments.

It is not known why city and county officials are protecting these few individuals. It is possible that the city and county officials received political donations to receive these credentials.

These facts are presented knowing the penalties of perjury.

[Print This Report](#)

1907

## SAN FRANCISCO POLICE DEPARTMENT INCIDENT REPORT

INCIDENT NUMBER: 226208769

## HEADING

TYPE OF INCIDENT	INITIAL SUPP	TIME STARTED 07/15/2015 07:00	TIME ENDED 10/23/2022 12:00	LOCATION OF OCCURRENCE 750 Market Street, SAN FRANCISCO, CA	
TIME REPORTED 10/23/2022 12:28	REPORTING UNIT 2F00 Internet	TYPE OF PREMISE All others, explain in Narrative	CAD NO.	RELATED CASE NUMBER 3TENDERLOIN300	LOCATION SENT TO

## OFFICER DECLARATION

PREPARED BY	REVIEWED BY Sgt Kimberly Ng 1817	OIC APPROVAL
-------------	-------------------------------------	--------------

## PERSON LISTINGS

CODE V	NAME (LAST, FIRST) Kline, Chris	DOB ***	RACE ***	SEX ***	DRIVERS LICENSE NO ***	LICENSING STATE ***
EMAIL	ckblueaqua@gmail.com	RESIDENCE ADDRESS ***			PHONE ***	
EMPLOYER NAME		BUSINESS ADDRESS ***			PHONE ***	

## NARRATIVE

I, Chris Ward Kline, a resident and employed within the city and county of San Francisco, report that the aforementioned dates and times, I was and still currently being harassed and cyberstalked with unwanted phone calls, messages, text, spam, etc.

It has come to my attention through professional relationships, prior knowledge, education and work experience that the city and county of San Francisco utilizes an app called One System. One System was designed by Biltfocus out of Nevada. The city and county of San Francisco issues credentials for the app for public health, safety for politicians for day to day business practices and these credentials are maintained within the Department of Emergency Management. The app One System allows the user to send text to voice and voice to text messages (which are considered audio) for surveys, public health, situational awareness and to guide people in need for the appropriate resources. Used incorrectly and outside the scope of state and federal law, it can be used to harass, threaten and cyberstalk.

Here is a brief 36 hour time line of events that impacted my life with the app One System.

- 1) On 10/22/2022, between the hours of 1200-1500 hrs, unknown individual(s) used One System to Cyberstalk to cause wins and losses in billiards of various people to include me
- 2) During the last 36 hours, these unknown individual(s), and for a longer period of aforementioned dates, to send data to others that was unsolicited, or alter messages, delete or send malware amongst other things.
- 3) This morning before and after Church at Glide Memorial, there were three attempts to have a vehicle strike while others were Cyberstalked with the intent to cause great bodily injury and/or aggravated assault.

Within the Department of Emergency Management, this data is considered surveillance and is stored within the Interoperable Communications as it is done with GPS and GPRS.

I will testify against any and all public officials responsible.

10988

## SAN FRANCISCO POLICE DEPARTMENT INCIDENT REPORT

INCIDENT NUMBER: 226208769

## HEADING

TYPE OF INCIDENT 653M 19050	INITIAL SUPP <input checked="" type="checkbox"/>	TIME STARTED 07/15/2015 07:00	TIME ENDED 10/23/2022 12:00	LOCATION OF OCCURRENCE 750 Market Street, SAN FRANCISCO, CA		
TIME REPORTED 10/23/2022 12:28	REPORTING UNIT 2F00 Internet	TYPE OF PREMISE All others, explain in Narrative		CAD NO.	RELATED CASE NUMBER	LOCATION SENT TO 3TENDERLOIN300

## OFFICER DECLARATION

PREPARED BY	REVIEWED BY Sgt Kimberly Ng 1817	OIC APPROVAL
-------------	-------------------------------------	--------------

## PERSON LISTINGS

CODE V	NAME (LAST, FIRST) Kline ,Chris	DOB ***	RACE ***	SEX ***	DRIVERS LICENSE NO ***	LICENSING STATE ***
EMAIL ckblueaqua@gmail.com	RESIDENCE ADDRESS ***				PHONE ***	
EMPLOYER NAME	BUSINESS ADDRESS ***				PHONE ***	

## NARRATIVE

I, Chris Ward Kline, a resident and employed within the city and county of San Francisco, report that the aforementioned dates and times, I was and still currently being harassed and cyberstalked with unwanted phone calls, messages, text, spam, etc.

It has come to my attention through professional relationships, prior knowledge, education and work experience that the city and county of San Francisco utilizes an app called One System. One System was designed by Bitfocus out of Nevada. The city and county of San Francisco issues credentials for the app for public health, safety for politicians for day to day business practices and these credentials are maintained within the Department of Emergency Management. The app One System allows the user to send text to voice and voice to text messages (which are considered audio) for surveys, public health, situational awareness and to guide people in need for the appropriate resources. Used incorrectly and outside the scope of state and federal law, it can be used to harass, threaten and cyberstalk.

Here is a brief 36 hour time line of events that impacted my life with the app One System.

- 1) On 10/22/2022, between the hours of 1200-1500 hrs, unknown individual(s) used One System to Cyberstalk to cause wins and losses in billiards of various people to include me
- 2) During the last 36 hours, these unknown individual(s), and for a longer period of aforementioned dates, to send data to others that was unsolicited, or alter messages, delete or send malware amongst other things.
- 3) This morning before and after Church at Glide Memorial, there were three attempts to have a vehicle strike while others were Cyberstalked with the intent to cause great bodily injury and/or aggravated assault.

Within the Department of Emergency Management, this data is considered surveillance and is stored within the Interoperable Communications as it is done with GPS and GPRS.

I will testify against any and all public officials responsible.

104989

## SAN FRANCISCO POLICE DEPARTMENT INCIDENT REPORT

INCIDENT NUMBER: 226208769

## HEADING

TYPE OF INCIDENT	INITIAL SUPP	TIME STARTED 07/15/2015 07:00	TIME ENDED 10/23/2022 12:00	LOCATION OF OCCURRENCE 750 Market Street, SAN FRANCISCO, CA
TIME REPORTED 10/23/2022 12:28	REPORTING UNIT 2F00 Internet	TYPE OF PREMISE All others, explain in Narrative	CAD NO.	RELATED CASE NUMBER 3TENDERLOIN300

## OFFICER DECLARATION

PREPARED BY	REVIEWED BY Sgt Kimberly Ng 1817	OIC APPROVAL
-------------	-------------------------------------	--------------

## PERSON LISTINGS

CODE	NAME (LAST, FIRST)	DOB ***	RACE ***	SEX ***	DRIVERS LICENSE NO ***	LICENSING STATE ***
V	Kline, Chris					
EMAIL	ckblueaqua@gmail.com	***			PHONE ***	
EMPLOYER NAME		BUSINESS ADDRESS ***			PHONE ***	

## NARRATIVE

I, Chris Ward Kline, a resident and employed within the city and county of San Francisco, report that the aforementioned dates and times, I was and still currently being harassed and cyberstalked with unwanted phone calls, messages, text, spam, etc.

It has come to my attention through professional relationships, prior knowledge, education and work experience that the city and county of San Francisco utilizes an app called One System. One System was designed by Bifocus out of Nevada. The city and county of San Francisco issues credentials for the app for public health, safety for politicians for day to day business practices and these credentials are maintained within the Department of Emergency Management. The app One System allows the user to send text to voice and voice to text messages (which are considered audio) for surveys, public health, situational awareness and to guide people in need for the appropriate resources. Used incorrectly and outside the scope of state and federal law, it can be used to harass, threaten and cyberstalk.

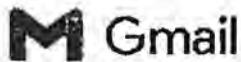
Here is a brief 36 hour time line of events that impacted my life with the app One System.

- 1) On 10/22/2022, between the hours of 1200-1500 hrs, unknown individual(s) used One System to Cyberstalk to cause wins and losses in billiards of various people to include me
- 2) During the last 36 hours, these unknown individual(s), and for a longer period of aforementioned dates, to send data to others that was unsolicited, or alter messages, delete or send malware amongst other things.
- 3) This morning before and after Church at Glide Memorial, there were three attempts to have a vehicle strike while others were Cyberstalked with the intent to cause great bodily injury and/or aggravated assault.

Within the Department of Emergency Management, this data is considered surveillance and is stored within the Interoperable Communications as it is done with GPS and GPRS.

I will testify against any and all public officials responsible.

105  
990



Chris K. &lt;ckblueaqua@gmail.com&gt;

## Your Online Police Report 226208769 Has Been Approved

CaSfPd@coplogic.com <CaSfPd@coplogic.com>  
Reply-To: sfpdonlinereports@sfgov.org  
To: ckblueaqua@gmail.com

Sun, Nov 6, 2022 at 6:43 AM

**THIS IS AN AUTOMATED RESPONSE -DO NOT REPLY TO THIS EMAIL**

Your online report has been approved and the incident case number is 226208769. Sensitive information has been replaced with \*\*\* in order to maintain your privacy in emails.

If you discover additional items missing, you can report this information by making an online Supplemental Report and entering your Original report number when requested.

This report has been assigned to the District Station Investigation Team in the police district where your incident occurred. District Stations are listed here:

<http://sf-police.org/index.aspx?page=796>.

You will be notified by the District Station Investigation Team if an arrest is made or your belongings are recovered.

If you have any further information that may assist the investigation, please call the Station Investigative Team or submit a Supplemental Report online.

If you wish to add more property to this report or add details such as serial numbers to the property listed in this report, you may file a Supplemental Report online by referencing the 9-digit report number provided above. Explain in the Comments field why you are submitting the Supplemental Report.

For crime prevention tips and safety awareness, visit <http://www.sfsafe.org/>

**THIS IS AN AUTOMATED RESPONSE -DO NOT REPLY TO THIS EMAIL**

The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and/or work product and as such is privileged and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.

---

[report-226208769.pdf](#)  
5K

106



This incident has been reported to the  
San Francisco Police Department  
and is pending approval.

San Francisco Police Department  
1245 3rd St - Crime Information Services Unit  
San Francisco, CA 94158  
415-575-7232

**General Information**

Incident Type: Harassing Phone Call  
Case Number: Pending  
Report Date: 10/23/2022 12:28 PM

**Reporting Person Information**

Name: Kline, Chris  
Home Address: 237 Kearny Street, 114, San Francisco, CA 94108, US  
Nighttime Phone: 415-513-9334  
Email: ckblueaqua@gmail.com  
Daytime Phone: 415-513-9334  
Race: White  
Sex: Male  
DOB: 12/25/1969  
Driver License No: 02876249  
Licensing State: CA

**Incident Information**

Incident Location: 750 Market Street, SAN FRANCISCO, CA 94108  
Incident Time (start): 07/15/2015 07:00 AM  
Incident Time (end): 10/23/2022 12:00 PM  
Location Type: All others, explain in Narrative

**Narrative**

I, Chris Ward Kline, a resident and employed within the city and county of San Francisco, report that the aforementioned dates and times, I was and still currently being harassed and cyberstalked with unwanted phone calls, messages, text, spam, etc.

It has come to my attention through professional relationships, prior knowledge, education and work experience that the city and county of San Francisco utilizes an app called One System. One System was designed by Bitfocus out of Nevada. The city and county of San Francisco issues credentials for the app for public health, safety for politicians for day to day business practices and these credentials are maintained within the Department of Emergency Management. The app One System allows the user to send text to voice and voice to text messages (which are considered audio) for surveys, public health, situational awareness and to guide people in need for the appropriate resources. Used incorrectly and outside the scope of state and federal law, it can be used to harass, threaten and cyberstalk.

**Incident Description**

Here is a brief 36 hour time line of events that impacted my life with the app One System.

- 1) On 10/22/2022, between the hours of 1200-1500 hrs, unknown individual(s) used One System to Cyberstalk to cause wins and losses in billiards of various people to include me
- 2) During the last 36 hours, these unknown individual(s), and for a longer period of aforementioned dates, to send data to others that was unsolicited, or alter messages, delete or send malware amongst other things.
- 3) This morning before and after Church at Glide Memorial, there were three attempts to have a vehicle strike while others were Cyberstalked with the intent to cause great bodily injury and/or aggravated assault.

Within the Department of Emergency Management, this data is considered surveillance and is stored within the Interoperable Communications as it is done with GPS and GPRS.

I will testify against any and all public officials responsible.

[Print This Report](#)

107  
992

# CLAIM AGAINST THE CITY AND COUNTY OF SAN FRANCISCO

Before completing this form please read the instructions on the back. Untimely claims will be returned. Please submit this form and supporting documentation to the Controller's Office, Claims Division, 1390 Market Street, 7<sup>th</sup> Floor, San Francisco, CA 94102 in person or by mail.

\* = REQUIRED \*\* = REQUIRED IF KNOWN

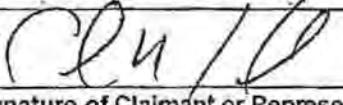
1. Claimant's Name and Home Address, (Please Print Clearly)		2. Send Official Notices and Correspondence to:	
* Chris WARD Kline 250 Kearny St Unit 618 City San Francisco State CA Zip 94108 Telephone Daytime 415-513-9334 Evening Cellular		* Chris WARD Kline 237 Kearny St PMB 114 City San Francisco State CA Zip 94108 Telephone Daytime 415-513-9334 Evening Cellular	
3. Date of Birth	12-25-1969	4. Social Security Number	213-86-5798
7. Location of Incident or Accident		5. Date of Incident	
** VAW MSS SFPO # 220046404		* 1/20/22 ** 2111 hrs	
8. Claimant Vehicle License Plate #, Type, Mileage, and Year **			

9. Basis of Claim. State in detail all facts and circumstances of the incident. Identify all persons, entities, property and City departments involved. State why you believe the City is responsible for the alleged injury, property damage or loss.			
* MATT HANEY, and others, ARE USING their credentials within public health + safety to keep surveillance on me that influenced others to commit robberies, Aggravated ASSAULT, then influence Police Officers, CAPTAINS to NOT investigate			

Name, I.D. Number and City Department of City Employee who allegedly caused injury or loss	Type of City Vehicle	Vehicle License Number and Bus or Train Number
** MATT HANEY, Board of Supervisor	** N/A	** N/A

10. Description of Claimant's injury, property damage or loss	11. Amount of Claimant's property damage or loss and method of computation. Attach supporting documentation. (See Instructions)
* from robbery: estimated \$1500.00 from Burglary of Residence \$200.00 lost wages Approximately \$300.00. on Restriction of Rights, violation Title 18, U.S.C. section 241 & 242 = \$1,000,000.00	ITEMS * glasses \$ 1,000.00 clothing \$ 250.00 personal items \$ 250.00 cash \$ 200.00 TOTAL AMOUNT \$ 1,301,700.00
Breakdown listed above	

12. Witnesses (if any) Name	Address	Telephone
1. SF Public Health, CAPTAIN Chris Canning		
2. Mayor + Board of Supervisors, Assembly MATT HANEY		

13. 	6/23/22	Do Not Write In This Space
Signature of Claimant or Representative Chris WARD Kline	Date 6/23/22	
Print Name	Relationship to Claimant	
CRIMINAL PENALTY FOR PRESENTING A FALSE OR FRAUDULENT CLAIM IS IMPRISONMENT OR FINE OR BOTH. (PENAL CODE §72)		

Presentation March 21, 2023 at 1730 hrs

Good evening and thank you Sunshine Ordinance Task Force for allowing me to speak to the Commission.

I'm Chris Ward Kline, a Northeastern University Criminal Justice graduate with Public Health/Safety experience within hospitals, hotels, retail, housing, homelessness areas, risk management, emergency management. I have also been involved with high level protections of foreign presidents, dignitaries, VIP's, etc. I have a wealth of knowledge regarding electronic surveillance, both collecting data, metadata both for legal and illegal purposes.

I also have experience as a security consultant having previously contracted with NCS Pearson and the Department of Transportation at LAX and surrounding airports as the Security Director shortly after 9/11 in revamping airport security.

Unfortunately, the city and county of San Francisco, is not turning over required files and data due to personal and political reasons. Imagine, having the gold card with unlimited withdrawals, the wine bottle that keeps pouring wine, or the ability to influence a person(s) to consistently do what you want, and making that person, genuinely think it was their own decision, when in fact it wasn't. This is the only reason, the mayor and other agencies refuse to turn over all files, because it would shed light to unauthorized utilization of technology and rain on their parade.

Let's review technology:

- 1) Reference page 1 - 1975 during the Church Commission, it was discussed 'U.S. perfected technology to monitor messages that go through the air...reminiscent of the Stassi in East Germany, KGB in Russia and of course the surveillance state of North Korea and China. It further discussed that a 'Dictator could impose a tyranny on its people'. The Church

Commission stated 'we must ensure all agencies operate within the law and with proper supervision'.

One Reason for the creation of the Sunshine Ordinance Task Force was for this very reason.

- 2) Reference pages 2-8 – Forbes article discusses the technology in 2003 which is widely utilized. That was over 19 years ago.
- 3) Reference page 9 – San Francisco Built a System (One System) to track all homeless people, but also every person and agency that works with homeless or receive funds from the city and county.
- 4) Reference pages 10-11 – Big Brother in SF, so much that in 2019 the Episcopal Community stated 'there's lots of privacy concern' reference One System
- 5) Reference pages 12-13 – Similar App to One System section VI (6) that sending fraudulent, threatening, harassing messages, spamming, bombing (tech term) is not allowed, but the city and county of San Francisco widely disregards!
- 6) Reference pages 14-23 – similar tech and app SurveyMonkey (now called Momentive) Acceptable Usage Policy clearly states under 'YOUR RESPONSIBILITIES "you may not use the Services to commit an unlawful activity; use the Services for activities where use or failure of the Services could lead to PHYSICAL DAMAGE, DEATH, MENTAL HARM, OR PERSONAL INJURY". Let that sink in for a second.  
\*\*\*\*The city and county of San Francisco utilizes SurveyMonkey, Survey Gizmo, MailChimp, One System, plus a host of other apps and technology.
- 7) Reference pages 24-31 – discusses the technology and some researchers, inventors in which technology has been around for over a century.
- 8) Reference pages 32/33 Bitfocus declaring it does not utilize DO NOT TRACK SIGNALS

So, One System, Bitfocus, Momentive, SurveyMonkey, and so on are terms that I never heard of until fairly recently, After speaking up about these concerns that

are public information, the city and county of San Francisco used some of these and others to cause to me, Chris Ward Kline:

- 1) Homelessness
- 2) Restrictions of jobs, income, revenue, grants to my Non-profit PAVEN (Prejudice And Violence Ends Now)
- 3) Monitored and harassed friends and family
- 4) Refused to step in and provide the resources (previously mentioned) to get home to my mother's funeral, my grandmother's funeral and great aunt's funeral between 2020-2021 – to teach me a lesson and to attempt to discredit me with my family.
- 5) Used to influence individuals to cause a robbery of myself, multiple hostile situations, false medical diagnosis, and even to use this technology to alter outcomes of billiard games and softball games. They even prevented me from traveling to Dallas for the Softball World Series in August 2022 and Las Vegas National Pool Tournament in March 2023.

And after repeated requests, the city and county denied not just any records but that zero records exist.

Reference page 34-35

Any app or technology used in the city and county of San Francisco such as One System, Surveillance by SFPD and Sheriff, Facebook, Twitter, Uber would fall under an appropriate MHz channel issued, to the city and county of San Francisco by the F.C.C. Reference page 34-35!

