

WRITTEN COMMENTS SUBMITTED TO THE TASK FORCE

APRIL 25, 2022 - SEPTEMBER 26, 2022

| MeetingDate | AgendaItem | Name | Comment |
|----------------|--|----------------|---|
| 5/9/2022 18:00 | PUBLIC COMMENTS - ITEMS NOT ON THE AGENDA | Seth Hall | Thank you to the City of Chula Vista and to Madaffer Enterprises for convening this important task force. As soon as possible, please consider voting on a resolution that reassures the viewing public that the task force chairperson and members have taken control of the task forces agenda. From an outside perspective, it appears so far that the agenda is controlled by a party who is not the chairperson, vice chairperson, or any seated member of the task force. This may have been necessary for the first meeting, but should no longer be the case going forward. In order for the public to have confidence the task force is being properly led by the communitys task force members, the task force must control its own agenda, and accordingly must control the minutes of the task force meeting. Each task force member is attaching their personal name to the work and outcomes of this task force, so each member deserves a fair and formal process for selecting how to spend the time you have. Thank you to each task force member for their volunteer time and attention to the important topic of privacy and surveillance technology. |
| 5/9/2022 18:00 | Presentation on privacy in other California cities | Seth Hall | Thank you to the City for assembling this summary of how so many cities are tackling the challenges of ensuring surveillance technology is operated according to best practices and designed to protect residents from potential abuse. As a member of the TRUST SD Coalitions Steering Committee, working on these same topics in San Diego, I personally would like to add that San Diego is on the cusp of adding a community-led oversight process that is very similar to the one in Oakland, which is summarized in the citys document. Our Privacy Advisory Board received final approval in April. The TRUST Surveillance Oversight ordinance is undergoing labor negotiations and is not far from reaching its final approval. The TRUST SD Coalition only reached this goal by uplifting community voices that have been previously left out. I have enormous optimism that this task force will make recommendations that will rebalance the needs of government with the inalienable rights of residents. While Chula Vista and San Diego are separated by borders on a map, our two cities are profoundly intertwined, and our communities share many fates. As such, the TRUST SD Coalition is advocating for Chula Vista to be represented among the members of San Diegos upcoming Privacy Advisory Board. I hope our cities can be close collaborators in enabling only safe and effective surveillance technology in our region, while we all work to acknowledge and prioritize the fundamental rights of our community members. |
| 6/8/2022 18:00 | Receive and File Meeting Summaries | Margaret Baker | Thank you for providing notes in a timely manner. Here are some changes that would help the general public engage more easily: The agenda item numbers need to be included for each item in the notes. Also, the physical location of each meeting should be included. A link to the post-meeting agenda would facilitate access to public e-comments, attachments and PPT presentations, and video-recordings of the meetings. The background documents and other archived materials for the Task Force are not easy to find. The meeting summaries fail to list former City Manager Gary Halpert who was participating on the dais. Could his role please be clarified in the meeting notes? |
| 6/17/2022 7:00 | | Sandra | This is test from eSCRIBE at 8:42 AM EST |
| 6/17/2022 7:00 | | Sandra | I had the tab open never closed- leaving comment at 9:11 Am EST Comment was supposed to close at 9:00am EST |