## SAN FRANCISCO DEPARTMENT OF PUBLIC HEALTH

With multiple specific detailed request(s), San Francisco Department of Public Health repeatedly denied records existed:

- 1) Reference SFDPH pages 36-42 show records that should have been kept, maintained and supplied upon request(s), but not provided upon request(s).
- 2) Reference SFDPH pages 43-46 shows a list of medical conditions and appropriate reporting steps to Public Health – at least one of these was reported to San Francisco Public Health, but not provided upon request(s)
- 3) Reference SFDPH pages 47-55 - City and county of San Francisco donates to third parties such as the Felton Institute who engages in surveillance type work, i.e. suicide hotline, HIV hotline, eviction services which are all, a public health responsibility, but SFDPH is simply stating there is no oversight, or files. More on Felton later as it cross references with the Sheriff Department. SFDPH, FELTON AND THE SHERIFF using computer programs that simply voices in your head, that mimic your inner voice. If you notice the printout concerning Felton, someone printed 'survey' on each page, because that is what they typically call the program. Page 55 clearly shows SFDPH uses HIV Surveillance technology.
- 4) Gross denial of utilization of Surveillance Equipment to include Ehars, Epi-x, One System and other surveillance systems which is a MAIN function of Public Health. Section 308(d) of the Public Health Service Act allows for a citizen to legally request and receive a copy of all surveillance activities for normal reasons and other reasons to challenge legally, the scope, actions and results of any research, interventions, trace contacting, HIV surveillance.
- 5) Reference SFDPH pages 56-59 shows Consumer Assessment of Healthcare Providers and Systems in regard to SurveyMonkey. Also enclosed is the federal agency H.H.S. third party and applications Impact Assessment – thus admitting to the utilization of these apps in each level of health care are the county, state and federal government.

SAN FRANCISCO DEPARTMENT OF PUBLIC HEALTH SIMPLY DENIED ALL FILES, BUT STATED IN AN EMAIL, THAT HIV SURVEILLANCE IS PROTECTED AND CANNOT BE RELEASED. SIMPLY PUT, SFDPH IS USING ILLEGALLY TO VIOLATE MY RIGHTS, ATTEMPT TO FORCE ME TO MOVE, AND RESTRICT INCOME, GRANTS, REVENUE.

#### SAN FRANCISCO SHERIFFS'S DEPARTMENT

With multiple specific detailed request(s), San Francisco Sheriff's Department repeatedly denied records existed:

- 1) Reference pages 60-64 show probably cause that Sheriff has collected records of members of the public and its own staff, some resulting in civil court hearings
- 2) Reference page 65 – shows camera and surveillance system that sits on top of Public Library and Asian Art Museum which is used by the Sheriff (and others), to collect data, metadata on anyone that walks in the path and directly to the entrance of City Hall. This system collects your phone data, phone number and other data for the sole purposes of simply tracking individuals, gay people during Gay Pride, political dissidents who may protest in front of City Hall, or other large civic gatherings.
- 3) Reference pages 66-69, shows Public Records Request December 13, 2022, with normal response of December 22, 2022 expected but their own Legal Department asked for an extension until and their own deadline of January 6, 2023. Here we are as of March 11, 2023, the request is still not completed – because they are in a legal jumbo because records do exist.
- 4) Part of my job as an investigator, I interacted with people on Probation, Parole or individuals who were sent to jail and/or prison. These interviews were recorded by the Sheriff Department but not released upon a valid specific request(s) i.e. San Francisco resident in 2001, was using crack, pulled a file alarm and I contacted 911, and was later testified at his parole hearing at San Quinton but the Sheriff states no records exist.
- 5) Reference pages 70-73 which shows an Internal Affairs report with supporting evidence sent certified mail, but this was not included with my requests nor was it investigated.

- 6) Reference pages 74-83 is budget that not only states that surveillance exist, but they contract the surveillance out to a third party....\$1,128,000 for a company that is for-profit – it is their goal to place people on surveillance to make more money. The Sheriff has a budget for 2 civilians, 25.5 sworn officers just for surveillance and two sworn officers for the Felton Institute page 79 for eviction services. Simply put, the Sheriff (and others) are using Felton Institute programs to place on people on surveillance that they want to move, discredit, political dissident, etc.
- 7) Reference pages 84-87 copies for the DA and Sheriff of Surveillance Technology in usage; clearly, there would be a few pages of files on me, but none exist.

**SAN FRANCISCO SHERIFF DEPARTMENT SIMPLY DENIED ALL FILES, EVEN THOUGH THEIR CORE ROLE IS TO CONDUCT SURVEILLANCE ON INMATES, PAROLE AND PROBATION; HOWEVER, THEY USE ON MEMBERS OF THE PUBLIC SUCH AS POLITICAL DISSIDENTS. SIMPLY PUT, SF SHERIFF IS USING ILLEGALLY TO VIOLATE MY RIGHTS, ATTEMPT TO FORCE ME TO MOVE, AND RESTRICT INCOME, GRANTS, REVENUE.**

#### **SAN FRANCISCO POLICE DEPARTMENT**

- 1) Reference pages 88-91 SFPD Must End Irresponsible Relationship with the Northern California Fusion Center – otherwise put, they are not reporting correctly, this is why they claim no files or data exist.
- 2) Reference pages 92-94 Bay Area Police Departments (Include San Francisco) using Stingray technology – again, if you are a political dissident, SFPD would use this on technology, but simply state it doesn't exist. This technology gives you real time GPS, GPRS, and with other technology, they could interfere with social gatherings, alter outcomes with softball, billiards, get someone agitated, cause an accident – REMEMBER, MOMENTIVE ACCEPTABLE USAGES AND USER RESPONSIBILITY THAT INCORRECT USAGES COULD CAUSE MENTAL HARM, DEATH, PHYSICAL INJURY, ETC.

- 3) Reference pages 95-108 multiple emails, police reports that SFPD simply state that they did not have any records. At least SFDPH admitted that they had emails sent by me.

#### BITFOCUS DESIGNER OF ONE SYSTEM

- 1) Reference pages 109-117 – shows various federal partners that utilize data supplied to them from cities such as San Francisco. These include H.H.S., Veterans Affairs and HUD. Also included would be SAMHSA which falls under H.H.S. which has an office on 90<sup>th</sup> 7<sup>th</sup> Street, San Francisco. Bitfocus recommendations for agencies to be highly involved with their technology include Emergency Services, Law Enforcement, Public Works, Parks and Recreation but not one file was given to Chris Ward Kline from several agencies listed in this complaint.

#### SURVEILLANCE TECHNOLOGY INVENTORY SAN FRANCISCO

- 1) Reference pages 118-142 which shows that the city uses this technology discussed but claim there is no files, meta data or data on Chris Ward Kline. Kaiser in San Francisco for a period of 6 years have over 600 pages of files but SF doesn't have one page.

#### DEPARTMENT OF EMERGENCY MANAGEMENT

- 1) Reference pages 143-144 – page 143 shows Interoperable Communications – this is where all the files exist in the county, but DEM says no files exist. Page 143 shows breakdown of Public Health, and they oversee Jail Services which links Public Health to the Sheriff. The sheriff also does security and operations control at the DEM, Public Health, Library, and several medical facilities. So these three combined say that the files do not exist, but with this presentation and the technology states, clearly shows that files do exist.
- 2) Reference page 145 – a release statement from the Department of Emergency Management concerning ACS Radio Nets – which are used for Emergency Communications during disasters. Any member of the

Northern California Amateur Radio Group or anyone with a little experience can tell you everything we just discussed in this presentation.

- 3) Reference pages 146-164 shows a Linkedin post concerning this technology followed by emails to local leaders in San Francisco. I also presented this at several meetings to include the San Francisco Tenderloin Station public meeting, which was recorded. Notice HSH 9/2/2022 information concerning agencies using the technology and the one dates 9/13/2022 which DEM and several others agencies asked HSH to remove them from the website, only due to public outcry and complaints, not because they were not using it as suggested.

#### DATA SHARING AND PRIVACY

- 1) Reference page 165

In closing, Oakland Privacy Advocacy Director Tracy Rosenberg commented 'the use of any surveillance technology with impunity is a recipe for disaster'.

Your office, Sunshine Ordinance Task Force in one of these checks and balances and I ask for a favorable ruling asking for a full release and disclosure from all parties and agencies named.

Respectfully,

A handwritten signature in black ink, appearing to read "Chris Ward Kline". To the right of the signature is the date "3/13/2023".

Chris Ward Kline

## Results of the investigation

---

On August 17, 1975 Senator Frank Church appeared on NBC's *Meet the Press*, and discussed the NSA, without mentioning it by name:

In the need to develop a capacity to know what potential enemies are doing, the United States government has perfected a technological capability that enables us to monitor the messages that go through the air. (...) Now, that is necessary and important to the United States as we look abroad at enemies or potential enemies. We must know, at the same time, that capability at any time could be turned around on the American people, and no American would have any privacy left: such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide.

If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology. (...)

I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return. <sup>[25]</sup><sup>[26]</sup>

# Now Hear This

Christopher Helman Forbes Staff

Follow

Sep 15, 2003, 12:00am EDT

 This article is more than 10 years old.

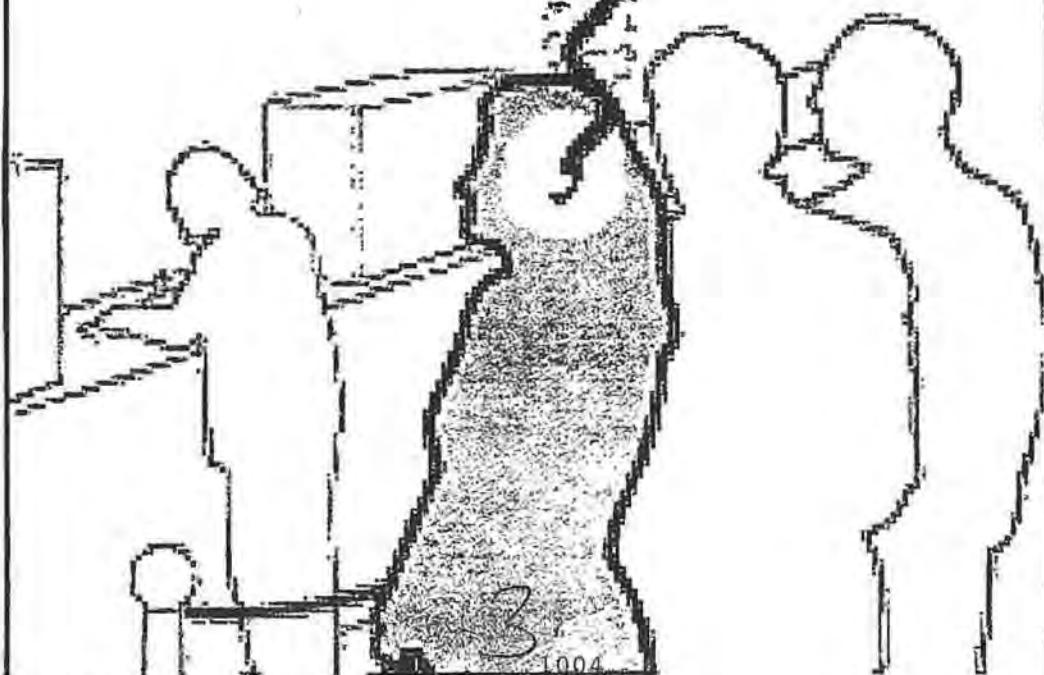
A new ultrasound system can zap a laserlike channel of sound over hundreds of feet to just one pair of ears in a crowd--a perfect pitch for marketers.

Cookie Preferences

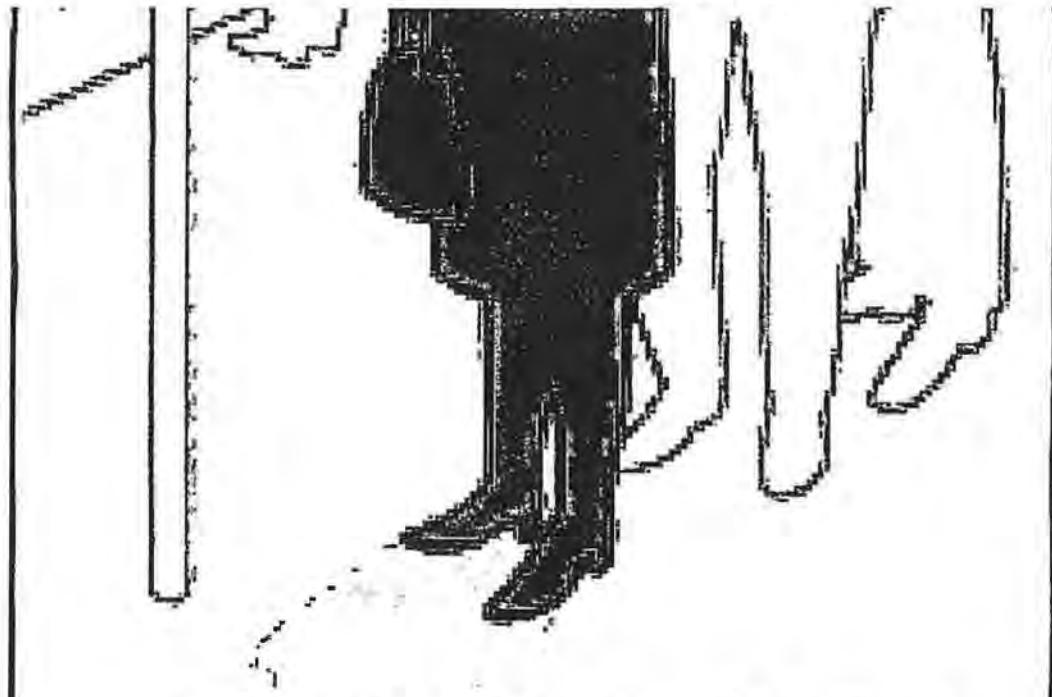
2  
1003

# How HSS Works

**Hyper sonic Sound is an aural laser. By blending ultrasonic waves, it yields a pinpointed audible tone. A woman at the front of a line hears a message no one else can.**



Cookie Preferences



## Steve Blanklawicz For Forbes

1100 units for testing at Wal-Mart and McDonald's. Sony has signed up to distribute the units in Europe. Gateway is considering including the technology in its line of televisions. And General Dynamics is installing them in the public address systems of U.S. Navy ships.

Woody's biggest win--until now, top secret--is the coming deployment of HSS in front of as many as 100 million supermarket shoppers a week. Disney and other big media companies plan to launch the ABC In-Store Network next year. The venture's budget calls for some 5,600 high-end supermarkets across 13 chains to spend \$250 million installing 40,000 plasma TV screens integrated with HSS emitters. The satellite-linked network will show news, previews of ABC shows and Disney movies, and, of course, advertising. Inaudible to anyone not standing in the checkout line, it wouldn't drive cashiers batty or interfere with other store announcements.

Marketers have always dreamed of whispering into the ears of individual shoppers as they mill around the aisles and inch along

checkout lanes. But speaker systems to date have annoyed everyone, employees especially, with their constant, ubiquitous noise pollution. Home uses abound, too. Imagine watching ESPN in bed at 1 a.m. without waking the wife.

Conventional loudspeakers spew a shotgun spray of sound waves in all directions. HSS, by contrast, shoots tightly focused waves of ultrasound (meaning it exceeds the frequency range of human hearing). When its various waves interact with each other, audible sounds emerge. An HSS emitter can transmit a message to a single person standing in a crowd 200 feet away, without anyone on either side being able to hear it. Motion-sensitive HSS emitters can flog Doritos on one end of the snack aisle and hawk Cracker Jack on the other. "HSS will eclipse anything I've invented so far," says Norris.

Tanned, 64 years old and gregarious, the self-taught engineer has made a fortune in four decades of inventing electronic gadgets outside the corporate tent. In 1967 he delivered a "transcutaneous Doppler," a forerunner of sonography. Since then Norris has devised a 20-hour cassette tape, the first palm-size digital voice recorder and an in-the-ear speaker that uses the bones of the skull to transmit sound. Norris sold the rights to that last device for \$5 million a decade ago. GN Netcom now sells \$40 million of them a year under the Jabra name for hands-free phone use.

His inspiration for HSS came in the late 1970s, when he found himself contemplating the characteristics of mixing. "I invent by analogy," he says. "I thought, 'It's commonplace that you can mix colors, smear them together to get new emerging colors. Likewise you can mix radio waves to get new frequencies.' So, I wondered, 'Why can't you mix sound to get new sounds?'"

Norris started on HSS in earnest in 1996. He puzzled out (and only later learned that 19th-century German physicist Hermann Helmholtz had gotten there before him) that when two tones are played simultaneously and loudly enough, they interact to create two new tones. One carries a frequency that is the sum of the two starting frequencies; the other is their difference. So if you blast inaudible ultrasonic frequencies of 100 kilohertz and 101 kilohertz, you get an inaudible 201 kilohertz overtone plus an undertone of 1 kilohertz that is well inside the range of hearing. And since ultrasound travels in a tight line akin to laser light, the emergent tones are audible only in a narrow, cylindrical path from source to ear.

It took seven years and \$45 million in venture capital and personal funds for Norris to solve the myriad distortion problems and figure out how to turn music or soda pop fizzing into ultrasound and back to music (or fizzing) again. Norris also figured out how to achieve his sound effect using only a dinner-plate-thick transducer instead of bulky speaker cones. HSS' transducer is a 28-micron-thick plastic film that flutters when exposed to an electric field (because it is "piezoelectric"). Alternate the charges fast enough and the minute fluttering of the film causes tiny dimples on its surface to push the air at ultrasound frequencies.

Norris and his engineers have tested and patented every method they could think of to make it work. So far American Technology has 17 HSS patents and 24 more pending. The promise of HSS has inspired investors to bid up ATC stock 100% to \$6 this year, giving the company a market cap of \$90 million. This, despite a first-quarter loss of \$1.4 million on \$314,000 in revenue, mostly from military contracts. Yet the stock could still be cheap. Norris, who owns a quarter of the company (and says he won't sell a share until the stock hits \$20), sees an annual sales rate of \$20 million in the

next 12 months. To do that ATC would need to deliver something like 40,000 units at \$500 each.

Norris and Chief Executive James Irish have drummed up hundreds of business leads by crisscrossing the country, shooting cacophonous jungle sounds and sweet symphonies to suits in the boardrooms or out windows into the startled ears of unsuspecting pedestrians. Sales efforts are aided by marketers such as Harbor Digital Services, which makes high-end signage and has introduced HSS to clients like McDonald's and IBM and is working on the supermarket deal with ABC. On seeing a handheld HSS emitter at work, marketers go into "immediate brainstorming mode," says Harbor's Jeffrey Dahlstrom. "The ABC guys carry it around everywhere they go."

Iport Media, which is incorporating HSS into displays for eyeglass stores, expects designers like Calvin Klein will gladly pay \$500 to \$1,000 to install motion-activated HSS for their racks, says Chief Executive Edward Weiner. The sales pitch would never cross the clerk's ears. "The idea is to get them to buy what you want by showing them the difference," says Weiner, who aims to place thousands of systems in two years.

Paul Drouin of IKS Media, who installs sound systems for McDonald's, has persuaded operators in Florida, Oklahoma and Texas to test HSS this summer. In time emitters built into soda fountains could help drive sales in the Golden Arches with a message like, "You know what goes great with Coke? McDonald's french fries."

HSS also is being integrated into consumer electronics, with Gateway exploring the idea of adding HSS to its plasma TVs to create surround-sound effects without the need for back-of-the-room speakers. DaimlerChrysler is <sup>100%</sup> considering putting it in cars so

that riders in the front and back seats can enjoy separate stereo systems. A buyer from Wal-Mart called Norris in July asking whether ATC could develop an HSS speaker to sit on top of a TV and direct sound to one viewer but not another. Norris expects it to hit shelves in a year for around \$200 a pop.

General Dynamics is installing HSS gear on Navy ships, including one over the captain's chair on the bridge of the U.S.S. *Winston S. Churchill*. The speaker cuts through the din to beam messages to the captain's ears only. Even cooler, but scarier, is HSS' amped-up cousin, the Long Range Acoustic Device. A ship seeking to warn off a suspicious dinghy can use the device to loudly hail the vessel from 500 yards away. If it gets closer, sailors can target it with 120 earsplitting decibels of siren sounds that cause spontaneous diarrhea, long-lasting migraines or nausea. Says Norris: "It's cleaner than the 50-caliber solution."



Christopher Helman

Follow

Tracking energy innovators from Houston, Texas. Forbes reporter since 1999.

[Editorial Standards](#)

[Reprints & Permissions](#)

ADVERTISEMENT

Cookie Preferences



PRIVACY TRADEOFF | 2. 4. 19 by DAN ROBITZSKI

# San Francisco Built a System to Track Homeless People

The system can coordinate help for the city's homeless, but requires a lot of personal data.

1010

/ Future Society / Data / Homeless / Privacy



## BIG BROTHER

San Francisco, unsurprisingly, has decided that the solution to the city's homelessness problem is to gather and analyze personal data.

Specifically, a program called ONE System is now gathering data about the approximately 7,500 homeless people in San Francisco so that the city can better coordinate its efforts to get people off the street. It's a program with noble aspirations, but some difficult-to-justify means — homeless participants will need to trade their private, personal data for the chance of receiving aid from the government, according to Bloomberg.

Since August, ONE System has helped around 70 homeless people get off the street, *Bloomberg* reports, and its creators hope it will halve the homeless population by 2022. To do so, the system, which Nevada-based tech startup BitFocus, Inc. developed for the city, collects data from 15 government agencies and also asks homeless participants to fill out a survey that asks about their daily routines, medical history, and other personal information that could be used to help them get appropriate help.

But the new system doesn't exactly erase the hurdles that homeless people already face — to get permanent housing in one of San Francisco's low-cost adult-supportive housing programs, homeless people must pass a background check that takes 45 days to complete and also often need to present a government-issued ID. On top of those systematic hurdles already facing homeless people, government employees will need to convince homeless people to participate in the program, even though some may have debilitating mental illnesses or be skeptical that the system's data won't make its way into the hands of the police.

1012

## UNSUBSCRIBE

So far, the data collected through ONE System has stayed out of law enforcement's hands and no one has tried to buy it, Chris Block, the director of coordinated entry for Episcopal Community Services of San Francisco, an organization contributing to the program, told *Bloomberg*. But there aren't any laws on the books that specifically protect the data the system collects or prevent it from being abused.

"There's a lot of privacy concerns," he said. "So far those issues haven't been significant, but that doesn't mean they won't come up in the future."

**San Diego County CoC Homeless Management Information System (HMIS)**  
**Agency Participation Agreement**

**Postings:** Privacy and Mandatory Collection notices (Appendices D and E) must be posted at the Agency.

- A. The Agency must post Privacy and Mandatory Collection notices at each intake desk or comparable location.
- B. Privacy and Mandatory Collection notices must be made available in writing at the client's request.
- C. If the Agency maintains a website, a link to the privacy notice must be accessible from the Agency's website.

**IV. Data Use**

Data contained in the HMIS will only be used to support the delivery of homeless services in the San Diego region. Each User will affirm the principles of ethical data use and client confidentiality as noted and contained in the HMIS User Agreement.

1. The Agency will not solicit or input information from clients unless it is essential to provide services, or conduct program evaluation.
2. The Agency understands that all client data will be maintained on a central server, which will contain all client information in an encrypted state. All client identifiable data is inaccessible to unauthorized users.
3. The Agency shall use the system to enter and corroborate services but not for location services for past due billing.
4. The Agency shall not be denied access to client data entered by the Agency. Agencies are bound by all restrictions placed upon the data by the client of any Participating Agency. The Agency shall diligently record in the HMIS all restrictions requested.
5. The Agency shall not knowingly enter false or misleading data under any circumstances.
6. The Agency shall maintain appropriate documentation of client consent to participate in the HMIS.
7. If a client withdraws consent for release of information, the Agency remains responsible to ensure that the client's information is unavailable to all other Agencies.
8. The Agency shall keep signed copies of the Multiparty Authorization form for a period of seven (7) years.

**V. Responsibilities**

The Agency is responsible for ensuring that its staff does not intentionally or unintentionally misuse the HMIS. Such misuses include and are not limited to: damage of computing resources, obtaining unauthorized resources, taking resources from another user, gaining unauthorized access to resources, or otherwise using or computing resources without proper authorization.

1. The Agency will maintain an environment free of illegal or malicious acts and the Agency's users agree to never use the system to perform an illegal or malicious act. Any attempt to increase the level of access to which the User is authorized or any attempt to deprive other authorized Users of resources or access to HMIS shall be regarded as a violation of this Agreement that will be addressed as set forth in the HMIS Policies and Procedures.
2. Any User who finds a possible security lapse on the system is obligated to report it to the HMIS System Administrator immediately.
3. The HMIS software application was paid for with U.S. Department of Housing and Urban Development (HUD) grant funds. The maintenance, upgrades and license purchases are limited by the sanctions of the HUD grant.

**VI. System Usage**

Computer Equipment and Services are intended for HMIS-related activities. Acceptable computer system use includes data intake, reports, research of Client, Client development, and public service purposes. Prohibited Usage includes, but is not limited to, the following activities: the sending of fraudulent, threatening, harassing, or obscene messages and/or materials; inappropriate mass mailing (spamming, flooding, bombing); creation or intentional distribution of computer viruses, worms, or Trojan horses; unauthorized access to or denial of service; attempted attacks on any computer system.. Abusers are subject to sanctions as outlined in the HMIS Policies and Procedures.

**VII. Rights**

The HMIS Lead Agency reserves all rights, including access audit, termination of agreements, of the HMIS application and the service resources that it owns and/or operates on behalf of the Continuum of Care. These procedures shall not be construed as a waiver of any rights of the HMIS Lead Agency or the Participating Agency, nor shall they conflict with applicable acts of law.

**VIII. Privileges**

The HMIS services and or equipment are a privilege and are assigned and managed by the HMIS Lead or designee(s). The Agency is responsible for proper use of the system as outlined in Section VI.

**San Diego County CoC Homeless Management Information System (HMIS)  
Agency Participation Agreement**

**IX. Confidentiality**

Although technological and procedural securities have been reasonably exhausted by the HMIS Lead to ensure client data confidentiality, this HMIS is being used by a multitude of end users and is therefore subject to the diligence to which the Participating Agencies' staff protects client records.

The protections that the HMIS put in place to protect client confidentiality include compliance with HUD Data and Technical Standards Final Notice, institution of a mandated HMIS training program for all HMIS users, consistent application of Policies and Procedures, and signed Agency End-User Agreements.

**X. Copyright**

The HMIS is protected by copyright and is not to be copied, except as permitted by law or by contract with owner of the copyright. The number of copies and distribution of copies are to be managed by the HMIS Lead. Interference with measures used by copyright holders to protect copyrighted works is prohibited.

Agency users storing materials copyrighted by others on the systems or displaying the materials through web pages must comply with copyright laws and guidelines.

**XI. Violations**

An individual violating any of the guidelines outlined in this agreement will be reported immediately upon discovery. Such suspected violations will be confidentially reported to the HMIS Lead and or the designee of that agency in accordance with the HMIS Policies and Procedures.

**Agreement**

I have read this HMIS Agency Participation Agreement and thoroughly understand that this technology is for HMIS purposes only and is to be used in accordance with the HMIS Policies and Procedures.

This Agreement is executed between the Participating Agency listed below and the Regional Task Force on Homelessness (RTFH) acting as the San Diego County HMIS Lead Agency and upon execution the Participating Agency will be given access to the HMIS. The Executive Director or Authorized Designees for each Agency will sign this agreement.

---

Participating Agency (Print)

---

Signature - Authorized Representative

---

Name (Print)

---

Date

---

HMIS Lead Agency (Print)

---

Signature - Authorized Representative

---

Name (Print)

---

Date

# Acceptable Uses Policy

LAST UPDATED: October 10, 2022

## Legal Compliance

You must use the Services in compliance with, and only as permitted by, applicable law. The use of our Services in conjunction with other tools or resources in furtherance of any of the unacceptable uses described herein is also prohibited. In the event of any violation of this Acceptable Uses Policy, Momentive may, in its sole discretion, do one or more of the following:

- suspend (temporarily or permanently) or terminate your use of the Services;
- block your access to the Services;
- remove or delete content from your account(s); or
- communicate such violation to impacted third parties and/or law enforcement authorities (where appropriate and subject to applicable law).

## Your Responsibilities

You are responsible for your Content, Customer Data, conduct, and communications with others while using the Services. You must comply with the following requirements when using the Services. If we become aware of Content or Customer Data that falls outside the bounds of what is acceptable under this policy, we may remove it and report it. We also take steps to prevent uses of our Services that are contrary to the spirit of this policy.

(a) You may not use the Services to commit an unlawful activity; use the Services for activities where use or failure of the Services could lead to physical damage, death, mental harm, or personal injury.

14  
1015

- (b) You may not provide any individual under the age of 16 (or under a higher age as provided in certain countries or territories) with access to the Services.
- (c) You may not purchase, use, or access the Services for the purpose of building a competitive product or service or for any other competitive purposes.
- (d) You may not misuse our Services by interfering with their normal operation or attempting to access them using a method other than through the interfaces and instructions that we provide.
- (e) You may not circumvent or attempt to circumvent any limitations that Momentive imposes on your use of our Services or your account(s) (such as by opening up a new account to create or distribute a survey, form, application, or questionnaire that we have closed for a violation of our terms or policies).
- (f) Unless authorized by Momentive in writing, you may not probe, scan, or test the vulnerability or security of the Services or any Momentive system or network.
- (g) Unless authorized by Momentive in writing, you may not use any automated system or software to extract or scrape data from the websites or other interfaces through which we make our Services available.
- (h) You may not deny others access to, or reverse engineer, the Services, or assist anyone else to do so, to the extent such restriction is permitted by law.
- (i) You may not store or transmit any viruses, malware, or other types of malicious software, or links to such software, through the Services.
- (j) You may not use the Services to infringe the intellectual property rights of others.
- (k) Unless authorized by Momentive in writing, you may not resell or lease the Services.
- (l) If your use of the Services requires you to comply with industry-specific regulations applicable to such use, you will be solely responsible for such compliance, unless Momentive has agreed with you in writing otherwise. You may not use the Services in a way that would subject Momentive to those industry-specific regulations without obtaining Momentive's prior written agreement. For example, you may not use the Services to collect, protect, or otherwise handle "protected health information" (as defined in 45 C.F.R. 1516

§160.103 under United States federal regulations) without entering into a separate business associate agreement with Momentive that permits you to do so.

(m) We may offer content like images or video that are provided by third parties. You may use that material solely in your Content or Customer Data. Momentive may modify or revoke that permission at any time in our sole discretion. In using such material, you may not imply that your Content, Customer Data, or use of the Services are affiliated with or run or endorsed by any company, product, brand or service depicted in that material unless you have obtained their permission.

(n) You may not engage in abusive or excessive usage of the Services, which is usage significantly in excess of average usage patterns of reasonable users similar to you, including any usage that adversely affects the speed, responsiveness, stability, availability, or functionality of the Services for other users. Momentive will endeavor to notify you of any abusive or excessive usage to provide you with an opportunity to reduce such usage to a level acceptable to Momentive which no longer causes such adverse effects.

(o) You must use a valid email address to register an account. You may not register accounts using a disposable or temporary email address, "bots," or other unauthorized automated methods.

(p) You may not host or transmit content that is or contains false, inaccurate, or intentionally deceptive information that is likely to cause harm to the public or adversely affect the public interest (including health, safety, election integrity, and civic participation).

(q) If Momentive determines, in its sole discretion, that your usage of the Services causes damage to our brand or reputation, or results in an excessive volume of complaints, Momentive, has the right to suspend or terminate your use of our websites and the Services.

## Phishing and Security

We strive to protect the security of all our users. We take specific measures to ensure respondents are not misled by surveys/forms/applications/questionnaires used for fraudulent or malicious purposes. We will suspend any use of the Services or remove any Content or Customer Data which comes to our attention that:

1/17

- attempts to collect, as determined in our sole discretion, social security numbers or similar government-issued identification numbers, credit card numbers (other than solely for collecting payment through an authorized payment processor as permitted by the Services), passwords, or other similar types of sensitive information;
- publishes a person's identifying information without their consent;
- is intended to deceive or mislead respondents, including by linking to websites with malicious software such as malware;
- promotes or recruits for pyramid schemes, multi-level marketing campaigns, or work-from-home and other false earning scams;
- knowingly and artificially boosts or inflates a website or webpage's search engine ranking or reputation, including by offering or selling social media "likes", followers, reviews, comments, or similar services; or
- hosts content that is downloadable, live-streamed, or merely intended to solicit clicks to other sites.

## Privacy and Impersonation

Users provide responses and information with the expectation that their information will be handled respectfully and not abused. Accordingly, you are responsible for complying with all applicable data protection laws and regulations with respect to any data that you submit to or collect through our Services.

- We encourage you to disclose your privacy practices when you use the Services and, if you do, we require you to act in accordance with those practices.
- You may not claim that a survey/form/application/questionnaire or other use of our Services is anonymous when it is not.
- You may not impersonate others when using the Services or collecting information.

## Email and Text Message Requirements

Momentive has a zero-tolerance spam policy. This means the following:

- Emails or text messages you send via the Services must include a valid survey/form/application/questionnaire for the purpose of collecting responses

(excluding certain automated messages such as “thank you” emails, as applicable).

- Emails you send via the Services must have a valid reply-to email address owned or managed by you. You may not use a “no reply” address as the sender email address.
- Text messages you send via the Services should include your company name.
- You can only use the Services to send emails and text messages to people that have opted in to, or otherwise validly consented to, receiving communications from you, the sender through that medium. If you don’t have proof that each recipient opted in for your emails or text messages (as applicable), don’t import them into any lists in the Services. We prohibit the use of harvested mailing lists.
- We prohibit the use of third-party, purchased, or rented mailing lists unless you are able to provide proof that individuals on the list have opted-in to receiving emails of the type you will be sending them.
- You must not send unsolicited email to newsgroups, message boards, distribution lists, or email addresses.
- You must not utilize the Services to send any email or text messages in a way not permitted by or compliant with applicable law, carrier compliance requirements or industry standards, or to any recipient who has opted out, unsubscribed, or otherwise objected to receiving such messages from you or another party on whose behalf you may be commissioned.
- You must not use the Services to send emails with deceptive subject lines or false or misleading header information.
- Email messages sent in connection with our Services must contain an “unsubscribe” link that allows subscribers to remove themselves from your email messages. You acknowledge and agree that you will not hide, disable, or remove or attempt to hide, disable, or remove the opt-out link from the email invitation. You will actively manage and process unsubscribe requests received by you directly within ten days of submission and update your email lists and address books to reflect the unsubscribe requests.
- You are responsible for ensuring that the email messages or text messages you send in connection with your surveys/forms/applications/questionnaires or any use of our Services do not generate a number of spam complaints or bounce rates in excess of industry standards. If Momentive determines that your level of spam complaints or bounce rate is higher than industry standards,

Momentive, at its sole discretion, has the right to suspend or terminate your use of our Services and websites. If you receive low response rates, high abuse rates or high bounce rates, or we receive complaints associated with your use of our Services, we may request additional information regarding your mailing lists to investigate and attempt to resolve the problem, or in some cases we may suspend or remove your email privileges.

- Text message invitations you send via our Services must have a valid reply “Stop”.
- You may not use Momentive’s text messaging services to access or allow access to emergency services.

If we believe you are violating any of these prohibitions, we may suspend (temporarily or permanently) or terminate your account(s).

## Violence and Hate Speech

We remove Content or Customer Data and may report information related to that Content or Customer Data to law enforcement authorities if we become aware of, or believe that, a genuine risk of harm or threat to public safety exists.

- Our Services may not be used to directly or indirectly threaten or attack others, or to organize or incite violence, harassment, terrorism, or property damage.
- Our Services may not be used for hate speech, or to promote or fund such acts. Examples of hate speech include attacking or advocating for the abuse or exclusion of people based on their ethnicity, national origin, political or religious affiliations, gender, age, sexual orientation, genetic predisposition, disability, medical or physical condition, veteran status, or any other protected classes under applicable law.
- Our Services may not be used to promote, incite, or glorify self-harm or acts of terrorism.

## Bullying, Harassment, and Criminal Activity

You may not use our Services to bully or harass others, in furtherance of any criminal activity, or in violation of any applicable law.

19  
2020

## Pornography and Offensive Graphic Material

We acknowledge nudity, pornography and gore may have a legitimate place in certain uses of our Services. However, we discourage the gratuitous inclusion of such materials.

- You may not include gratuitous graphic violent material or pornography in connection with the use of our Services.
- We recommend adding a conspicuous warning screen before displaying any material which may be offensive in nature.
- You may not under any circumstances share, transmit, upload, or store materials that constitute any of the following: unlawful pornography; material that shows a child engaging in or depicted as engaging in sexually explicit activity, for example, child sexually exploitative material (including material which may not be illegal child sexual abuse material but which nonetheless sexually exploits or promotes the sexual exploitation of minors); or materials that are otherwise indecent.

## Intellectual Property Infringement

Please respect the intellectual property rights of others. You must have the appropriate rights to use any Content or Customer Data. It is your responsibility to determine what rights you need, to obtain and maintain those rights, and to understand how you are permitted to exercise those rights. You may include Content, including any third-party logos, brands and other indicia of source, (a) to the extent permitted as a fair use or otherwise under applicable law, and (b) so long as the use does not (i) cause confusion as to the origin or sponsorship of a good or service, (ii) imply sponsorship or endorsement by the trademark owner where none exists, or (iii) inaccurately describe a product or service. We recommend that you seek independent legal counsel if you have questions about your use of content or intellectual property owned by a third party.

## How to Report Policy Violations

20  
2021

If you suspect that someone's use of our Services is in violation of this policy, please contact us immediately by filing an abuse report

(<https://smforms.wufoo.com/forms/r1vlkf520jsvo8o/>) and we will investigate the matter. Please include the URL of the survey/form/application/questionnaire or other content at issue.