| | | | |
|-----------------|-----------------|----------------|---|
| 8/15/2022 18:00 | PUBLIC COMMENTS | Nancy Relaford | <p>This agenda seems like a last minute demolition of both the process and the timeline for the Task Forces work. Where did the idea come from to send barely discussed draft reports to City department heads and key staff for consideration and response at this point in the process, before recommendations have been finalized and submitted to the City Manager for her report to Council?</p> <p>All of the reports posted with the agenda are clearly preliminary and need research and discussion in the next weeks. They are not ready to be vetted for implementation by departments even in the most general sense. As just one example, the Privacy Oversight & Transparency Subcommittee Report draft would benefit from editing and discussion:</p> <p>Disclaimer is used where Policy is meant; both may be needed, but the difference is critical</p> <p>More research is needed into existing legal requirements that the City is already bound to comply with (and whether it is currently in compliance); for example, ALPR operation, privacy policy, and breach disclosure are governed by CA SB-34: Automated license plate recognition systems: use of data.</p> <p>There are many more examples in all of the reports; the point is that these reports are not, and last we heard were not expected to be, complete enough after cursory discussion today to be considered and responded to outside of the Task Force process and original timeline. I trust the Task Force members will push back on this bizarre expectation.</p> |
| 8/15/2022 18:00 | Work Session #3 | Margaret Baker | <p>I am writing to thank Task Force members for their time, expertise, and commitment to set in place processes that will protect the civil liberties and proper governance of technology and data that the City is already using and types and uses going forward. I also am writing in strong opposition to the process proposed for tonight's Work Session. The Task Force should NOT submit the preliminary policy recommendations for consideration by City staff at this time. Community members have not had an opportunity to review them and the draft recommendations do not reflect the community's efforts to provide a process and ordinances to protect civil rights and civil liberties. The stated deadline for the work of the Task Force is already too short, and there is not adequate opportunity for deliberation and robust community input on these important policy provisions.</p> |
| 8/22/2022 18:00 | Work Session #4 | Nancy Relaford | <p>ADD" Any required notifications, policy postings, disclosures, signage, or other actions mandated under State law (e.g. SB-34) or other laws and ordinances must be researched, included in policies, and followed. When in doubt, the City should opt for broader adherence to the spirit of the law or requirement, rather than narrow technical compliance. In addition, Welcoming City criteria must be considered as part of surveillance technology policy and transparency review."</p> <p>Something like this needs to be added to the recommendations. There are very clear requirements for ALPR policy posting and breach notifications spelled out in SB34 and I'm sure other technologies have similar requirements that the city should be in compliance with. The part about the spirit of the law rather than technical compliance would have prevented the City deciding that sharing ALPR with ICE didnt violate state law because it doesn't technically contain PII. That was an extremely narrow and incorrect interpretation.</p> |



April 25, 2022

City of Chula Vista
Technology and Privacy Advisory Task Force
276 Fourth Avenue
Chula Vista, California 91910
Email: privacytaskforce@chulavistaca.gov

RE: Surveillance Technology Ordinance

Dear Members of the Chula Vista Technology and Privacy Advisory Task Force:

I write today on behalf of the Electronic Frontier Foundation (EFF), a California-based nonprofit that advocates for civil liberties as society adopts more and more advanced technologies. Our organization has helped to develop, inform, and enforce municipal surveillance oversight programs across the United States. In my personal capacity, I was recently honored with the San Diego Society of Professional Journalists' Sunshine Award for bringing transparency to the types of surveillance in use across San Diego County.¹

We congratulate the city of Chula Vista for taking this first step towards reviewing surveillance technologies through the lens of privacy. However, more needs to be done. We urge the Task Force to cooperate with local civil rights and social justice organizations to negotiate a robust surveillance oversight ordinance that allows for public involvement and transparency, and that designates the power of final approval of technology acquisitions and policies to elected officials.

Too often, public safety agencies acquire powerful technologies after closed-door conversations with vendors, shutting the community out of discussions that will have a significant impact on their rights. Privacy, civil rights, and individual freedoms are often either an afterthought for officials or seen as a hindrance to investigations, when in reality addressing these issues is a crucial element to public safety and maintaining a healthy relationship between the government and its constituents. Without proper deliberation and safeguards, surveillance technology can have a number of deleterious effects, including misuse, racial and socio-economic bias, over-policing, and waste of public

¹ Fraley, Malaika. "EFF Director of Investigations Dave Maass Honored With Sunshine Award For Driving Public Disclosure of Government Surveillance Records." Electronic Frontier Foundation. March 23, 2022. <https://www.eff.org/deeplinks/2022/03/eff-director-investigations-dave-maass-honored-sunshine-award-driving-public>

funds.

In recent years, the Chula Vista Police Department (CVPD) has adopted sophisticated surveillance technologies that have proven controversial and damaging to community relations. Of these, one of the most troubling has been the use of automated license plate readers to collect data on drivers, which CVPD was found to have shared with immigration enforcement agencies in apparent violation of multiple state laws.²

CVPD has also deployed the "Drones as First Responders" program, an unorthodox system at odds with commonly accepted use across the United States. While many police agencies use drones sparingly for emergency situations, swat operations, or documenting crime scenes, CVPD has deployed drones more than 10,000 times to respond to routine calls for service, including a variety of low-level incidents such as vandalism and people sleeping in public.³⁴ In fact, welfare checks and psychological evaluations accounted for 19% of drone-involved cases—incidents that social workers and mental health professionals would be better suited to address than remote-controlled police robots. If a member of the community were to read CVPD's formal policy for Unmanned Aerial System (UAS) Operations, they would discover a bare, 2½-page document generated by the company Lexipol.⁵ They would not get a clear understanding of how the program works or what safeguards are in place. In addition, *Voice of San Diego* raised legitimate questions about the relationship between CVPD officers and the drone vendor, which has resulted in an employment "revolving door."⁶

CVPD has been planning to build a real-time crime center (RTCC), a surveillance facility that would allow police to analyze and combine data from a large variety of sources, including drones and license plate readers.⁷ This model of policing, pushed by vendors with much to gain, should raise red flags for public officials, especially without strong

² Solis, Gustavo. "Chula Vista gives immigration officials, others access to license plate reader data." San Diego Union-Tribune. Dec. 6, 2020.

<https://www.sandiegouniontribune.com/communities/south-county/chula-vista/story/2020-12-06/chula-vist-a-gives-immigration-officials-others-access-to-license-plate-reader-data>

³ Chula Vista Police Department. "Drone Program." Retrieved April 22, 2022.

<https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program>

⁴ Mejias Pascoe, Sophia. "Police Drone Footage Is Off Limits – Unless This Legal Challenge Takes Flight." *Voice of San Diego*. May 5, 2021.

<https://voiceofsandiego.org/2021/05/05/police-drone-footage-is-off-limits-unless-this-legal-challenge-takes-flight/>

⁵ Chula Vista Police Department. "Policy 613: Unmanned Aerial System (UAS) Operations." February 20, 2020. <https://www.chulavistaca.gov/home/showpublisheddocument/16381/637178753321100000>

⁶ Mejias Pascoe, Sophia. "Chula Vista PD's Drone Program Opened a Revolving Door for Officers." *Voice of San Diego*. April 6, 2021.

<https://voiceofsandiego.org/2021/04/05/chula-vista-pds-drone-program-opened-a-revolving-door-for-officer-s/>

⁷ Marx, Jesse. "Chula Vista Is Building a Real-Time Crime Center." *Voice of San Diego*. Sept. 2, 2021.

<https://voiceofsandiego.org/2021/09/02/chula-vista-is-building-a-real-time-crime-center/>

RE: Surveillance Technology Ordinance
April 25, 2022
Page 3 of 3

controls grounded in community input. Such a center would supercharge privacy-invasive surveillance, without commensurate improved oversight.

The Task Force has quite the task ahead of you, but by promoting an ordinance that is inclusive of communities and permanently shifts power to elected officials, the city of Chula Vista will be better suited to balance public safety with privacy and civil liberties.

Best regards,

Dave Maass
Director of Investigations
Electronic Frontier Foundation

Nancy Relaford
nrelaford@
gmail.com

Chula Vista Privacy Task Force first meeting 4/25/22, 6pm

Nancy:

Hello, my name is Nancy Relaford, I'm a member of the Ad Hoc STOP CV Surveillance group and of Showing Up for Racial Justice - SURJ San Diego.

Reading your biographies this morning gave me real hope for the work of this task force. Thank you all for being willing to serve.

As the Task Force examines the city's use of technology and its implications for privacy, we ask that you keep a strong focus on **surveillance** technologies, which carry unique risks to individual privacy and civil rights.

As others have mentioned, there are serious concerns about Chula Vista's surveillance technology programs, including drones and automated license plate recognition, ALPR.

Perhaps most troubling is the city's persistent failure to protect the sensitive personal data that these technologies massively collect, retain, aggregate, and make available to outside entities, including for-profit companies and government agencies. Data that over time create intimate searchable records of not only who we are, but where we live, travel, assemble, worship, and with whom we associate.