**Community:** (<https://www.facebook.com/surveymonkey/>)

Developers ([https://developer.surveymonkey.com/?ut\\_source=legal&ut\\_source2=acceptable-uses-policy](https://developer.surveymonkey.com/?ut_source=legal&ut_source2=acceptable-uses-policy)) •

Facebook (<https://www.facebook.com/surveymonkey/>) • Twitter (<https://twitter.com/Surveymonkey>) •

LinkedIn (<https://www.linkedin.com/company/surveymonkey/>) •

Our Blog (<https://www.surveymonkey.com/curiosity/>) • Instagram (<https://www.instagram.com/surveymonkey/>) •

Youtube (<https://www.youtube.com/surveymonkey>)

**About Us:** ([https://www.momentive.ai/en/about/?utm\\_source=surveymonkeyfooter](https://www.momentive.ai/en/about/?utm_source=surveymonkeyfooter))

Leadership Team ([https://www.momentive.ai/en/about/leadership/?utm\\_source=surveymonkeyfooter](https://www.momentive.ai/en/about/leadership/?utm_source=surveymonkeyfooter)) •

Board of Directors ([https://www.momentive.ai/en/about/directors/?utm\\_source=surveymonkeyfooter](https://www.momentive.ai/en/about/directors/?utm_source=surveymonkeyfooter)) •

Investor Relations ([https://investor.momentive.ai/home/default.aspx?utm\\_source=surveymonkeyfooter](https://investor.momentive.ai/home/default.aspx?utm_source=surveymonkeyfooter)) •

App Directory ([https://www.surveymonkey.com/apps/?ut\\_source=legal&ut\\_source2=acceptable-uses-policy](https://www.surveymonkey.com/apps/?ut_source=legal&ut_source2=acceptable-uses-policy)) •

Newsroom (<https://www.momentive.ai/en/newsroom/>) •

Office Locations (<https://www.surveymonkey.com/mp/aboutus/office-locations/>) •

Imprint (<https://www.surveymonkey.com/mp/imprint/>) • Careers (<https://www.momentive.ai/en/careers/>) •

Sitemap (<https://www.surveymonkey.com/mp/sitemap/>) • Help (<https://help.surveymonkey.com/en/>) •

Log In (<https://www.surveymonkey.com/mp/sign-in/>) • Sign Up (<https://www.surveymonkey.com/mp/sign-up/>)

**Policies:** (<https://www.surveymonkey.com/mp/legal/>)

Terms of Use (<https://www.surveymonkey.com/mp/legal/terms-of-use/>) •

Privacy Notice (<https://www.surveymonkey.com/mp/legal/privacy/>) •

California Privacy Notice (<https://www.surveymonkey.com/mp/legal/region-specific-privacy-statement/>) •

Acceptable Uses Policy (<https://www.surveymonkey.com/mp/legal/acceptable-uses-policy/>) •

Security Statement (<https://www.surveymonkey.com/mp/legal/security/>) •

GDPR Compliance (<https://www.surveymonkey.com/mp/privacy/>) •

Email Opt-In ([https://www.surveymonkey.com/user/email-opt-in/?ut\\_source=legal&ut\\_source2=acceptable-uses-policy](https://www.surveymonkey.com/user/email-opt-in/?ut_source=legal&ut_source2=acceptable-uses-policy))

Accessibility (<https://help.surveymonkey.com/en/create/accessibility/>) •

Cookies Notice (<https://www.surveymonkey.com/mp/legal/cookies/>)

21/22

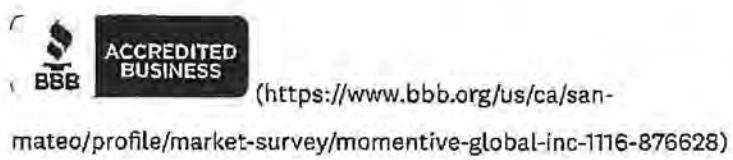
- Margin of Error Calculator (<https://www.surveymonkey.com/mp/margin-of-error-calculator/>) •
- Questionnaire (<https://www.surveymonkey.com/mp/online-questionnaires/>) •
- Demographic Questions (<https://www.surveymonkey.com/mp/gathering-demographic-information-from-surveys/>) •
- Training Survey (<https://www.surveymonkey.com/mp/training-survey/>) •
- Offline Survey (<https://www.surveymonkey.com/mp/offline-surveys/>) •
- 360 Review Template (<https://www.surveymonkey.com/templates/360-degree-employee-evaluation-survey-template/>)

---

English

SurveyMonkey is brought to you by momentive.ai ([https://www.momentive.ai/en/?utm\\_source=surveymonkeyfooter](https://www.momentive.ai/en/?utm_source=surveymonkeyfooter)). Shape what's next with AI-driven insights and experience management solutions built for the pace of modern business.

Copyright © 1999-2023 Momentive



23  
1028

**Use Cases:** ([https://www.surveymonkey.com/?ut\\_source=legal&ut\\_source2=acceptable-uses-policy](https://www.surveymonkey.com/?ut_source=legal&ut_source2=acceptable-uses-policy)) •

Online Polls (<https://www.surveymonkey.com/mp/online-polls/>) •

Facebook Surveys (<https://www.surveymonkey.com/mp/facebook/>) •

Survey Template (<https://www.surveymonkey.com/mp/survey-templates/>) •

Scheduling Polls (<https://www.surveymonkey.com/mp/online-schedule-poll/>) •

Google Forms vs. SurveyMonkey (<https://www.surveymonkey.com/mp/surveymonkey-better-than-google-forms/>) •

Employee Satisfaction Surveys (<https://www.surveymonkey.com/mp/employee-satisfaction-surveys/>) •

Free Survey Templates (<https://www.surveymonkey.com/mp/free-survey-templates/>) •

Mobile Surveys (<https://www.surveymonkey.com/mp/mobile-surveys/>) •

How to Improve Customer Service (<https://www.surveymonkey.com/mp/6-keys-improving-teams-customer-service-skills/>) •

AB Test Significance Calculator (<https://www.surveymonkey.com/mp/ab-testing-significance-calculator/>) •

NPS Calculator (<https://www.surveymonkey.com/mp/nps-calculator/>) •

Questionnaire Templates (<https://www.surveymonkey.com/mp/sample-survey-questionnaire-templates/>) •

Event Survey (<https://www.surveymonkey.com/mp/post-event-survey-questions/>)

Sample Size Calculator (<https://www.surveymonkey.com/mp/sample-size-calculator/>) •

Writing Good Surveys (<https://www.surveymonkey.com/mp/writing-survey-questions/>) •

Likert Scale (<https://www.surveymonkey.com/mp/likert-scale/>) •

Survey Analysis (<https://www.surveymonkey.com/mp/how-to-analyze-survey-data/>) •

360 Degree Feedback (<https://www.surveymonkey.com/mp/360-employee-feedback-survey-example/>) •

Education Surveys (<https://www.surveymonkey.com/mp/education-surveys/>) •

Survey Questions (<https://www.surveymonkey.com/mp/survey-question-types/>) •

NPS Calculation (<https://www.surveymonkey.com/mp/net-promoter-score-calculation/>) •

Customer Satisfaction Survey Questions (<https://www.surveymonkey.com/mp/customer-satisfaction-survey-questions/>) •

Agree Disagree Questions (<https://www.surveymonkey.com/mp/2-tips-for-writing-agree-disagree-survey-questions/>) •

Create a Survey (<https://www.surveymonkey.com/mp/how-to-create-surveys/>)

Online Quizzes (<https://www.surveymonkey.com/mp/quiz/>) •

Qualitative vs Quantitative Research (<https://www.surveymonkey.com/mp/quantitative-vs-qualitative-research/>) •

Customer Survey (<https://www.surveymonkey.com/mp/customer-satisfaction-surveys/>) •

Market Research Surveys (<https://www.surveymonkey.com/mp/market-research-surveys/>) •

NPS Survey (<https://www.surveymonkey.com/mp/net-promoter-score/>) •

Survey Design Best Practices (<https://www.surveymonkey.com/mp/survey-guidelines/>) •

2024

# Woody Norris

## HyperSonic Sound

COMPUTING AND TELECOMMUNICATIONS

Elwood "Woody" Norris proves that there is no magic formula for becoming a successful inventor. Born in October 23, 1939 in Barrelville, Maryland, his mother and father had eighth-grade and third-grade educations, respectively, and Norris's formal training stopped with high school.

Nonetheless, his aptitude for electronics and entrepreneurship and his enthusiasm for creating new technologies has taken him to the top of his game. He has garnered over 100 patents and has created a variety of successful inventions to his credit in fields as diverse as sound technology, transportation, and medicine.

Norris learned about electronics by tinkering with radios in his youth and discovered a natural ability to understand how circuitry worked. He joined the Air Force, where he received some training in radar and electronics while working on triggers for bombs. He took a job at a nearby television station as a cameraman to supplement his military income and thought that he might pursue acting after his military service was complete. As a high school student, he had enjoyed participating in school productions and possessed some talent as a performer.

Instead, when Norris left the Air Force as Airman Second Class, he took a job at the University of Washington fixing electronic equipment. Within two years, he was named director of the campus' Engineering Experiment Station. When a local company approached him, he took on the task of developing a sonar version of radar to listen to sounds inside the body. This "Doppler" tool emitted ultrasonic sound into the skin. Changes in the pitch of the sound waves that bounced back allowed physicians to

1025

<https://lemelson.mit.edu/resources/Woody-norris#:~:text=Norris%20is%20perhaps%20best-known,one%20who%20can%20hear%20it.>



"hear" movement inside the patient. The tool, licensed to Medical Development Corporation (which was later acquired by American Hospitals), was helpful to the development of the Sonogram, and, as Norris received company stock for the device, it also helped him make enough money to set up his own company.

Norris later sold a phonographic tone arm he had been working on and evolved a specialization in audio-related devices. His subsequent inventions included headsets for mobile phones, a hearing-aid-sized FM radio, and automobile audio systems. He also created a child locator device for tracking kidnapped children, an alarm worn by a person to alert him that his artificial hip is starting to separate, and a design for a vehicle dubbed the AirScooter®, an easy-to-fly, lightweight, inexpensive aircraft that has the ability to hover in one spot while a pilot gets his bearings. Norris has worked with NASA engineers to develop a prototype of the AirScooter, which he dreams will one day be viable as a commuter vehicle.

Norris is perhaps best-known for his work on what is known as HyperSonic Sound technology (HSS). HSS or directional sound targets a listener with sound waves similar to the way a laser beam directs light, so that the individual who is targeted is the only one who can hear it. As a result, different people in one room could feasibly listen to different music, watch totally different television shows or movies, or hear different advertising messages without the use of headphones.

In conjunction with American Technology Corp. (now Genasys Inc.), Norris worked on HSS and other audio technologies, including a compact sub-woofer and "sonic bullets," which emit intense beams of sound at targeted individuals who pose a threat to others, giving them painful migraines.

Norris has been honored with numerous awards for his work including Product of the Year awards from *Popular Science* and *Business Week*, and the 1997 Award for Technological Innovation in the sound category from *Discover Magazine*. He won the prestigious \$500,000 Lemelson-MIT Prize in 2005 for his HSS technology.

Norris founded and served as Director and President of Parametric Sound Corporation, now known as Turtle Beach Corporation, and also served as Chief Scientist at Turtle Beach. He also founded LRAD Corporation and was the Chairman of LRAD Corporation's Board of Directors until 2010.

Most recently, Norris has been working on the BolaWrap, a handheld, non-lethal restraining device, currently being used by hundreds of law enforcement agencies. The small device works like a lasso, designed to detain people without causing severe injury. Norris expects to offer a range of new product solutions to "help meet the challenges of modern policing."

Norris currently serves as Chief Technology Officer for Wrap Technologies Inc.

**DON'T MISS OUR NEXT NEWSLETTER!**

[SIGN UP](#)

222 Third Street, Suite 0300 Cambridge, MA 02142  
[info-lemelson@mit.edu](mailto:info-lemelson@mit.edu) • 617-253-3352

---

© Massachusetts Institute of Technology

[Privacy](#) | [Accessibility](#) | [Login](#)

26  
1027

WIKIPEDIA

# Woody Norris

**Elwood Adrian "Woody" Norris** (June 18, 1919 – April 25, 2007) was an American professional basketball player.<sup>[1]</sup> He played for the Indianapolis Kautskys in the National Basketball League during the 1941–42 season, served in the United States Army Air Forces during World War II, then continued his basketball career with the Kautskys between 1945 and 1948.<sup>[1][2][3]</sup> In college he played basketball and football for Butler University.<sup>[2]</sup>

## References

1. "Elwood Norris NBL stats" (<https://www.basketball-reference.com/nbl/players/n/norriel01n.html>). *basketball-reference.com*. Sports Reference LLC. Retrieved May 5, 2019.
2. "Woody Norris" (<http://peachbasketsociety.blogspot.com/2015/12/woody-norris.html>). *Peach Basket Society*. December 9, 2015. Retrieved May 5, 2019.
3. "Elwood Norris Statistics" ([https://www.justsportsstats.com/basketballstatsindex.php?player\\_id=norriwo01](https://www.justsportsstats.com/basketballstatsindex.php?player_id=norriwo01)). *Just Sports Stats*. Retrieved May 5, 2019.

Woody Norris	
Personal information	
Born	June 18, 1919 Washington, Indiana
Died	April 25, 2007 (aged 87) Bloomington, Indiana
Nationality	American
Listed height	6 ft 1 in (1.85 m)
Listed weight	170 lb (77 kg)
Career information	
High school	Washington (Washington, Indiana)
College	Butler (1938–1941)
Position	Forward / Guard
Career history	
1941–1942	Indianapolis Kautskys
1945–1948	

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Woody\\_Norris&oldid=1081063478](https://en.wikipedia.org/w/index.php?title=Woody_Norris&oldid=1081063478)"

This page was last edited on 5 April 2022, at 03:03 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

## WIKIPEDIA

# Hermann von Helmholtz

**Hermann Ludwig Ferdinand von Helmholtz**<sup>[a]</sup> (31 August 1821 – 8 September 1894) was a German physicist and physician who made significant contributions in several scientific fields, particularly hydrodynamic stability.<sup>[5]</sup> The Helmholtz Association, the largest German association of research institutions, is named in his honor.<sup>[6]</sup>

In the fields of physiology and psychology, Helmholtz is known for his mathematics concerning the eye, theories of vision, ideas on the visual perception of space, color vision research, the sensation of tone, perceptions of sound, and empiricism in the physiology of perception. In physics, he is known for his theories on the conservation of energy, work in electrodynamics, chemical thermodynamics, and on a mechanical foundation of thermodynamics. As a philosopher, he is known for his philosophy of science, ideas on the relation between the laws of perception and the laws of nature, the science of aesthetics, and ideas on the civilizing power of science.

## Contents

### Biography

Early yearsUniversity posts

### Research

MechanicsSensory physiologyOphthalmic opticsNerve physiologyAcoustics and aestheticsElectromagnetism

### Philosophy

### Quotations

### Students and associates

### Honours and legacy

### Works

## Hermann von Helmholtz



<b>Born</b>	Hermann Ludwig Ferdinand Helmholtz 31 August 1821 Potsdam, Province of Brandenburg, Prussia
<b>Died</b>	8 September 1894 (aged 73) Charlottenburg, Province of Brandenburg, Kingdom of Prussia, German Empire
<b>Education</b>	Medizinisch-chirurgisches Friedrich-Wilhelm-Institut (M.D., 1842)
<b>Known for</b>	Studies in the <u>conservation of energy</u> <u>Helmholtz coil</u> <u>Helmholtz condition</u> <u>Helmholtz decomposition</u> <u>Helmholtz equation</u> <u>Helmholtz free energy</u> <u>Helmholtz free entropy</u> <u>Helmholtz layer</u>

WIKIPEDIA

# Genasys

**Genasys Inc.** is based in San Diego, California. Its long-range acoustic device (LRAD) products are used for long-range acoustic hailing and mass notification. The company was previously named **American Technology Corporation** (ATC) until 2010<sup>[1]</sup> and as **LRAD Corporation** until 2019.<sup>[2]</sup> The company's stock trades on the NASDAQ Capital Market with the ticker symbol "GNSS".<sup>[2]</sup>

Contents	
<a href="#">History</a>	
<a href="#">Products</a>	
<a href="#">References</a>	
<a href="#">External links</a>	

## History

Genasys was founded in Utah by Elwood "Woody" Norris as the American Technology Corporation in 1980.<sup>[3]</sup> From 1988 to early 1992 the company was inactive. Norris recapitalized the company as a Delaware Corporation in 1992.<sup>[4]</sup> In 1996, the company launched its first directed sound technology and began engineering sound solutions for the commercial, government, and military markets. In response to the October 2000 attack on the USS Cole, the company's engineering team developed their long-range acoustic device (LRAD) product line. With the introduction of LRAD systems in 2003, the company created the acoustic hailing device (AHD) market, followed by the introduction of multidirectional mass notifications systems in 2012. The

## Genasys Inc.

Type	Public
Traded as	Nasdaq: <u>GNSS</u> ( <a href="https://www.nasdaq.com/symbol/gnss">https://www.nasdaq.com/symbol/gnss</a> )
Industry	Technology/Manufacturing
Founded	1980 in <u>Utah, U.S.</u>
Founder	Elwood Norris
Headquarters	<u>San Diego, California, U.S.</u>
Area served	Worldwide
Key people	Richard S. Danforth ( <u>CEO</u> ) Dennis Klahn ( <u>CFO</u> ) General John G. Coburn (Ret.) (Chairman)
Products	<u>Long Range Acoustic Device</u> LRAD-RX LRAD 1000Xi LRAD 1000RXL LRAD 100X LRAD 500X LRAD 300X LRAD 450XLi LRAD 100X
Website	<a href="https://genasys.com">genasys.com</a> ( <a href="https://genasys.com/">https://genasys.com/</a> )

company acquired Genasys, a Spanish company based in Madrid and provider of location-based mass messaging solutions for emergency warning and workforce management in January 2018, and subsequently adopted the name Genasys for itself.<sup>[2]</sup>

## Products

---

- Long-range acoustic device (LRAD), which is a high-intensity directional acoustic array designed for long-range communication and mass notification.<sup>[5]</sup>

## References

---

1. "LRAD CORPORATION" (<http://listofcompanies.co.in/2012/02/08/lrad-corporation/>).
2. LRAD Corp. (October 25, 2019). "LRAD Corporation Rebranding as Genasys Inc. to Reflect Broader Commitment to Critical Communications" (<https://www.globenewswire.com/news-release/2019/10/23/1933797/0/en/LRAD-Corporation-Rebranding-as-Genasys-Inc-to-Reflect-Broader-Commitment-to-Critical-Communications.html>). *GlobeNewswire News Room*. Retrieved November 5, 2019.
3. "Utah Business Search - Utah.gov" (<https://secure.utah.gov/bes/>). *secure.utah.gov*.
4. "EDGAR Filing Documents for 0000936392-96-000513" (<https://www.sec.gov/Archives/edgar/data/924383/0000936392-96-000513-index.html>). *www.sec.gov*.
5. "American Technology Ships \$1.5 Million in LRAD Orders" ([http://www.freshnews.com/news/defense-west/article\\_37263.html](http://www.freshnews.com/news/defense-west/article_37263.html)). *FreshNews.com*. Retrieved 2007-04-06.

## External links

---

- Official website (<http://www.lradx.com/>) 
- Investor information on Yahoo! Finance (<https://finance.yahoo.com/q?s=lrad&ql=1>)
- SEC Filings (<https://www.sec.gov/cgi-bin/browse-edgar?company=LRAD&owner=exclude&action=getcompany>)

---

Retrieved from "<https://en.wikipedia.org/w/index.php?title=Genasys&oldid=1127892767>"

---

This page was last edited on 17 December 2022, at 06:54 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

1031  


[Sign in](#)

M

POPULAR  
MECHANICS

## Scientists Can Now Use WiFi to See Through People's Walls

**Tim Newcomb**

Thu, January 19, 2023 at 1:11 PM PST



WiFi Signals Can See People Through WallsCarnegie Mellon University

- Researchers at Carnegie Mellon University can map human bodies through walls using WiFi signals.
- The technology tracks key points on the body for detection, extending previous research into using WiFi signals to locate humans.
- The study's authors position the breakthrough as helpful to privacy, even if it opens the possibilities for much easier, cheaper human tracking.

It isn't immediately clear how using only a WiFi signal to track human movement through walls *improves* personal privacy ... but that's what a new study from Carnegie Mellon University claims.

In a recently published paper, the researchers expanded on the study of employing WiFi signals to

on

Get the Complete Connectivity solution.

[GET IT NOW](#)

(855) 335-7919

X

[Make Yahoo Your Homepage](#)

Discover something new every day from News, Sports, and more.

1032

<https://www.yahoo.com/finance/news/scientists-now-wifi-see-peoples-211100294.html>

30

1/6



*"We developed a deep neural network that maps the phase and amplitude of WiFi signals to UV coordinates within 24 human regions. The results of the study reveal that our model can estimate the dense pose of multiple subjects, with comparable performance to image-based approaches, by utilizing WiFi signals as the only input."*

This pathway opens the options for low-cost, broadly accessible human tracking through walls.

High-cost technology has successfully mapped people's movements through walls for years. And researchers at the Massachusetts Institute of Technology have spent over a decade working on ways to more easily see people through walls, whether using cell phone signals or WiFi. In the Carnegie Mellon study, scientists had WiFi signals send and receive a body's coordinates and then used DensePose to map the body.

From the study:

*"Advances in computer vision and machine learning techniques have led to significant development in 2D and 3D human pose estimation from RGB cameras, LiDAR, and radars. However, human pose estimation from images is adversely affected by occlusion and lighting, which are common in many scenarios of interest."*

By reducing the need for the advanced—and expensive—technology, the Carnegie Mellon researchers say they can make human tracking more available. Somehow, they've also positioned the breakthrough as a privacy-positive situation. You

# Privacy Statement

As a Human Services data company, we take privacy particularly seriously at Bitfocus.

This privacy policy explains what personal information we collect from you, how we use, and for what reasons we may share it. This statement applies only to our public website and other Bitfocus services displaying it. Other services may include specific statements that provide additional limits and safeguards applicable to those particular Bitfocus services and customers.

## What We Collect

We collect information to provide you with the best experience with our services. Depending on which services you use, we collect different kinds of personal information. We also may receive information from third parties.

### Information you Provide

Primarily, we collect information you send us. For example, when you register for an event, sign up for our mailing list, or submit a question on our website we collect the information you submit in order to process those requests. We also collect messages you send us. Conversations with our representatives—including phone calls, emails and chat sessions—may be monitored and recorded.

We also collect information about how you use and interact with our services. This includes information about the device you used, your connection, and details of how you used our services.

### Information from Third-Parties

We may also receive a limited amount of information about you from third parties. For example, we may use demographic or location information provided by third parties to better understand how our services are being used.

## How We Use It

We use the information we collect for two general purposes: (1) to maintain, protect, and improve our services; and (2) to provide you with tailored content and communications.

We use collected information to better understand how our services are being used, to support and protect them, and to continue to improve and refine them.

Collected information is also used to improve our communications with you. For example, we record your past conversations with representatives to improve our ability to respond efficiently. We may also contact you with information about our services, including changes and improvements. We respect your choices about what communications you like to receive.

1034  
32

## When We Share It

[SCHEDULE A DEMO](#)

We only share your personal data with your consent or as necessary to provide any service you have requested or authorized, with a limited number of trusted business partners to process it on our behalf and in compliance with this privacy statement.

### With Consent

We may share personal information with outside parties when we have your consent to do so.

### Legal Reasons

We also may share information to third parties for legal reasons. We will share information when required by law or legal process, or as necessary to protect the safety, rights, or property of Bitfocus and our users.

## Cookies

We use cookies, web beacons, and similar technology to improve your experience and report visitor interactions. Cookies are small text files placed on your device that allow us to identify you when you visit our website and online services. Most browsers include a variety of tools to manage cookies, including alerting you when cookies are sent or blocking them entirely. However, these and other choices may impact your experience with our services.

## California Privacy Notice

Do Not Track (DNT) is an effort to develop a way for internet users to control the tracking of their online activities. Although the World Wide Web Consortium (W3C) is working to develop a DNT technology standard, none has been adopted. Bitfocus, therefore, does not use DNT signals.

Bitfocus does not authorize the collection of Personal Identifiable Information (PII) from our users for third party use through advertising technologies without separate user consent.

## How to Contact Us with Questions

Contact us at [support@bitfocus.com](mailto:support@bitfocus.com) with any questions, concerns or comments about this statement or our privacy program at Bitfocus. Click [here](#) to submit a whistleblower claim.

### Recent Blog Posts



New Outreach Tools to Transform Your Unsheltered Homelessness Care



Optimizing Client & Staff Care While Short Staffed



SOC2 Series: Why Data Security Is Crucial for HMIS Comparable Databases



(800)-594-9854

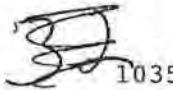
Sign up for our email updates.  
Email Address\*

Bitfocus is a leading system administration and software development firm offering superior value-priced services for Human Services data systems. Our user friendly technology and seasoned public policy professionals form a unique blend that delivers the best possible technological solutions for your community.

**Customer Support:**  
[support@bitfocus.com](mailto:support@bitfocus.com)

**Subscribe**

**General Inquiries:**  
[info@bitfocus.com](mailto:info@bitfocus.com)

 33  
1035



## Universal Licensing System

[FCC](#) > [WTB](#) > [ULS](#) > [Online Systems](#) > [License Search](#)
[FCC Site Map](#)

ULS License

### Trunked Public Safety 700 MHz License - WQMR423 - San Francisco, City and County of

[? HELP](#)
[New Search](#) [Printable Page](#) [Reference Copy](#) [Map License](#)
[MAIN](#) [ADMIN](#) [LOCATIONS](#) [FREQUENCIES](#) [MAP](#)

Call Sign	WQMR423	Radio Service	SY - Trunked Public Safety 700 MHz
Status	Active	Auth Type	Regular
<b>Dates</b>			
Grant	08/04/2020	Expiration	10/28/2030
Effective	08/04/2020	Cancellation	
<b>Control Points</b>			
1	SFIA COMMUNICATIONS DEPT SAN FRANCISCO, SAN MATEO, SAN FRANCISCO, CA P: (650)821-3644		

**Licensee**

FRN	0001540731 ( <a href="#">View Ownership Filing</a> )	Type	Governmental Entity
-----	---	------	---------------------

**Licensee**

San Francisco, City and County of 200 PAUL AVE SAN FRANCISCO, CA 94124-3100 ATTN SHOME VASUDEVAN SYSTEM ADMIN	P:(415)928-9559 F:(415)467-7004 E: <a href="mailto:dt.licenses.fcc@sfgov.org">dt.licenses.fcc@sfgov.org</a>
--	---

**Contact**

San Francisco, City and County of Shome K Vasudevan 200 PAUL AVE, BUILDING B SAN FRANCISCO, CA 94124 ATTN Shome Vasudevan	P:(415)928-9559 E: <a href="mailto:shome.vasudevan@sfgov.org">shome.vasudevan@sfgov.org</a>
---	--

**Land Mobile Data**

Extended Implementation (Slow Growth)	No	Assoc. Call Signs
--	----	-------------------

**Eligibility**

90.523(A) - GOVERNMENT AGENCIES SAN FRANCISCO INTERNATIONAL AIRPORT PUBLIC SAFETY RADIO SYSTEM

34

**Ownership and Qualifications**

1036

**Radio Service Type** Mobile

**Regulatory Status** Private Comm      **Interconnected** No

**Alien Ownership**

The Applicant answered "No" to each of the Alien Ownership questions.

**Basic Qualifications**

The Applicant answered "No" to each of the Basic Qualification questions.

**Demographics**

Race

Ethnicity

Gender

**ULS Help**

[ULS Glossary](#) - [FAQ](#) - [Online Help](#) - [Technical Support](#) - [Licensing Support](#)

**ULS Online Systems**

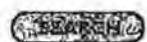
[CORES](#) - [ULS Online Filing](#) - [License Search](#) - [Application Search](#) - [Archive License Search](#)

**About ULS**

[Privacy Statement](#) - [About ULS](#) - [ULS Home](#)

**Basic Search**

By Call Sign     



[FCC](#) | [Wireless](#) | [ULS](#) | [CORES](#)

[Help](#) | [Tech Support](#)

Federal Communications Commission  
45 L Street NE  
Washington, DC 20554

Phone: 1-877-480-3201  
TTY: 1-717-338-2824  
[Submit Help Request](#)

35  
1037

(6) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis; and

(7) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about its effectiveness and any known adverse information about the technology such as unanticipated costs, failures, or civil rights and civil liberties abuses.

"Personal communication device" means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

"Protected Class" means a class of persons with shared characteristics based on sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, gender identity, gender expression, or sexual orientation, or any other class protected under the California Unruh Civil Rights Act.

"Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group. Surveillance Technology<sup>1</sup> includes but is not limited to the following: international mobile subscriber identity (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers; closed-circuit television cameras; gunshot detection hardware and services; video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; mobile DNA capture technology; biometric software or technology, including facial, voice, iris, and gait-recognition software and databases; software designed to monitor social media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network. Surveillance Technology does not include the following devices, hardware, or software:

(1) Office hardware, such as televisions, computers, credit card machines, copy machines, telephones, and printers, that are in common use by City Departments and used for routine City business and transactions;

(2) City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resource, permit, license, and business records;

(3) City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology, including payroll, accounting, or other fiscal databases;

(4) Information technology security systems, including firewalls and other cybersecurity systems intended to secure City data;

(5) Physical access control systems, employee identification management systems, and other physical control systems;

(6) Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

(7) Manually-operated technological devices used primarily for internal City communications, which are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices, and email systems;

(8) Manually-operated and non-wearable handheld cameras, audio recorders, and video recorders, that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

(9) Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

(10) Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury, and used and/or kept in the ordinary course of providing City services;

(11) Parking Ticket Devices;

(12) Police Department interview rooms, holding cells, and internal security audio/video recording systems;

(13) Police department computer aided dispatch (CAD), records/case management, Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems;

(14) Police department early warning systems; and

(15) Computers, software, hardware, or devices intended to be used solely to monitor the safety and security of City facilities and City vehicles, not generally accessible to the public.

"Surveillance Technology Policy" means a written policy that includes:

(1) A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose;

(2) A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services;

(3) The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited;<sup>1</sup>

(4) A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed;

(5) The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information;

(6) The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

(7) The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

(8) How collected information can be accessed or used by members of the public, including criminal defendants;

(9) Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy;

(10) The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology;

(11) The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy; and

(12) What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

(Added by Ord. 101-19, File No. 190110, App. 5/31/2019, Eff. 7/1/2019; Ord. 107-19, File No. 190568, App. 6/14/2019, Eff. 7/15/2019)

CONFIDENTIAL NOTE

1. See in Ord. 101-19 and Ord. 107-19.

# 1. PROJECT SUMMARY

## 1.1 Background

Our vision is that homelessness in San Diego would be rare, brief and non-recurring. In order to accomplish our vision, we must know the scope of the problem, know the characteristics of those who find themselves homeless, and understand which homeless resolution strategies are effective and which are not. Reliable data enables our community to work confidently towards our goals as we measure outputs, outcomes, and impacts.

A Homeless Management Information System (HMIS) is the information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program interim rule 24 CFR 578. It is a locally-administered data system used to record and analyze client, service and housing data for individuals and families who are homeless or at risk of homelessness. HMIS is a valuable resource because of its capacity to integrate and un-duplicate data across projects in a community. Aggregate HMIS data can be used to understand the size, characteristics, and needs of the homeless population at multiple levels: project, system, local, state, and national. The Longitudinal Systems Analysis (LSA) report, produced from a CoC's HMIS and submitted annually to HUD, provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care. This report could not be written if communities were not able to provide HUD with reliable, aggregate data on the clients they serve.

In 2010 the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its *Opening Doors: Federal Strategic Plan to Prevent and End Homelessness*. Since then many of the federal agencies that provide McKinney-Vento Act and other sources of funding for services to specific homeless populations have joined together and are working with HUD to coordinate the effort.

HMIS is now used by the federal partners and their respective programs in the effort to end Homelessness, which include:

- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Housing and Urban Development (HUD)
- U.S. Department of Veterans Affairs

The HMIS Data Standards provide communities with baseline data collection requirements developed by each of these federal partners. The HMIS Data Standards Manual is designed for CoC's, HMIS Lead Agencies, HMIS System Administrators, and HMIS Users to help them understand the data elements that are required in an HMIS to meet participation and reporting requirements established by HUD and the federal partners.

HUD is responsible for coordinating the collection of data, overseeing HMIS rules and regulations, and reporting to Congress through the AHAR, and will continue to manage the HMIS regulations, provide support and guidance to local CoC's and HMIS Lead Agencies, and provide guidance to users in collaboration with the federal partner agencies. The 2014 release of the Data Dictionary and Manual is the first joint publication of HUD and the federal partners and is intended to provide guidance to communities around federal expectations for HMIS. The HMIS Data Standards Manual was updated most recently in June 2020.



-Search-

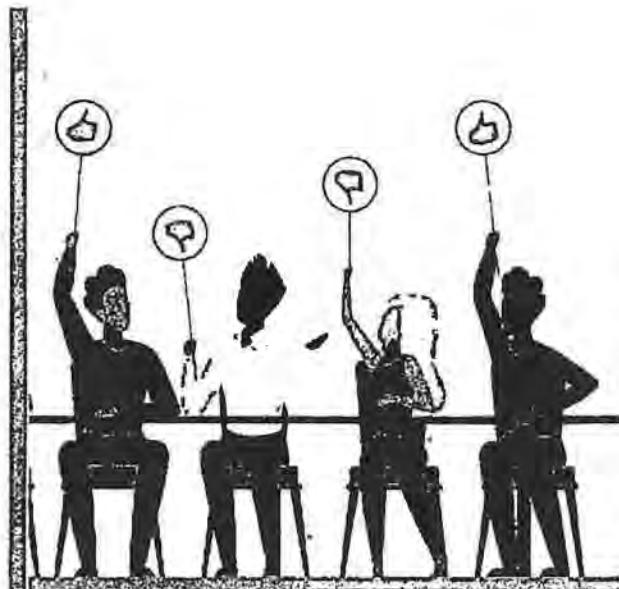
**U.S. Department of Health and Human Services (HHS)  
Substance Abuse and Mental Health Services  
Administration (SAMHSA):**

**Projects for Assistance in Transition from Homelessness  
(PATH)**

**Required Data Collection & HMIS Project Type**

Funded Components:		PATH: Street Outreach & Supportive Services Only	PATH: Street Outreach & Supportive Services Only
Data Element #	HMIS Project Type (Right): HMIS Element Name (Below):	Street Outreach (HMIS Project Type 4)	Services Only (HMIS Project Type 6)
3.01-3.917	Universal Data Elements (All)	X	X
4.02	Income and Sources	X	X
4.03	Non-Cash Benefits	X	X
4.04	Health Insurance	X	X

- FY2022 Data Standards
- HMIS Data Standards Introduction
- Project Descriptor Data Elements (PDDE)
- Universal Data Elements (UDE)
- Program Specific Data Elements (PSDE)
- Federal Partner Program Elements
- Metadata Elements
- HMIS Data Entry
- HMIS Lead
- CoC Lead
- HOPWA
- PATH**
- VA
- HUD CoC
- HUD ESG
- RHY
- HUD-VASH



#### 4. Prepare to Go Live

##### 4.1: Policies & Procedures

##### 4.2: Create Communication Plan

##### 4.3: Configure Outreach

##### 4.4: Training

-----  
may bring.

## Establish an Outreach Coordination Committee

As part of implementing Clarity Outreach, it is important to establish a strong Outreach Coordination Committee to help prepare the community and manage the rollout. Bitfocus recommends creating an Outreach Coordination Committee that includes a mix of stakeholders and community leadership. It is important to consider the anticipated level of involvement, interest, and influence within the project. Assess the landscape to identify stakeholders who are aligned with the project and may bring varying any potential conflict or varying degrees of cooperation each stakeholder

Consider the following stakeholders for your community's Outreach Coordination Committee:

STAKEHOLDER	VALUE PROVIDED
CoC Representatives	Ensure outreach services are well integrated into the homelessness response system and are aligned with the community's coordinated efforts.
HMIS System Administrators	Understand HMIS software and Clarity Outreach module and can provide insight into potential workflows and data collection
Individuals with Lived Experience	Provide critical insight into the experience of being homeless, receiving services, living in encampments, and more
Outreach Providers	Experience providing outreach services, and understanding of day-to-day workflows and challenges
Funders	Knowledge of funding opportunities, limitations, and restrictions

- Emergency Services
- Public Works
- Park and Recreation

on homelessness. They could already have outreach and engagement processes in place that can provide insight into services, and coordinate with new efforts

[Back to Top](#)



STEP 2

## 1.2 Define Roles & Responsibilities

Once you have created your implementation committee, the next step is to define clear roles and responsibilities. Before the project begins, identify the staffing and support your community will need for rollout. These individuals will support the remaining steps in the rollout process.

Consider who will fulfill the following project needs:

ROLE	RESPONSIBILITY
Project Management	Coordinates all parts of project rollout, and communicates with the project team to ensure that timelines and responsibilities are clear and that all milestones are met
System Configuration	Configures Clarity Human Services to meet the needs of the outreach project
Communication	Plans and completes communication to service providers and the community at large to apprise them of timelines, processes and process changes, milestones, and other key information
Training Content Development	Develops content used to train service providers and other impacted staff which may include slide decks, job aids, workflow diagrams, and other materials
Training Facilitation	Conducts training for service providers and other impacted staff

## DATA COLLECTION AND INTEGRATION IN HMIS

One the primary challenges providers identified was with collecting client data through multiple data systems. In particular, nearly all providers interviewed discussed a need for further integration with the County's HMIS, Clarity, to reduce duplicative data entry and the burden it places on agency staff, as well as the resulting impact on data quality. Broader integration of data across systems, including County health, mental health, criminal justice, and other departments, was also needed to improve coordination across systems and provide a holistic view of the experience and outcomes of people experiencing homelessness across the county.

### SANTA CLARA COUNTY'S CLARITY SYSTEM

The County's Clarity system, developed and administered by Bitfocus, is the primary means of gathering information on programs that serve people experiencing homelessness across the community (see text box for additional information on HMIS). Overall, providers were satisfied with the Clarity system and agreed it improved significantly upon the previous HMIS. Among other benefits, providers appreciated the ability to generate standard reports to analyze client outcomes and to satisfy funder reporting requirements. Providers also appreciated the support available from Bitfocus staff and reported that the recent "Data Literacy Institutes" provided by Bitfocus, which take a deeper dive into reporting functionalities for both agency staff and managers, were helpful to gain skills for maximizing the functionality of the system.

However, nearly all providers also reported some frustration with certain functionalities of the Clarity system, and acknowledged that most staff were not able to take full advantage of the all of the system's capabilities due to a lack of technical expertise. Some providers were not aware of all functionalities or customization options that are currently available. In addition to reporting gaps discussed in the next section, providers cited specific areas for improvement, including:

- Additional case management functionalities.
- Capturing additional information, such as tracking historical changes in client income.
- Building out the location tab to allow for descriptions of other locations where clients may be found (e.g. where they pick up medication or where they access certain services).
- More accurate GPS location tabbing functionality, as currently it is not effectively pinning a location.
- Capability to track and manage landlord relationships or potential roommates for shared housing.
- Texting capabilities to contact clients in their preferred mode of communication.
- Streamlined reporting functionality (see *Reporting & Analytics* below for more detail).
- More prominent notifications when a client has been referred to housing.

Each Participating Agency is required to have a Progressive Discipline Policy.

## 5. PRIVACY AND SECURITY

### **5.1 Privacy and Security**

#### *Privacy and Security Policy*

The HMIS Privacy and Security Policies and Procedures apply to any person accessing HMIS data, however, Participating Agencies subject to more restrictive regulations will be honored. In order to incorporate any Participating Agency's more restrictive regulations, additional implementation elements may be utilized to provide a cohesive framework for policies and procedures.

#### *Procedure*

All HMIS Lead Agency assets (e.g., workstations, laptops, and other systems or devices that process and/or store HMIS information) must be protected by commercial anti-virus and internet security software solutions.

- HMIS Lead Agency devices used to access HMIS shall utilize a firewall between the workstation and any external system including the internet;
- Security solutions must be updated when new versions or releases become available;
- Security software and operating system patches shall be applied within a reasonable time when they become available; and
- Any HMIS information stored on media shall be encrypted.