Surveillance technology can and does negatively impact the privacy, free movement and other civil rights and liberties of community members, and undermines community trust and safety. Any benefits or efficiencies of its use must be balanced against these risks, with strong policies, ongoing independent oversight, and public accountability built in.

Historically, surveillance has been used to intimidate and control some communities and groups more than others. The communities and activities most impacted by systemic racism and overpolicing are also the most impacted by surveillance technology. The risks are not equally distributed, and the most vulnerable members of the community must be heard as you consider technology safety and privacy.

In formulating our "Surveillance and Community Safety Ordinance," we have worked in coalition and consultation with organizations representing immigrant, BIPOC, LGBTQ+, unhoused, racial justice, and faith communities, as well as experts in privacy rights, technology & legal issues.

We are asking the Task Force to adopt this surveillance technology ordinance, which includes provisions for:

- Informed public debate at the earliest stage of the process
- Determination of whether benefits outweigh costs and concerns
- Establishment of a thorough surveillance use policy

- Ongoing independent oversight and accountability

We are counting on you, the members of this Task Force, to thoroughly examine and articulate the complex and unique privacy risks of **surveillance technology**, and to actively welcome all community voices into the discussion. We hope to see a commitment to transparency, two-way communication, and community outreach in all phases of your work. We look forward to presenting our draft ordinance to the Task Force and discussing these issues with you in more detail. Thank you.

April 25, 2022

To: Technology and Privacy Advisory Task Force Members

Re: Need for a Surveillance and Community Safety Ordinance in Chula Vista

Congratulations on your appointment to the newly formed Technology and Privacy Advisory Task Force.

We, the undersigned community, civil rights, and service organizations are writing to highlight the urgent need for a surveillance technology and privacy ordinance in the City of Chula Vista. For over a year, we have been voicing our concerns and studying best practices in cities, like the City of San Diego, that also face challenges associated with the increased use of surveillance technology. We have developed an ordinance based on our research, and ask you to build on our proposed Surveillance and Community Safety Ordinance and recommend its adoption by the Chula Vista City Council.

Surveillance technology carries inherent risks to individual privacy, civil rights, and civil liberties that must be protected by enforceable ordinances, consistent policies and practices, and independent oversight. Transparency, accountability, and oversight of police and governmental use of surveillance technology cannot simply be left implicit within broad technology policy or subsumed within a general set of privacy policies covering less intrusive technologies. Surveillance technology includes not just technology capable of accessing information, but also technology systems that are capable of aggregating information from both public and non-public sources. Such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations. We ask that you address the special risks associated with current and potential uses of surveillance technology and data in all phases of your information-gathering and deliberation process, and that you prioritize an enforceable ordinance as part of the technology privacy policy package ultimately proposed by the Task Force and adopted by the City of Chula Vista.

The City of Chula Vista takes great public pride in the steps it has taken to achieve its status both as a Welcoming City and as a Smart City. Surveillance technology offers potential benefits for certain efficiencies in government and law enforcement, but it can also negatively impact the privacy, free movement and other civil rights and liberties of community members, and undermine community trust and safety. Historically, surveillance has been used to intimidate and control certain communities and groups more than others. As a Welcoming City, Chula Vista must do more to protect the civil liberties, rights and safety of all.

Investigative reporting in local and national media has raised awareness and revealed serious concerns about lack of transparency, accountability, and oversight of Chula Vista's surveillance programs. Instead of learning from our city officials that CVPD shared our ALPR data with ICE, CBP, and other federal agencies for over three years, we have been shocked to learn about such practices through outside sources. Further, we have been frustrated by the City's handling of these revelations and the resulting scrutiny. Rather than acting swiftly to acknowledge and

Re: Need for a Surveillance and Community Safety Ordinance in Chula Vista, April 25, 2022

correct the mistakes, establish independent oversight, and repair damaged community relationships, Chula Vista city officials have continued to prioritize and expand police surveillance programs despite concerted public opposition. These events have revealed larger issues regarding lack of open government, trust and safety that affect all members of our community, and especially the most marginalized. The lasting harm to community trust in Chula Vista caused by the City's failure to exercise accountability and full transparency regarding its surveillance technology programs cannot be overstated.