Participating Agency End-users are advised that these policies do not allow any use that is unlawful or other applicable rules and regulations, or is specifically prohibited by this policy or another applicable agency policy.

Under no circumstances will end-users store Personally Identifiable Information (PII) on any personally owned media; end-users may not place PII on a work-owned USB drive for personal use.

PII and removable data devices (e.g., USB drives, CDs, and external drives) must be protected by appropriate physical means from modification, theft, or unauthorized access. Such records and confidential information contained therein remain subject to the HMIS Policies and Procedures. When these media have reached the end of their useful life, the data will be disposed of in a manner consistent with the procedures outlined in this policy.

#### **Risk Analysis Management - HMIS Lead Agency Risk Analysis**

The HMIS Security Officer, in conjunction with executive management, and the HMIS Lead Agency Privacy Officer, will perform a modified Security Risk Analysis (RA) in accordance with the National Institute of Standards and Technology (NIST). The minimum content of the RA shall consist of:

- List of assets (i.e. hardware, software, data, physical sites);
- Threats to each of the listed assets (ex.: hacking, malware, misuse of data, burglary);

- Likelihood threats and impact of threat exploitation; and
- Heat map of likelihood versus impact.

Any decisions on selection of security measures to reduce risk must be documented and based on the RA.

Lack of funds to support security measures may be a mitigating factor for the current fiscal term, however lack of funds should be addressed in a Short-Term Security Mitigation Plan that is three (3) to five (5) years in implementation length and addresses funding.

#### **HMIS Vendor**

The CoC is responsible for the process and selection of the region's HMIS Vendor.

The HMIS Lead Agency is responsible for ensuring HMIS is operated in accordance with HMIS standards via the HMIS Vendor Contract.

The HMIS Lead Agency will include provisions in the HMIS Vendor contract requiring the physical security of the facilities and media storing the data is protected.

- The HMIS Vendor is required to take steps, consistent with the most current HMIS technical and security standards, to prevent unauthorized access to the data and the software (See Section 5.2 "Access Controls");
- The HMIS Lead Agency, through the HMIS Vendor contract, will take measures to ensure the system is protected from intrusion and risks to data loss is minimized;
- The HMIS Vendor will maintain software consistent with the most up-to-date HMIS technical and security standards:
  - The HMIS Vendor must retain a log of system changes and/or software version changes;
  - Security gaps or issues, identified by the HMIS Vendor or HMIS Lead Agency, shall be resolved in an expedient manner; and
  - The HMIS Lead Agency is responsible for ensuring all vendor-released enhancements, upgrades and bug fixes are applied promptly.

Participating Agencies shall be notified of changes by HMIS Lead Agency where appropriate.

#### **Data Backup**

HMIS Vendor shall store and maintain backup versions of the data in a separate physical location consistent with the most up-to-date HMIS technical and security standards. Examples include:

- HMIS Vendor servers on which the HMIS data is stored shall utilize firewalls;
- HMIS Vendor will also perform daily, weekly and monthly data backups;
  - Backups will be held offsite at a secondary (hot) data center;
- Intra-day and day-end backups will be held on a local server as well as offsite at the secondary data center.

Entities providing funding to Participating Agencies, or projects required to use HMIS, will not have automatic access to the HMIS.

- Access to HMIS will only be granted according to the Access Controls;
- Funders requesting access to HMIS data, or summary reports, must submit through their contracted Participating Agency;

Any requests for reports or information from an individual or group who have not been explicitly granted access to the HMIS will be directed to the HMIS Lead Agency.

- No individual client data will be provided to meet these requests without Evaluations Committee review of the data request.

### **Verbal Consent for Services**

In an effort to more efficiently serve the client, the HMIS Lead Agency may authorize the use of a verbal process for assessment and documentation by 2-1-1 San Diego. The verbal process does not replace in person enrollment.

- The verbal process to collect information shall replace a written signature on the Multiparty Authorization (MPA) with a telephonic signature which will allow for authorized access to the client's data, and shall collect relevant identifiers to ensure unique identification of the individual and record of the Authorization;
- Authorized Participating Agencies shall certify in the HMIS they have talked to the individual, and to the best of their ability, collected the required unique identifiers and have indicated such by including a telephone reference number on the electronic file in the HMIS;
- "Data Not Collected" for identifier fields shall require physical corroboration prior to delivery of services;
- Verbal Consent process shall be monitored on an ongoing basis and should be used sparingly when a written signature is not possible;
- The HMIS Lead Agency must provide written authorization to Participating Agencies wishing to use the verbal consent process.

### **Research Projects**

Request for research projects must be approved by the HMIS Lead Agency. Should the HMIS Lead Agency determine that additional review is required, the request will be forwarded to the Evaluations Committee for a final determination.

Research that is approved by the Institutional Review Board (IRB) must meet the Office for Human Research Protections (OHRP) requirements for use of individual client data. Waiver of Informed Consent by an IRB does not constitute a waiver of individual privacy rights under other federal or state laws.

Requirement of an IRB for research is exempt at 45 CFR 46.101 where:

- Unless otherwise required by the research entity or Participating Agency heads, research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy:
  - Research and demonstration projects which are conducted by or subject to the approval of the research entity or Participating Agency, and which are designed to study, evaluate, or otherwise examine;
  - Public benefit or service programs;
  - Procedures for obtaining benefits or services under those programs;
  - Possible changes in or alternatives to those programs or procedures; or
  - Possible changes in methods or levels of payment for benefits or services under those programs.

Access to client-level data for uses or disclosures not described here must be done only utilizing the Multiparty Authorization.

### **HMIS Reporting and Publication**

The HMIS Lead Agency may utilize data in the HMIS for federal reporting, local evaluation, analysis, and publication.

To foster full transparency, identifiable project-level data pertaining to CoC and/or federally, state, or locally funded program performance may be published by the HMIS Lead Agency upon request by the Governance Board, Full Membership, and/or its subcommittees. Identifiable client-level data may only be released within the HMIS with client Authorization solely for coordination of housing and services. Clients may authorize the HMIS to release their information outside of the HMIS (ex.: Community Information Exchange (CIE)).

### **Participating Agency Procedure Notification**

At minimum, the HMIS Lead Agency requires Participating Agencies to post signs (Appendix F) where data collection occurs. The sign will include the following language:

*"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information as mandated by law or as requested from entities that fund this program. Other personal information we collect is necessary to operate programs, improve services, and better understand homelessness. We collect appropriate information only. A Privacy Notice is available upon request."*

Participating Agencies must notify individuals seeking their assistance of data collection, use, and that disclosure will occur for the purposes of:

- Coordination of individual referrals, case management, housing, or other services; and
- Sharing with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information.

### **Data Standard Compliance**

Participating Agencies and the HMIS Lead Agency are jointly responsible for ensuring project data in the HMIS meets the thresholds outlined in this policy:



# Surveillance Technology Inventory

This inventory shows all currently identified surveillance technologies. For each technology, City departments are required to create a Surveillance Impact Report, a Surveillance Technology Policy, and Annual Reports.

A "Surveillance Technology" is defined as:

- A software, electronic device, system using an electronic device, or similar device
- used, designed, or primarily intended to
- collect, retain, process, or share
- audio, electronic, visual, location, thermal, biometric, olfactory or similar information
- specifically associated with, or capable or being associated with, any individual or group

The Surveillance Ordinance includes 15 separate exemptions for technologies not required to be inventoried. For more details, refer to the ordinance directly.

Our current inventory of surveillance technologies by department will continue to grow as additional technologies are identified.

*Last updated October 24, 2022.*

1948

# Documents

## Adult Probation Department

Adult Probation: GPS Monitoring

Ankle Bracelet

Upcoming

GPS Monitoring Ankle Bracelet

Adult Probation: Survey Monkey

Upcoming

An online survey software that helps organizations or individual users create and run professional online surveys.

## Airport

Airport: Airport Gunshot Detection

- proof of concept

Upcoming

The detectors sense for the presence of a gunshot, conducting full analysis on the device (no real-time audio is sent back). In the event of an activation, the alert message is sent over our proprietary wireless mesh (potentially hopping over multiple detectors) back to the gateway. The gateway connects to the AmberBox Response Platform servers via a VPN and HTTPS connection. The AmberBox Response Platform servers are hosted by our cloud provider, Google Cloud.

Airport: App-Based Commercial  
Transportation Management  
System  
Upcoming

Airport uses data provided by Transportation Network Companies (TNCs) to track the whereabouts of specific vehicles (license plate info and geo-location information provided by TNCs in real-time at four different points of a TNC's journey on the Airport's premises) to support permit compliance.

Airport: Electronic Toll Readers  
Upcoming

Vehicle-mounted transponder that is activated by an antenna on a toll lane. Individual account information is stored in the transponder. The antenna identifies the individual transponder and reads the associated account information. The amount of the toll is deducted from the associated account.

Airport: Hootsuite  
Upcoming  
Social Media Marketing and Management Dashboard

Airport: License Plate Recognition  
System Surveillance Technology  
Policy

System includes high-performance IP cameras and powerful software that provides consistent and reliable results. The system converts the image (picture of the license) to computer data that can be checked against a database.

Airport: License Plate Recognition  
System Surveillance Impact Report

August 4, 2021

System includes high-performance IP cameras and powerful software that provides consistent and reliable results. The system converts the image (picture of the license) to computer data that can be checked against a database.

### Airport: Media Access Control

#### (MAC) Address

##### Upcoming

The media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller. It is used as a network address for most network technologies, including Ethernet, Wi-Fi, and Bluetooth. Airport operates an extensive Wi-Fi network throughout the Airport's facilities.

### Airport: ParkAssist Parking

#### Guidance System

##### Upcoming

The sensors determine parking stall availability and the cameras provide a snapshot of license plates to assist the public in locating their vehicles via Park Assist "Find My Car" smartphone app.

### Airport: Pre-Security Closed Circuit

#### Television (CCTV) Cameras

#### Surveillance Impact Report

August 4, 2021

Pre-Security Closed Circuit Television (CCTV) Cameras

### Airport: Pre-Security Closed Circuit

#### Television (CCTV) Cameras

#### Surveillance Technology Policy

August 4, 2021

Pre-Security Closed Circuit Television (CCTV) Cameras

### Airport: Survey Monkey

##### Upcoming

An online survey software that helps organizations or individual users create and run professional online surveys.

### Airport: Third-Party Cameras

#### Surveillance Technology Policy

February 17, 2022

## Third-Party Cameras used at the San Francisco Airport.

### Airport: Third-Party Cameras

#### Surveillance Impact Report

February 17, 2022

Third-Party Cameras used at the San Francisco Airport.

## Animal Care and Control

### Animal Care and Control: Security

Cameras

Upcoming

Security Cameras

## Arts Commission

### Arts Commission: Constant

Contact

Upcoming

Email marketing service. Records names and emails of individuals who subscribe.

### Arts Commission: Hootsuite

Upcoming

Social Media Monitoring

### Arts Commission: Meltwater

Upcoming

Meltwater is a software designed to monitor social media and traditional media.

10532

Arts Commission: Security  
Cameras Surveillance Technology  
Policy

August 4, 2021

Surveillance systems are located in the San Francisco Arts Commission Galleries to monitor exhibition space at all times, as well as throughout City-owned Cultural Centers.

Arts Commission: Security  
Cameras Surveillance Impact  
Report

August 4, 2021

Surveillance systems are located in the San Francisco Arts Commission Galleries to monitor exhibition space at all times, as well as throughout City-owned Cultural Centers.

## Asian Art Museum

Asian Art Museum: AdRoll

Upcoming

Uses advanced audience targeting to create awareness and drive high-quality new site traffic. It helps grow customer acquisition. Its growth marketing platform makes it easy to find the proper audience, create personalized, cross-channel experiences, and measure impact.

Asian Art Museum: Google Tag

Manager

Upcoming

A Google marketing platform and tag management system that helps website owners track codes and collect analytics about their website. It helps website owners make decisions about their

1054  
123

website. Data is stored in a centralized location. It can also assist with analytics for purposes such as marketing, tracking customer conversion rates, and other site analytics.

Asian Art Museum: MailChimp

Upcoming

Marketing automation platform and email marketing service

Asian Art Museum: Mobile Fuse

Upcoming

A mobile technology company that helps target and influence consumers. Their proprietary technology utilizes location and consumer mindset as a foundation to fuel customer insights. Consumer mindset is determined by leveraging environmental data including time of day, weather conditions, local event and census information that gives advertisers a holistic view into the user's mindset.

Asian Art Museum: Security

Camera System Surveillance

Technology Policy

August 4, 2021

Monitoring and recording device

Asian Art Museum: Security

Camera System Surveillance

Impact Report

August 4, 2021

Monitoring and recording device

Asian Art Museum: Steelhouse

Upcoming

Provides self-service advertising software that provides marketers with everything they need to build their own ads and launch retargeting and prospecting campaigns through display, mobile, native, and social media. The analytics and reporting feature is integrated into Google Analytics, which allows tracking and verification of all traffic and conversions across devices. It can be used to create reporting dashboards, display metrics, visualize metrics, etc.

**Asian Art Museum: Survey Gizmo****Upcoming**

An enterprise-level data collection platform that collects feedback through surveys and gives surveyors fast and accurate reporting

**Asian Art Museum: Survey Monkey****Upcoming**

An online survey software that helps organizations or individual users create and run professional online surveys.

## **Assessor-Recorder**

No surveillance technology inventory reported to date

## **Board of Appeals**

No surveillance technology inventory reported to date

## **Board of Supervisors**

**Board of Supervisors: MailChimp****Upcoming**

Marketing automation platform and an email marketing service

City Administrator's Office: Buffer  
(311)

Upcoming

Cloud based Social Media response system. It is a social media management software that allows organizations build their audience and grow their brand on social media. Allows organizations to measure and analyze content performance, track key engagement metrics, and measures stories, individual posts, and hashtags. It also measures audience demographics.

City Administrator's Office:  
MailChimp (Committee on  
Information Technology)

Upcoming

Marketing automation platform and email marketing service

City Administrators' Office : Survey  
Monkey (Committee on Information  
Technology)

Upcoming

An online survey software that helps organizations or individual users create and run professional online surveys.

City Administrator's Office:  
Security Camera System  
Surveillance Technology Policy  
(Real Estate Department, Media  
Security Group)

August 4, 2021

Cameras, workstations, and Network Video Recorders (NVRs) to record security video.

City Administrator's Office:  
Security Camera System  
Surveillance Impact Report (Real  
Estate Department, Media Security  
Group)

1057 126

August 4, 2021

Cameras, workstations, and Network Video Recorders (NVRs) to record security video.

## **City Attorney's Office**

City Attorney's Office: MailChimp

Upcoming

Marketing automation platform and an email marketing service

## **City Planning**

City Planning: BuildingEye

Upcoming

Web application which allows public to subscribe and receive notifications for permit related events. It stores some personal information such as name and email address.

City Planning: Google Web

Analytics

Upcoming

Used for department's public facing web site to collect access data including browser type, source IP address, page accessed and timestamp

City Planning: GovDelivery

Upcoming

Used for newsletters and public engagement. GovDelivery records the names and emails of individuals who subscribe to its services.

City Planning: MailChimp

Upcoming

Used for newsletters and public engagement. MailChimp records the names and emails of individuals who subscribe to its services.

**City Planning: Microsoft IIS Access****Log****Upcoming**

Server side logging that can be enabled on a URL group to record the following data: Client IP address, user name, data, time, service and instance, server name, server IP address, time taken, etc.

**City Planning: Time-lapse Camera****Upcoming**

Takes individual photos that can be left separate or woven together to create professional-looking time-lapse videos with ease. The camera runs automatically and is powered by AA batteries and can capture up to 30,000 images before its batteries require changing.

## **Civil Service Commission**

No surveillance technology inventory reported to date

## **Child Support Services**

**Child Support Services: Sonitrol****Security Cameras Surveillance****Technology Policy**

August 4, 2021

Building security system which uses security cameras at points of entry and surveillance cameras at points of entries, public

lobby, and interview areas.

#### Child Support Services: Sonitrol

#### Security Cameras Surveillance

#### Impact Report

August 4, 2021

Building security system which uses security cameras at points of entry and surveillance cameras at points of entries, public lobby, and interview areas.

## **Children and Families Commission**

No surveillance technology inventory reported to date

## **Controller**

Controller: Emma

Upcoming

Emma Marketing Software

Controller: Survey Monkey

Upcoming

Survey Monkey

## **Department of Building Inspection**

1060 129

Department of Building Inspection:  
ForcePoint  
Upcoming  
Web security software for monitoring, filtering and reporting web traffic

Department of Building Inspection:  
Survey Monkey  
Upcoming  
An online survey software that helps organizations or individual users create and run professional online surveys.

## **Department of Children, Youth & Their Families**

No surveillance technology inventory reported to date

## **Department of Elections**

Department of Elections: Constant Contact  
Upcoming  
Email marketing service.

Department of Elections: Cooler Email  
Upcoming  
Email marketing service.

Department of Elections: NestCameras Surveillance Technology Policy

November 18, 2021

Cameras for internal viewing and streaming.

Department of Elections: NestCameras Surveillance ImpactReport

November 18, 2021

Cameras for internal viewing and streaming.

Department of Elections: SurveyMonkeyUpcoming

An online survey software that helps organizations or individual users create and run professional online surveys.

## Department of Emergency Management

Department of EmergencyManagement: Closed CircuitTelevision Cameras (CCTVs)Surveillance Technology Policy

August 4, 2021

The system is maintained by DT and monitored by Sheriff's Department staff on site. Not monitored by DEM Staff.

Department of EmergencyManagement: Closed CircuitTelevision Cameras (CCTVs)Surveillance Impact Report

August 4, 2021

The system is maintained by DT and monitored by Sheriff's Department staff on site. Not monitored by DEM Staff.

Department of EmergencyManagement: HootsuiteUpcoming

Upcoming

### Social media monitoring

Department of Emergency

Management: Public Safety Crime

Cameras

Upcoming

The system is administered by SFPD and maintained by DT. DEM's role is limited to providing copies of video at the request of SFPD personnel.

Department of Emergency

Management: ShotSpotter

Upcoming

An advanced system of sensors, algorithms and artificial intelligence to detect, locate and alert police to gunfire. It analyzes audio signals for potential gunshots, determines the location of the sound source, analyzes the pulse features to determine if the sound is likely to be gunfire, and notifies law enforcement and emergency responders. This system is maintained by the vendor and administered and paid for by SFPD.

Department of Emergency

Management: Tweetdeck

Upcoming

Social media monitoring. TweetDeck is a social media dashboard application for management of Twitter accounts. Originally an independent app, TweetDeck was subsequently acquired by Twitter Inc. and integrated into Twitter's interface.

## Department of the Environment

No surveillance technology inventory reported to date

10632

## Department of Homelessness and Supportive Housing

Department of Homelessness and  
Supportive Housing: Homeless  
Shelter Reservation System  
Upcoming

The system uses biometric finger imaging and photos to enroll single adult shelter clients, manage their reservations and identify and check-in those clients to the adult shelters.

Department of Homelessness and  
Supportive Housing: Security  
Camera System Surveillance  
Technology Policy

August 4, 2021

Security camera collects images, which are available to staff for real-time review

Department of Homelessness and  
Supportive Housing: Security  
Camera System Surveillance  
Impact Report

August 4, 2021

Security camera collects images, which are available to staff for real-time review

## Department of Human Resources

Department of Human Resources:  
Security Cameras Surveillance  
Technology Policy

August 4, 2021

Security cameras

DEPARTMENT OF PUBLIC RESOURCES:Security Cameras SurveillanceImpact Report

August 4, 2021

Security Cameras

## Department of Public Health

Department of Public Health:Closed Circuit Television Cameras(CCTVs) Surveillance TechnologyPolicy

August 4, 2021

Security cameras located at various locations - A TV system in which signals signals are not publicly distributed, but monitored, primarily for surveillance and security purposes. Relies on strategic placement of cameras and observation of the camera's input on monitors somewhere.