Formation of the Task Force gives us renewed hope for genuine engagement with community groups and for demonstrated commitment to the values we share and which stand at the core of the "Welcoming City" model. We expect and demand that Chula Vista meet a high standard of accountability, transparency, community consultation, and open governance.

Members of our organizations possess relevant lived experience, professional knowledge, and other types of expertise. In writing our Surveillance and Community Safety Ordinance for Chula Vista, we drew upon a readily available body of expert knowledge as well as a number of existing ordinances in California cities. Our draft ordinance includes these main features:

- A detailed, enforceable process for all phases of the approval, acquisition, use, and oversight of all city surveillance technology
- Parameters for formation of an independent civilian body to oversee this process and make informed recommendations to the City Council
- Provisions for:
 - Informed public debate at the earliest stage of the process
 - Determination of whether benefits outweigh costs and concerns
 - Establishment of a thorough surveillance use policy
 - Ongoing independent oversight and accountability

We look forward to discussing this with you in more detail as the Task Force carefully considers our proposed Surveillance and Community Safety Ordinance. An electronic version of this letter including a link to the Ordinance will be sent to the Task Force via email.

A Smart City must constantly anticipate and mitigate the unique and evolving risks associated with surveillance technology, and a Welcoming City must always prioritize and protect its community members' rights and privacy. We stand ready to work with you in the coming months as the Task Force tackles these complex issues and proposes policies to protect and provide real safety for all community members.

Thank you for your consideration.

Sincerely yours,

Ad Hoc STOP Chula Vista PD Surveillance group
STOPCVSurveillance@gmail.com

Re: Need for a Surveillance and Community Safety Ordinance in Chula Vista, April 25, 2022

Supporting Organization Signatories

Advancing Students Forward

AFT 1931 Local - Immigrant Student Support Committee

Alliance of Californians for Community Empowerment - ACCE

Border Angels

Change Begins With ME

Espacio Migrante

Indivisible San Diego Persist

Oakland Privacy

Pillars of the Community

Rise Up San Diego

San Diego Immigrant Rights Consortium

Secure Justice

Showing Up for Racial Justice - San Diego (SURJ-SD)

South Bay People Power

Take Action San Diego

Tech Lead San Diego

Tech Workers Coalition San Diego

Think Dignity

USD Center for Digital Civil Society

USD Immigration Law Society

USD Values Institute

US-Mexico Border Program, American Friends Service Committee

We The People SD

Surveillance & Community Safety Ordinance

April 25, 2022

ORDINANCE ADDING CHAPTER 10 TO THE CHULA VISTA MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Chula Vista's ("City") acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF CHULA VISTA DOES ORDAIN AS FOLLOWS:

SECTION 1. This Ordinance shall be known as the Surveillance and Community Safety Ordinance.

SECTION 2. Chula Vista Municipal Code Chapter 10, is hereby added as set forth below (chapter and section numbers are indicated in **bold type**).

Chapter 10 REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

10.010. DEFINITIONS. The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "City" means any department, agency, bureau, and/or subordinate division of the City of Chula Vista as provided by Chapter [placeholder] of the Chula Vista Municipal Code.

3. "City staff" means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.

4. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.

5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a 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 City business.

7. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

8. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

9. "Surveillance technology" means any software, electronic device, system utilizing an electronic device, or similarly used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or

similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast and or predict criminal activity or criminality, biometric identification hardware or software.

A. "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

- 1). Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;
- 2). Parking Ticket Devices (PTDs);
- 3). Manually-operated, non-wearable, handheld digital 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;
- 4). Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- 5). Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- 6). City databases 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.
- 7). Medical equipment used to diagnose, treat, or prevent disease or injury.
- 8). Police department interview room cameras.
- 9). Police department case management systems.
- 10). Police department early warning systems.
- 11). Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

11. "Surveillance Impact Report" means a publicly released written report including at a minimum the following:

- A. **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
- B. **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
- C. **Location:** The location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
- D. **Impact:** An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;
- E. **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
- F. **Data Types and Sources:** A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
- G. **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
- H. **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
- I. **Third Party Dependence:** 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;
- J. **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
- K. **TrackRecord:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse

information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

12. "Surveillance Use Policy" means a publicly released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

- A. **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
- B. **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;
- C. **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;
- D. **Data Access:** The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- E. **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
- F. **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), 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;
- G. **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
- H. **Third Party Data Sharing:** If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- I. **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
- J. **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use 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 legally enforceable sanctions for violations of the policy; and

- K. **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

10.020 Privacy Advisory Commission (PAC) Notification and Review Requirements

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

- A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
- 1). Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - 2). Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.
- B. Upon notification by City staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, City staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to 10.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify the proposal, or take no action.
- C. Should the Privacy Advisory Commission not make a recommendation pursuant to 10.020.1.B, City staff may proceed and seek Council Approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section 10.030.

2. PAC Review and Approval Required for New Surveillance Technology Before City Council Approval

- A. Prior to seeking City Council approval under Section 10.030. City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review and approval at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 10.010.
- B. The Privacy Advisory Commission shall approve, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to City staff. City staff shall present such modifications to the Privacy Advisory Commission for approval before seeking City Council approval under Section 10.030.

- C. Failure by the Privacy Advisory Commission to make a determination on a presented item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.
 - D. City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.
3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval
- A. Prior to seeking City Council approval for existing City surveillance technology under Section 10.030. City staff shall submit a Surveillance Impact Report and Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 10.010..
 - B. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.
 - C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
 - D. Within sixty (60) days of the Privacy Advisory Commission's action in 10.020.1.C. City staff shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.
 - E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff to proceed to the City Council for approval of the item pursuant to Section 10.030..

10.030. City Council Approval Requirements for New and Existing Surveillance Technology.

- 1. City staff must obtain City Council approval prior to any of the following:
 - A. Accepting state or federal funds or in-kind or other donations for surveillance technology;
 - B. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
 - C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or

- D. Entering into a continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
- E. Notwithstanding any other provision of this section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process

- A. After the PAC Notification and Review requirements in Section 10.020. have been met, City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Impact Report and proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.
- B. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.
- C. For Approval of Existing Surveillance Technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 10.020.3.E, if the City Council has not reviewed and approved such item within four City Council meetings from when the item was initially scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 10.020.A.1

10.035. Use of Unapproved Technology during Exigent Circumstances or Large-Scale Event

- 1. City staff may not temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy.

10.040. Oversight Following City Council Approval

1. On March 15th of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must present a written Annual Surveillance Report for Privacy Advisory Commission review for each approved surveillance technology item. If City staff is unable to meet the March 15th deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.

B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding Surveillance Use Policy that will resolve the concerns.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the Annual Surveillance Report.

D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 10.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

2. Based upon information provided in City staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 10.030 and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

10.050. Enforcement

1. Violations of this article are subject to the following remedies:

A. Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective City department, and the City of Chula Vista, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.

- B. Persons subjected to surveillance technology in violation of this ordinance shall be notified through mail within 10 days of confirmation that their information has been obtained, retained, accessed, shared or used in violation of this ordinance.
- C. Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in the Superior Court of the State of California against the City of Chula Vista and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater).
- D. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in; an action brought under paragraphs (A) or (B).
- E. Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

10.060. Secrecy of Surveillance Technology

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

10.070. Whistleblower Protections.

1. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

- A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
- B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.

2. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under this Ordinance.

3. Any employee or applicant who is injured by a violation of this section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

SECTION 3. Existing Surveillance Use Policies for the Domain Awareness Center, Forward Looking Infrared Thermal Imaging Camera System, and Cell Site Simulator, Must Be Adopted as Ordinances.

Within 180 days of the effective date of this ordinance, City staff shall return to City Council with an ordinance or ordinances adopting and codifying any existing surveillance use policies under the Chula Vista Municipal Code but only after proper PAC and City Council review of all existing surveillance use policies, incorporating 15-day public notice period in each instance to allow for public awareness.