Department of Public Health:Closed Circuit Television Cameras(CCTVs) Surveillance Impact Report

August 4, 2021

Security cameras located at various locations - A TV system in which signals signals are not publicly distributed, but monitored, primarily for surveillance and security purposes. Relies on strategic placement of cameras and observation of the camera's input on monitors somewhere.

## Department of Public Health:

Survey Monkey

Upcoming

Survey Monkey

## Department of Public Works

Department of Public Works: Aerial

10/5 34

Drone Surveillance Impact Report

August 4, 2021

Aerial drone

Department of Public Works: AerialDrone Surveillance TechnologyPolicy

August 4, 2021

Aerial drone

Department of Public Works:Automatic License Plate ReaderSurveillance Impact Report

August 4, 2021

Automatic License Plate Reader

Department of Public Works:Automatic License Plate ReaderSurveillance Technology Policy

August 4, 2021

Automatic License Plate Reader

## Department on the Status of Women

No surveillance technology inventory reported to date

## Department of Technology

Department of Technology: Archive

Social

Upcoming

Social media archiving permits consistent response to records

135

requests

Department of Technology:

Community Safety Cameras

Upcoming

Chapter 19 of the Admin Code defines "Community Safety Cameras means any digital recording surveillance system installed at fixed locations in an open and obvious manner by the City and County of San Francisco to film public streets, sidewalks or common areas of public housing complexes."

Department of Technology: Drone

Surveillance Impact Report

August 4, 2021

Drone

Department of Technology: Drone

Surveillance Technology Policy

August 4, 2021

Drone

Department of Technology: Emma

Upcoming

Emma is an online, mass marketing email platform that DT uses to send email communications about planned maintenance, service upgrades, and other news and operations items.

Department of Technology: Local

Area Networks in City-Owned

Housing

Upcoming

Local Area Networks in City-Owned Housing

Department of Technology:

Outdoor Facility Cameras

Surveillance Technology Policy

August 4, 2021

Outdoor Facility Cameras

Department of Technology  
Outdoor Facility Cameras  
Surveillance Impact Report  
August 4, 2021  
Outdoor Facility Cameras

## District Attorney

District Attorney: Surveillance

Technology Exemption

Certification

August 19, 2021

The District Attorney's Office letter to the Controller certifying exemption from compliance to avoid interference with investigative or prosecutorial functions.

## Ethics Commission

No surveillance technology inventory reported to date

## Fine Arts Museums

Fine Arts Museums: Bidtellect

Upcoming

The information collected by Bidtellect includes name, email address, password, telephone number, computer IP address, mobile device unique ID and real-time geographic information. The combination of this data is then used to determine the interest and behaviors of a unique user so that Bidtellect can deliver personalized advertising content to them

**Fine Arts Museums: CCTVs****Upcoming**

Security cameras located at various locations - A TV system in which signals signals are not publicly distributed, but monitored, primarily for surveillance and security purposes. Relies on strategic placement of cameras and observation of the camera's input on monitors somewhere

**Fine Arts Museums: Data Studio****Upcoming**

Advertisement integration and analytics - A Google product that helps prepare data visualizations by providing the resources to turn data into informative, easy to share, and fully customizable dashboards and reports. To use it, must connect data sets such as those from Google Marketing Platform products, Google consumer products, databases, updated CSV files, or social media platforms.

**Fine Arts Museums: Datorama****Upcoming**

Visualization platform

**Fine Arts Museums: Facebook****Business Manager****Upcoming**

A free platform that runs and tracks ads, manages pages and ad accounts, or allow third-parties manage ad placements, etc. It helps advertisers integrate Facebook marketing efforts across the organization's business with external partners

**Fine Arts Museums: Falcon****Upcoming**

This Social Media listening tool tracks a user's interactions with the museum's social media channels over time. I.e. whether they have commented on posts in the past in addition to the current one

### Fine Arts Museums: Flashtalking

#### Upcoming

Flashtalking does not collect or process directly-identifiable information, such as a person's name and email address, or hold sensitive data of any sort. Flashtalking's products and policies limit their collection and use of personal data to online identifiers such as IP addresses, cookie IDs and device IDs, which they use for fraud detection, engagement analysis, and advertising delivery.

### Fine Arts Museums: Google

#### Adwords

#### Upcoming

Search ad platform - Google's advertising system through which advertisers bid on certain keywords in order for their clickable ads to appear in Google's search results. Advertisers pay for these clicks. Also known as "Google Ads"

### Fine Arts Museums: Google

#### Analytics

#### Upcoming

A free tracking tool offered by Google that shows how visitors use a website. A tracking code is added to the website so Google Analytics knows to track website visitors and any actions they perform. When a user visits the website, Google Analytics drops a cookie on the user's browser. Cookies are small files that contain information about the user's activities. Using these cookies, Google Analytics will know how a user behaves on your website and then collect this information. The reporting feature shows the demographics and geographic region of website visitors (i.e. age, gender), among other characteristics (interests, behavior, mobile, etc.).

### Fine Arts Museums: MailChimp

#### Upcoming

Mailchimp may gather personal information such as name, email address or telephone number. Mailchimp may also automatically

139

gather information such as information about a user's device such as IP address. Mailchimp uses cookies and other tracking technologies.

Fine Arts Museums: Meraki  
Upcoming  
Cloud-controlled WiFi, routing, and security

Fine Arts Museums: Optmyzr  
Upcoming  
Optimizes advertisers' pay-per-click advertising. It assembles raw AdWords and Bing Ads information into comprehensive visualizations so advertisement account managers can follow highlights and trends and guide their ad placement strategies. It relies on robust automation that is enabled and enhanced with AdWords scripts.

Fine Arts Museums: The Trade Desk  
Upcoming  
The information collected by The Trade Desk includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and clickstream data. This data is gathered using several different methods including log files, cookies, clear gifs, and social media features.

## Fire Department

Fire Department: 360-Degree Cameras on Department Apparatus (Fire Trucks)  
Upcoming  
360-degree cameras attached to department apparatus (fire trucks) assist drivers in seeing other people or objects around them. Cameras record footage on a 30-hour loop.

Fire Department: Body-Worn  
Cameras Surveillance Impact  
Report

October 21, 2021  
Body-worn cameras

Fire Department: Body-Worn  
Cameras Surveillance Technology  
Policy

October 21, 2021  
Body-Worn Cameras

Fire Department: Critical Mention  
Upcoming

Critical Mention is software designed to monitor social media and traditional media.

Fire Department: Drone  
Surveillance Impact Report

August 4, 2021  
Drone

Fire Department: Drone  
Surveillance Technology Policy

August 4, 2021  
Drone

Fire Department: Mounted  
Cameras on Mobile Command  
Vehicle

Vehicle has mounted cameras for monitoring of surrounding area through live video feed.

Fire Department: Surveillance  
Cameras Surveillance Impact  
Report

August 4, 2021  
Mounted security cameras at Department facilities.

Fire Department: Surveillance  
Cameras Surveillance Technology  
Policy

August 4, 2021

Mounted security cameras at Department facilities.

Fire Department: Survey Monkey  
Upcoming

An online survey software that helps organizations or individual users create and run professional online surveys.

## **Health Service System**

No surveillance technology inventory reported to date

## **Human Rights Commission**

No surveillance technology inventory reported to date

## **Human Services Agency**

1073  
142



January 19, 2022

### Mayor Breed's Attack on San Francisco's Surveillance Ordinance is Misguided

San Francisco-In a lengthy press release issued on January 18, 2022 by the office of San Francisco mayor London Breed, the mayor declares her intention to water down San Francisco's surveillance ordinance, whether by supervisor vote or by ballot initiative. The release seeks, inaccurately, to claim the ordinance is preventing the San Francisco Police Department from using Business Improvement District owned cameras to monitor retail corridors.

As evidence, Breed points to the *Williams v San Francisco* case, filed by the ACLU of Northern California and the Electronic Frontier Foundation. However, that case involves the use of private cameras to monitor protests against police brutality after the murder of George Floyd. Breed states in her press release that protests and First Amendment protected activities should not be monitored remotely by private camera networks by the Police Department. The looting that did occur in San Francisco around the time of the protests was not prevented by SFPD's real-time access to the camera network.

San Francisco's surveillance ordinance **does not** prevent the use of any equipment or technology besides the use of facial recognition, which is banned. It simply requires the creation of a usage policy and impact report that is reviewed and approved by the Board of Supervisors. If the San Francisco Police Department wants to use the cameras under certain circumstances, all they need to do is ask and describe the specific circumstances when use would be allowed. That request was never made and now it is almost three years since the ordinance was passed, and the equipment was used without ever doing so. Now the intent seems to be to revise the surveillance ordinance so that it never will and that private camera networks can be used with impunity.

*Oakland Privacy's advocacy director Tracy Rosenberg commented: The use of any surveillance technology with impunity is a recipe for disaster. We've seen the building of a surveillance state with just these kinds of demands for unfettered and unregulated use. "Trust us" is not the answer for technology. It's having clear rules of the road. San Francisco's mayor and police department saying "we don't want no stinkin' rules" is really disappointing. Rules are not "an obstacle," they are a safety measure."*

San Francisco's mayor goes on to provide two scenarios for this unfettered and unregulated use of private camera networks by the police department. The first expands the existing exemption for serious threats of injury or death to a person to include "organized theft or robbery."

The second imposes a waiver of any rules when there is an "open-air drug market" or when crime statistics have increased in a 14-day period. It isn't clear whether the waiver applies to a particular block where drug dealing is said to occur, an entire neighborhood like the Tenderloin or the entire City. To the best of our knowledge, the private camera networks in San Francisco's downtown area are in Union Square and operated by the business improvement district, and aren't located in the Tenderloin. The other camera network close to downtown in San Francisco is in Japantown. It isn't clear what impact real-time police access to cameras in Japantown and Union Square would have on the Tenderloin.

MARCH 15, 2023

CHRIS WARD KLINE  
250 KEARNY ST  
618  
SAN FRANCISCO, CA 94108  
415-513-9334

RE: EXPLANATION OF INTRO ALL PAGES 1-12

Pg 1-2: DOJ critiquing proposed Gang Injunction in 2006 that would have utilized surveillance type of equipment. A few people and agencies did without the injunction and placed people on surveillance without court order or paperwork, then simply state that the paperwork doesn't exist because there was no warrant. If person continues to make waves, they attempt at all costs to claim the suspect, claimant or plaintiff as having mental health issues.

With this, you can 'isolate or quarantine' a person from his friends and family. Public Health uses this same surveillance for epidemics, sheriff and police to place people on gang surveillance (that the law didn't catch, so to teach them a lesson) and the mayor or others, place political dissidents on that pose a political threat. DEM (Department of Emergency Management) is the agency that collects and saves all the information, but they too, can utilize in an illegal manner. This type of surveillance is simply called Cyberstalking which will clearly show the city and county of San Francisco has the devices, the technology and equipment to store such behavior. A check and balance allows the state of California to have a copy of these files, as does the DOJ, Department of Commerce, Labor, Intelligence Community, Health and Human Services, amongst other county, state and federal partners due to protections and potential violations of the Constitution.

Pg 3: 14<sup>th</sup> Amendment Equal Protection and Other Rights state cannot deprive any person of life, liberty or property without due process of law....

Pg 4: 14<sup>th</sup> Amendment S1.5.2 right to be free from official stigmatization ref: 1971 Wisconsin v. Constantineau

Pg 5: 14 Amendment s1.5.3 Property Deprivations and Due Process – No state shall make or ENFORCE any law which shall abridge the privileges or immunities of citizens of the United States

Pg 6: Cyberstalking to include equipment, technology and prohibitions to include all electronic forms of communications

Pg 7: Penalties for Cyberstalking include imprisonment for 2, 3, or 4 years and/or a fine of up to \$10,000 – one of the main reasons every would deny at all costs to prevent release of files

Pg 8: Document on SFgov website listing a portion of agencies and departments that utilize an app and application called One System. Please note the numbers of listed agencies to include the Department of Public Health. UCSF, Swords to Plowshares, Veterans Affairs – THIS IS A PARTIAL LIST AND I WILL AT A FUTURE DATE PROVIDE A COMPLETE LIST OF ALL SAN FRANCISCO AGENCIES UNDER THE CITY AND COUNTY OF SAN FRANCISCO

Pg. 9: Document on SFgov website that list applicable codes of professional conduct that would call under

- 1) SFPD
- 2) SHERIFF
- 3) PUBLIC HEALTH
- 4) DEM
- 5) Ultimately the Mayor's Office as she uses behavioral surveillance staff, and authorized \$53 million to fund Urban Alchemy, which every individual is placed on electronic surveillance, which is monitored by the Sheriff, SFPD and Mayor's Office through their devices, emails and phone numbers. So if I walk by one of these individuals, any one of the aforementioned agencies can bounce the surveillance and leave it on me for as long as they want.

 An official website of the United States government, Department of Justice.  
[Here's how you know](#)

**U.S. DEPARTMENT OF JUSTICE  
OFFICE OF JUSTICE PROGRAMS**

[Home](#) / [About NCJRS](#) / [Virtual Library](#)

# San Francisco's Proposed Gang Injunction: What Will it Mean, What Are the Problems, and How Will it Work?

**NCJ Number:** 218338

**Date Published:** November 2006

**Length:** 4 pages

## Annotation

After reviewing a proposed preliminary injunction being sought by San Francisco's City Attorney against individuals it believes are members or associates of an alleged street gang called Oakdale Mob, this paper identifies problems with such an injunction and considers the likelihood of its effectiveness.

## Abstract

An injunction is a court order that prohibits a named person or persons from continuing a particular activity named in the injunction. The proposed injunction against the Oakdale Mob aims to stop a public nuisance alleged to be illegal drug sales and possession, possession of illegal firearms, and assault with a firearm. The injunction would impose 11 specific restrictions on the activities of certain individuals identified by the city as gang members or associates. These restrictions would include a 10 pm curfew, a prohibition against associating with any other gang member or associate in public, and other activities already prohibited by law. Gang injunctions present many problems due to the severe limitations they impose on individual rights. One of the most commonly debated issues is injunctions' casting

*INTRO 077A11 Pg 1*

of a broad net that may mistakenly restrict the movements and associations of innocent people who have not engaged in behavior that violates a law. The short-term effects of gang injunctions generally show decreased crime rates in neighborhoods affected; however, over a long period of time (more than 1 year), the effects are marginal or minimal. Injunctions are more likely to have a positive long-term effect if accompanied by the development of constructive community programs for youth who may be attracted to or associated with gangs.

## Additional Details

**Corporate Author:**

Ctr on Juvenile and Criminal Justice 40 Boardman Place, San Francisco, CA 94103, United States

**Sale Source:**

Ctr on Juvenile and Criminal Justice 40 Boardman Place, San Francisco, CA 94103, United States

**Publication Format:**

Document (Online)

**Publication Type:**

Legislation/Policy Analysis

**Language:**

English

**Country:**

United States of America

**Note:**

\*This document is currently unavailable from NCJRS. Downloaded May 7, 2007.

---

## Downloads

**No download available**

---

---

---

## Availability

INTR9078A11 Pg 2

## Fourteenth Amendment Equal Protection and Other Rights

Amdt14.1 Overview of Fourteenth Amendment, Equal Protection and Rights of Citizens

Amdt14.2 State Action Doctrine

### Section 1 Rights

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

E INTRO - All Pg 3

In some cases, the Court also appeared to expand the notion of liberty to include the right to be free from official stigmatization, finding that the threat of such stigmatization could in and of itself require due process.<sup>12</sup> Thus, in the 1971 case *Wisconsin v. Constantineau*, the Court invalidated a statutory scheme in which persons could be labeled "excessive drinkers" without any opportunity for a hearing and rebuttal, and could then be barred from places where alcohol was served.<sup>13</sup> Without discussing the source of the entitlement, the Court noted that the governmental action at issue impugned the individual's "reputation, honor, or integrity."<sup>14</sup>

By contrast, in the 1976 case *Paul v. Davis*, the Court appeared to retreat from recognizing damage to reputation alone, holding instead that the liberty interest extended only to those situations where loss of one's reputation also resulted in the loss of a statutory entitlement.<sup>15</sup> In *Davis*, the police had included plaintiff's photograph and name on a list of "active shoplifters" circulated to merchants without an opportunity for notice or hearing. The Court rejected the constitutional challenge, holding that state law "does not extend to respondent any legal guarantee of present enjoyment of reputation which has been altered as a result of petitioners' actions. Rather, his interest in reputation is simply one of a number which the State may protect against injury by virtue of its tort law, providing a forum for vindication of [that] interest by means of damage actions."<sup>16</sup> Thus, it appears that unless the government's official defamation has a specific negative effect on an entitlement, such as the denial of the right to obtain alcohol that occurred in *Constantineau*, there

14<sup>th</sup> Amendment S1.5.2

INTRO - All Pg \$  
1080

## Amdt14.S1.5.3 Property Deprivations and Due Process

Fourteenth Amendment, Section 1:

*All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.*

---

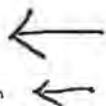
INTRO - All pg 5  
1081

## What Does Cyberstalking Consist Of?

Cyberstalking as a criminal offense, consists of using the internet or other electronic means to harass another person.

The communication can be done through:

- Text messages,
- Social media comments,
- Direct messages,
- Email and
- Other electronic forms of communication



The actor typically engages in the behavior deliberately and persistently to annoy or harass someone. Sometimes, the acts can be minor and cause a slight upset in the targeted person. Still, some cyberstalking cases are severe and disturbing and can lead to serious feelings of fear, stress, anxiety, or worry.

## Does California Prohibit Cyberstalking?

Yes, California makes it illegal for anyone to engage in a course of conduct that causes fear, annoyance, or terror. A course of conduct includes any action occurring two or more times over a certain period, regardless of how brief that is likely to continue.

The state does not have a separate cyberstalking law. The elements of the offense are the same as those for traditional (or in-person) stalking. The statute includes online forms of stalking by having a provision stating that written credible threats include those made through electronic communication.

Electronic communication devices include, but are not limited to, the following:

- Telephones,
- Cell phones
- Computers, and
- Video recorders.



Under California Penal Code § 646.9, stalking (and cyberstalking) consists of willful and malicious:

- Repetitive following, or
- Harassment involving credible threats.

INTRO - A11 pg 6

1082

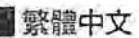
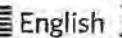
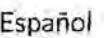
The potential penalties include imprisonment for 2, 3, or 4 years and/or a fine of up to \$10,000. Cyberstalking is also a felony if the actor has been convicted of domestic violence or violating a restraining order. In that case, the possible punishments include a prison sentence of 2, 3, or 5 years.

Oct 28, 2022

X

X

INR0 - 11. Pg 7  
1083

HOME     ABOUT HSH     SERVICES     PARTNER RESOURCES     PROJECTS AND PUBLIC POSTINGS  
CALENDAR     COVID-19

You are here: Home / Partner Resources / Data Sharing and Privacy / Partner Agencies with ONE System Access

## Partner Agencies with ONE System Access

3rd Street Youth Center and Clinic

AIDS Housing Alliance

Asian Women's Shelter

Bay View Hunters Point Multipurpose Senior Services

Bernal Heights Neighborhood Center

Brilliant Corners

Catholic Charities CYO

Chinatown Community Development Corporation

Citizens Housing Corporation

Community Awareness & Treatment Services (CATS) Community Housing Partnership

1684

INITRO - 11/11

P58

Compass Family Services

Conard House

Curry Senior Center (CC)

Delivering Innovation in Supportive Housing (DISH)

 Department of Homelessness and Supportive Housing (HSH) Dolores Street Community Services

Episcopal Community Services (ECS)

Eviction Defense Collaborative

First Place for Youth

Five Keys Charter Schools & Programs

 Glide Community Housing

GP/TODCO Inc.