SECTION 4. Severability. If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

SECTION 5. Effective Date. This ordinance shall become effective immediately on final adoption if it receives four or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

CIVIC SUCCESS PUBLIC SERVICE AT ITS BEST

SUMMARY

The mission of the San Diego County Grand Jury (Grand Jury) is to represent the citizens of San Diego County by investigating, evaluating, and reporting on the actions of local governments and special districts. In fulfilling this mission, the 2021/2022 San Diego County Grand Jury has investigated numerous citizen complaints regarding the operation of various public agencies. Some of these investigations may result in the issuance of Grand Jury reports containing recommendations for improving the performance within those entities. Occasionally, while performing its general oversight responsibilities, the Grand Jury discovers noteworthy examples of community service by public agencies and issues a commendation.

In this report, the Grand Jury recognizes the following San Diego County agencies for their contributions to the community:

- Chula Vista Police Department-Drone as First Responders
- La Mesa Homeless Outreach and Mobile Engagement (HOME)

INTRODUCTION

The Grand Jury ordinarily reports the results of its investigations together with recommendations to the public agencies or special districts studied. The 2021/2022 San Diego County Grand Jury has found that the performance of the subjects of investigation in the above mentioned three programs has been commendatory and worthy of public recognition as *Civic Successes ~ Public Service at its Best*.

PROCEDURES

During its studies, the Grand Jury conducts interviews with representatives of the entity under investigation and others with knowledge about the issues, actions, and circumstances involved. The Grand Jury may also collect documentary information relevant to the study from all available sources. Site visits are made when appropriate. All information gathered is carefully weighed by the Grand Jury.

CHULA VISTA POLICE DEPARTMENT DRONE AS FIRST RESPONDERS

DISCUSSION

The Chula Vista Police Department Drone as First Responder (DFR) program operates drones to investigate, provide airborne support, decrease response times, preserve the peace, and provide real-time information to responding officers before they arrive on scene. In some cases, the use of drones eliminates the need to dispatch patrol units. The program has been operating since 2018 and has expanded to cover the entire city of Chula Vista. With over 10,000 responses since its inception, the DFR program has reduced response times, improved police interactions, and increased public safety for the City of Chula Vista.

The City of Chula Vista laid the groundwork for the DFR program beginning in 2016 when they began looking into utilizing drones. The CVPD met with the ACLU twice in the Spring of 2016 for evaluation of the program's privacy protections.

The Federal Aviation Administration (FAA) selected Chula Vista in 2017 as one of ten test sites nationwide—and the only law enforcement agency—to beta test the UAS Integration Pilot Program, a piloted drone program aimed at integrating drones into the national air space.

In October 2018, the Chula Vista Police Department officially started the DFR program. The DFR program protects the privacy of Chula Vista residents by only launching drones in response to 911 calls; the drones do not patrol. These drones do not enter areas where citizens have an expectation of privacy, such as buildings or fenced yards, except with a duly executed warrant or in an emergency. On the drone's return flight to the launch area, the cameras are stowed horizontally and are not recording video footage.

Each drone has a high-definition digital video camera. The drones weigh less than fifty-five pounds each, are battery operated, and have several rotors like a helicopter. A pilot on the ground operates the drone remotely, using a handheld controller. The pilot also communicates with officers in the field to give them information and tactical intelligence about the situation they are responding to.

CVPD received a waiver from the FAA to fly beyond visual line of sight (BVLOS) in May 2019. The BVLOS waiver increases the range from the launch sites from one mile to up to three miles in any direction within city limits, significantly increasing the service area. CVPD also was the first in the nation to obtain a two-to-one waiver, which allows it to launch two drones from each location, increasing coverage for the community and first responders.

The initial launch site was the roof of the Chula Vista Police Department building. Chula Vista added an additional launch site on the roof of the Paradise Valley Hospital in August 2019. This site is approximately two miles south of the police department headquarters and allows the drones to cover the entire western portion of the city. CVPD subsequently added two additional launch sites at Southwestern College and Ayers Hotel in the eastern parts of the city. With the addition of these new launch sites, the DFR program now has city-wide coverage, except for the area over Brown Field.

The CVPD entered into a Subscription Services Agreement with Motorola Solutions in February 2020; the agreement covers the products and services offered by Motorola in connection with CVPD's DFR program. The Grand Jury is aware that members of the public have raised concerns regarding this agreement, but the Grand Jury did not investigate and takes no position on those concerns in this report.