Hamilton Families

Heluna Health

Homeless Children's Network

Homeless Prenatal Program

Homeless Youth Alliance

Hospitality House

Huckleberry Youth Programs

John Stewart Company

Larkin Street Youth Services

1085  
162

INTR0-A11 PS 9

LGBT Center

Lyric

Mary Elizabeth Inn

Mercy Housing

Mission Housing Development Corporation

Mission Neighborhood Health Center

Positive Resource Center (PRC)

Providence Foundation

Raphael House

Reality House West

SafeHouse

Salvation Army

San Francisco Housing Authority

San Francisco Human Services Agency (HSA)

San Francisco Unified School District

SF Department of Public Health (DPH)

SF Health Plan

St Vincent de Paul Society

Swords to Plowshares

Tenderloin Housing Clinic

163  
1086

INFO-A11 PG 10

Tenderloin Neighborhood Development Corporation (TNDC)

United Council of Human Services

University of California San Francisco

Automatic Translation Disclaimer

440 Turk Street  
San Francisco, CA 94102  
Contact Us

SEARCH

Search this website

---

© 2020-2022 San Francisco Department of Homelessness and Supportive Housing. All Rights Reserved.

164  
1087

FNTR0-A11 pg 11



**DEPARTMENT OF HOMELESSNESS AND SUPPORTIVE HOUSING**  
**STATEMENT OF INCOMPATIBLE ACTIVITIES**

**I. INTRODUCTION**

This Statement of Incompatible Activities is intended to guide officers and employees of the San Francisco Department of Homelessness and Supportive Housing ("Department") about the kinds of activities that are incompatible with their public duties and therefore prohibited. For the purposes of this Statement, and except where otherwise provided, "officer" shall mean the executive director ("director"); and "employee" shall mean all employees of the Department.

This Statement is adopted under the provisions of San Francisco Campaign & Governmental Conduct Code ("C&GC Code") section 3.218. Engaging in the activities that are prohibited by this Statement may subject an officer or employee to discipline, up to and including possible termination of employment or removal from office, as well as to monetary fines and penalties. (C&GC Code § 3.242; Charter § 15.105.) Before an officer or employee is subjected to discipline or penalties for violation of this Statement, the officer or employee will have an opportunity to explain why the activity should not be deemed to be incompatible with their City duties. (C&GC Code § 3.218.) Nothing in this document shall modify or reduce any due process rights provided pursuant to the officer's or employee's collective bargaining agreement.

In addition to this Statement, officers and employees are subject to Department policies and State and local laws and rules governing the conduct of public officers and employees, including but not limited to:

- Political Reform Act, California Government Code § 87100 et seq.;
- California Government Code § 1090;
- San Francisco Charter;
- San Francisco Campaign and Governmental Conduct Code;
- San Francisco Sunshine Ordinance;
- Applicable Civil Service Rules;
- Applicable codes of professional conduct, including, but not limited to:
  - o California Board of Behavioral Sciences;
  - o Business and Professions Code of California;
  - o Title 16, California Code of Regulations;
  - o California Health and Safety Code;
  - o California Penal Code;
  - o California Welfare and Institutions Code;
  - o California Family Code;
  - o California Corporations Code;

# Respondent's Response

**From:** Walton, Briseida (POL)  
**Sent:** Wednesday, February 22, 2023 10:58 AM  
**To:** SOTF, (BOS)  
**Cc:** Toomey, William (POL)  
**Subject:** RE: SOTF - Complaint Filed with the Sunshine Ordinance Task Force - File No. 23013(E)  
**Attachments:** SOTF File 23013(E) - 2023.02.23 SFPD Response.pdf

Good morning,

In response to SOTF file no. 23013(E): Complaint filed by Complaint filed by Chris Ward Kline against the SF Police Department for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b),(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner, please see attached documents.

Thank you.

Sincerely,

Briseida Walton  
San Francisco Police Department | Legal Division  
1245 3rd Street  
San Francisco, CA 94158  
Desk: 415.837.7180  
Email: [briseida.walton@sfgov.org](mailto:briseida.walton@sfgov.org)

Notice: The information contained in this electronic message may be confidential and may be subject to the attorney-client privilege and/or the attorney work product doctrine. It is intended only for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, you are hereby notified that any use, dissemination or copying of this communication is strictly prohibited. If you have received this electronic message in error, please delete the original message from your e-mail system. Thank you.

**From:** SOTF, (BOS) <[sotf@sfgov.org](mailto:sotf@sfgov.org)>  
**Sent:** Wednesday, February 15, 2023 4:16 PM  
**To:** Toomey, William (POL) <[William.Toomey@sfgov.org](mailto:William.Toomey@sfgov.org)>  
**Cc:** [ckblueaqua@gmail.com](mailto:ckblueaqua@gmail.com) <[ckblueaqua@gmail.com](mailto:ckblueaqua@gmail.com)>  
**Subject:** SOTF - Complaint Filed with the Sunshine Ordinance Task Force - File No. 23013(E)

Good Afternoon:

The Police Department has been named as a Respondent in the attached complaint filed with the Sunshine Ordinance Task Force (SOTF). In an effort to provide the SOTF information in an easy to understand format the SOTF has prepared a revised request format for responding to complaints (attached). **The SOTF requests that you submit your response to our office the allegations including any and all supporting documents, recordings, electronic media, etc., to the Task Force within five (5) business days of receipt of this notice.** In developing and submitting your response, please use the attached instructions, "Preparing San Francisco Sunshine Ordinance Task Force Respondents Materials," to address your defense of this complaint.

This is your opportunity to provide a detailed explanation to allow the Task Force to be fully informed in considering your response prior to the meeting.

Please refer to the File Number 23013(E ) when submitting any new information and/or supporting documents pertaining to this complaint.

Cheryl Leger

Assistant Clerk, Board of Supervisors

Tel: 415-554-7724



Click to complete a Board of Supervisors Customer Service Satisfaction form.

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*



CITY AND COUNTY OF SAN FRANCISCO  
**POLICE DEPARTMENT**  
HEADQUARTERS  
1245 3<sup>RD</sup> Street  
San Francisco, California 94158



**LONDON N. BREED**  
MAYOR

**WILLIAM SCOTT**  
CHIEF OF POLICE

February 22, 2023

Via email [sotf@sfgov.org](mailto:sotf@sfgov.org)

Sunshine Ordinance Task Force  
1 Dr. Carlton B. Goodlett Place, City Hall, Room 244  
San Francisco, CA 94102.

Re: Complaint No. 23013(E) - filed by Chris Ward Kline against the Police Department

Dear Sunshine Ordinance Task Force:

The San Francisco Police Department (SFPD) is in receipt of the Complaint filed by Chris Ward Kline against the SF Police Department for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

SFPD takes responsibility for not providing a response in a timely manner. On September 26, 2022, SFPD responded to Complainant's Public Records request (reference # P084503-091622), dated September 16, 2022, by mistakenly sending Complainant an extension letter instead of SFPD's Response letter. We realized the oversight upon receiving SOTF Complaint 23013(E). On February 16, 2023, SFPD apologized for the oversight and sent Complainant the letter we intended to provide on September 26, 2022, via email [CKBlueaqua@gmail.com](mailto:CKBlueaqua@gmail.com).

SFPD submits the following supporting documents to the Sunshine Ordinance Taskforce for your consideration:

**Attachment 1**

- 1) SFPD response letters for Reference # P084503-091622
- 2) Public Records request, dated September 16, 2022

Thank you for your courtesy in this regard.

Sincerely,

Lieutenant William Toomey # 1262  
Risk Management - Legal Division



CITY AND COUNTY OF SAN FRANCISCO  
POLICE DEPARTMENT  
HEADQUARTERS  
1245 3<sup>RD</sup> Street  
San Francisco, California 94158



LONDON N. BREED  
MAYOR

WILLIAM SCOTT  
CHIEF OF POLICE

September 26, 2022

*Via email CKBlueaqua@gmail.com*

Chris Ward Kline  
237 Kearny Street Apt 104  
San Francisco, CA 94108

RE: Public Records Request, dated September 16, 2022, Reference # P084503-091622

Dear Chris Ward Kline:

The San Francisco Police Department (SFPD) received your Public Records Act request, dated September 16, 2022.

You requested, “*From: Chris K.  
Sent: Tuesday, September 13, 2022 4:19 PM  
To: Breed, Mayor London (MYR) ; Colfax, Grant (DPH) ; Walton, Shamann (BOS) ; Peskin, Aaron (BOS)  
Cc: SFPD, Chief (POL) ; Pojman, Natalie (DPH) ; Varisto, Michaela (DPH)  
Subject: Department of Emergency Management Response*

*This message is from outside the City email system. Do not open links or attachments from untrusted sources.*

*Good evening,*

*Department of Emergency Management Response denies and record within 72 hours or request.*

*It should be noted that on a SF govt website, the partner agencies list was changed by IT and an appropriate list of previous and new are recorded which points to obstruction.*

*I will be asking for a complete list and once again, I respectfully request the documents from Public Health, and any/all agencies that have record that include but not limited to:*

*‘Electronic Surveillance (ELSUR) indices, the Microphone Surveillance (MISUR) indices, the Physical Surveillance (FISUR) Indices, and the Technical Surveillance (TESUR) Indices, for both main file records and cross reference files’.*

*Respectfully,*

*Chris Ward Kline."*

**SFPD Response:**

A public records request must specify an identifiable record or category of records sought, Cal Govt. Code § 6253(b). SFPD is more than happy to assist you in identifying documents, but a request must be sufficiently clear and defined to enable SFPD to understand what records are the subject of the request.

At this time, SFPD has determined that your request does not meet the legal definition under Cal Govt. Code § 6253(b).

If you have any questions, please contact the Legal Division at (415) 837-7394.

Thank you for your courtesy in this regard.

Sincerely,

Lieutenant William Toomey # 1262  
Risk Management - Legal Division



CITY AND COUNTY OF SAN FRANCISCO  
POLICE DEPARTMENT  
HEADQUARTERS  
1245 3<sup>RD</sup> Street  
San Francisco, California 94158



LONDON N. BREED  
MAYOR

WILLIAM SCOTT  
CHIEF OF POLICE

September 26, 2022

*Via email CKBlueaqua@gmail.com*

Chris Ward Kline  
237 Kearny Street Apt 104  
San Francisco, CA 94108

RE: Public Records Request, dated September 16, 2022, Reference # P084503-091622

Dear Chris Ward Kline:

The San Francisco Police Department (SFPD) received your Public Records Act request, dated September 16, 2022.

You requested, *"From: Chris K.*

*Sent: Tuesday, September 13, 2022 4:19 PM*

*To: Breed, Mayor London (MYR) ; Colfax, Grant (DPH) ; Walton, Shamann (BOS) ; Peskin, Aaron (BOS)*

*Cc: SFPD, Chief (POL) ; Pojman, Natalie (DPH) ; Varisto, Michaela (DPH)*

*Subject: Department of Emergency Management Response*

*This message is from outside the City email system. Do not open links or attachments from untrusted sources.*

*Good evening,*

*Department of Emergency Management Response denies and record within 72 hours or request.*

*It should be noted that on a SF govt website, the partner agencies list was changed by IT and an appropriate list of previous and new are recorded which points to obstruction.*

*I will be asking for a complete list and once again, I respectfully request the documents from Public Health, and any/all agencies that have record that include but not limited to:*

*'Electronic Surveillance (ELSUR) indices, the Microphone Surveillance (MISUR) indices, the Physical Surveillance (FISUR) Indices, and the Technical Surveillance (TESUR) Indices, for both main file records and cross reference files'.*

*Respectfully,*

*Chris Ward Kline"*

SFPD is invoking the extension of time to respond to your request pursuant to Government Code section 6253(c) due to the need to search and review our records. Once it has been determined whether the information you request is available, we will advise you within 14 days, but no later than October 10.

If you have any questions, please contact the Legal Division at (415) 837-7394.

Thank you for your courtesy in this regard.

Sincerely,

Acting Lieutenant Walter Ware # 66  
Risk Management - Legal Division

# Public Records Request (P084503-091622)

## ▼ Public Records Request Details

---

Department: Legal

Category of Records: Public Records Request

Describe the Record(s)  
Requested:

From: Chris K.  
Sent: Tuesday, September 13, 2022 4:19 PM  
To: Breed, Mayor London (MYR) ; Colfax, Grant (DPH) ; Walton, Shamann (BOS) ; Peskin, Aaron (BOS)  
Cc: SFPD, Chief (POL) ; Pojman, Natalie (DPH) ; Varisto, Michaela (DPH)  
Subject: Department of Emergency Management Response

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Good evening,

Department of Emergency Management Response denies and record within 72 hours or request.

It should be noted that on a SF govt website, the partner agencies list wss changed by IT and an appropriate list of previous and new are recorded which points to obstruction.

1008

I will be asking for a complete list and once again, I respectfully request the documents from Public Health, and any/all agencies that have record that include but not limited too:

'Electronic Surveillance (ELSUR) indices, the Microphone Surveillance (MISUR) indices, the Physical Surveillance (FISUR) Indices, and the Technical Surveillance (TESUR) Indices, for both main file records and cross reference files'.

Respectfully,

Chris Ward Kline

Incident Number: *if known*  
Police Officer(s) Involved: *if known*  
Time of Incident: *specify AM or PM, if known*  
Date Range From: *if applicable*  
Date Range To: *if applicable*

Preferred Method to Receive  
Records:

Electronic via Records Center

▼ **Public Records Archive Summary**

---

Will you post this request to the  
online archive?:

➤ **Create an Activity to Retrieve Records**

---

➤ **Send for Review**

---

➤ **Time Extension**

---

➤ **Denials, Exemptions & Redaction Codes**

---

➤ **Cost Estimate/Payment Details**

---

➤ **Clarification**

---

➤ **Trending -- Internal Use Only**

---

➤ **Notes**

---

➤ **Message History**

---

➤ **Request Details**

---

**From:** SOTF, (BOS)  
**Sent:** Wednesday, February 15, 2023 4:17 PM  
**To:** Toomey, William (POL)  
**Cc:** ckblueaqua@gmail.com  
**Subject:** SOTF - Complaint Filed with the Sunshine Ordinance Task Force - File No. 23013(E)  
**Attachments:** SOTF - Complaint Procedure 2019-10-02 FINAL.pdf; Preparing SOTF Respondent Materials FINAL for PILOT.pdf; 23013 A-E Complaint.pdf; Affirmation Letter 23013 (E).pdf

Good Afternoon:

The Police Department has been named as a Respondent in the attached complaint filed with the Sunshine Ordinance Task Force (SOTF). In an effort to provide the SOTF information in an easy to understand format the SOTF has prepared a revised request format for responding to complaints (attached). **The SOTF requests that you submit your response to our office the allegations including any and all supporting documents, recordings, electronic media, etc., to the Task Force within five (5) business days of receipt of this notice.** In developing and submitting your response, please use the attached instructions, "Preparing San Francisco Sunshine Ordinance Task Force Respondents Materials," to address your defense of this complaint. This is your opportunity to provide a detailed explanation to allow the Task Force to be fully informed in considering your response prior to the meeting.

Please refer to the File Number 23013(E) when submitting any new information and/or supporting documents pertaining to this complaint.

Cheryl Leger  
Assistant Clerk, Board of Supervisors  
Tel: 415-554-7724



Click to complete a Board of Supervisors Customer Service Satisfaction form.

[The Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*

SUNSHINE ORDINANCE TASK FORCE

Tel: 415 554-7724  
Fax: 415 554-7854  
TDD/TTY: 415 554-5227



City Hall, Room 244  
1 Dr. Carlton B. Goodlett Place  
San Francisco 94102-4689

February 15, 2023

Lt. William Toomey  
Police Department

Re: Sunshine Ordinance Task Force, File No. 23013(E)

Dear Lt. Toomey:

Please review the complaint as described below and acknowledge your department's position on File No. 23013(E) regarding an alleged violation of the Sunshine Ordinance.

**File No. 23013 E** Complaint filed by Chris Ward Kline against A-E SF Police Department (E) e for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

Please choose ONE answer. You may, if you wish, also attach any additional explanation.

- [a] acknowledge noncompliance for all allegations below
- [b] department/agency declares no-contest to all allegations below
- [c] deny one or more allegations below (please state an additional explanation which of the allegations you deny, and supporting evidence and/or argument)

If you or your entity acknowledges noncompliance or declares no-contest, the SOTF may, at its discretion, issue an Order of Determination against you or your entity for the allegations listed above without a hearing, and thereafter refer the matter to the Compliance & Amendments Committee for monitoring as needed.

Please respond within the next five business days of the date on this notice, with your acknowledgment. If it is not received within five business days, we will assume that you have acknowledged no-contest.

Very Truly Yours,

Matthew Yankee, Chair  
Sunshine Ordnance Task Force

MY:cal

cc: Chris Klein, Petitioner

**From:** SOTF, (BOS)  
**To:** Michael Petrelis; Heckel, Hank (MYR); Hussey, Deirdre (DPH); ckblueaqua@gmail.com; Lim, Victor (DEM); Pojman, Natalie (DPH); Miyamoto, Paul (SHF); Toomey, William (POL)  
**Cc:** Young, Victor (BOS); Somera, Alisa (BOS); Calvillo, Angela (BOS)  
**Subject:** SOTF - Notice of Complaint Committee hearing, March 21, 2023 - 5:30 PM; Room 408, City Hall  
**Attachments:** SOTF - Complaint Procedure 2019-10-02 FINAL.pdf

Good Afternoon:

Notice is hereby given that the Complaint Committee of the Sunshine Ordinance Task Force (Task Force) shall hold hearings on complaints listed below to: 1) determine if the Task Force has jurisdiction; 2) review the merits of the complaints; and/or 3) issue a report and/or recommendation to the Task Force. ***Please confirm your attendance for this hearing.***

Date: March 21, 2023

Location: Room 408, City Hall

Time: 5:30 p.m.

Complainants: Your attendance is required for this meeting/hearing.

Respondents/Departments: Pursuant to Section 67.21 (e) of the Ordinance, the custodian of records or a representative of your department, who can speak to the matter, is required at the meeting/hearing.

**File No. 22134** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 22135** Complaint filed by Michael Petrelis against Mayor London Breed for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, by failing to respond to a public records request in a timely and/or complete manner.

**File No. 23013A** Complaint filed by Chris Ward Kline against Department of Public Health for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013B** Complaint filed by Chris Ward Kline against Office of the Sheriff for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013C** Complaint filed by Chris Ward Kline against Mayors Office for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013D** Complaint filed by Chris Ward Kline against Department of Emergency Management for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**File No. 23013E** Complaint filed by Chris Ward Kline against San Francisco Police Department (E) e for allegedly violating Administrative Code (Sunshine Ordinance), Section(s) 67.21, 67.24(b)(o), and 67.25 by failing to respond to a request for public records in a timely and/or complete manner.

**Documentation (evidence supporting/disputing complaint)**

For a document to be considered, it must be received at least five (5) working days before the hearing (see attached Public Complaint Procedure).

For inclusion in the agenda packet, supplemental/supporting documents must be received by **5:00 pm, March 15, 2023**.

Cheryl Leger  
Assistant Clerk, Board of Supervisors  
Tel: 415-554-7724

 Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form.

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

*Disclosures: Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors website or in other public documents that members of the public may inspect or copy.*