The drones have responded to over 10,000 separate emergencies from October 2018 through March 2022. Drones as first responders reduce the response time for emergencies and improve

the officers' decision making by providing real-time information to the officers before they arrive on scene. As of March 2022, the DFR program has prevented the need for dispatching a patrol unit over 2,500 times.

The Grand Jury commends the Chula Vista Drone as First Responder program for its valuable contributions to law enforcement and for improving the safety of the citizens of Chula Vista.

LA MESA HOMELESS OUTREACH AND MOBILE ENGAGEMENT (HOME)

DISCUSSION

There are many city and county departments as well as numerous private and non-profit groups trying to solve the problems of homelessness in San Diego. The Grand Jury interviewed the leaders of city and county agencies, faith-based organizations, philanthropies, and non-profits, and evaluated their websites. The Grand Jury discovered that the La Mesa HOME program included specific goals and plans, detailed who was responsible for implementation, clearly cited the timeline for the deliverables, and provided a metric for how their success would be measured.

The La Mesa City Council created a Citizen Task Force on Homelessness in July 2019 to better connect those experiencing homelessness with existing County services. This group was made up of representatives from Alvarado Parkway Institute, Regional Task Force on Homelessness (RTFH), Interfaith Shelter, The Salvation Army, Crisis House, Home Start, Sharp Grossmont Hospital, the County of San Diego, People Assisting the Homeless (PATH), and others. At task force meetings, the service providers shared their experiences and challenges with providing homeless and mental health services in La Mesa and the region. The Citizen Task Force then created recommendations that were grouped by In-Program Service Areas, Description of Activity, Potential Funding Sources, Responsible Agency, and Strategies/Five Year Goals. Concurrently, the city sought input from the police department. The HOME team would use techniques designed to reduce trauma and harm with the goal of decreasing interventions by police officers.

In September 2020, the City issued a recommendation that the HOME pilot program be created. This plan included fiscal impact, alternative models, a detailed program including phases, and next steps to achieve their four goals (see Appendix 1):

- Enhance the City's public communication and coordination related to the homeless.
- Improve the City's ability to prevent homelessness, provide direct outreach to the homeless population, address public safety, and respond to nonemergency calls for service.
- Expand the City's ability to connect homeless residents to transitional and permanent housing opportunities.
- Identify viable one-time and ongoing grant funding opportunities.

This program was subsequently adopted. As a result, the HOME program allows for the

reallocation of sworn officers and PD resources to other aspects of public safety, such as community policing, DUI enforcement, and criminal investigation.

The City of La Mesa Homeless Action Plan is readily accessible on the City's website (<https://www.cityoflamesa.us/1646/HOME-Program>) as well as on social media at <https://www.facebook.com/lamesaca>.

The Grand Jury reviewed the agreement between the City of La Mesa and PATH. La Mesa chose the perfect partner. PATH has a long history of success with the homeless in San Diego and was California's non-profit of the year for Assembly District 78 in 2021. The agreement with PATH contained goals, performance measures, and performance monitoring, along with housing resources and supportive services. According to the Action Plan, "the city will partner with the County, neighboring cities, the Regional Task Force for the Homeless (RTFH), and the East County Homeless Task Force to identify suitable sites, apply for funding, and develop political and community consensus to develop housing. PATH will work with local landlords to identify and create additional housing opportunities in La Mesa." To help prevent inadvertent unintended escalation with uniformed officers, two PATH experts, an outreach technician and a clinical homeless outreach specialist were assigned to La Mesa full time for the pilot year. The program even addressed transportation: the preliminary budget included the purchase of an eight-passenger van for transporting homeless individuals to temporary housing.

The HOME website contains a link to the latest quarterly report. These reports are easy for the public to read, are quite informative, and transparent.

The HOME website also contains email and telephone information for the HOME program so the public can easily report someone experiencing homelessness. The HOME program outreach workers involved businesses by providing contact information to get direct help for the homeless.

The City of La Mesa is in the 2nd year of its pilot program: La Mesa Homeless Outreach and Mobile Engagement (HOME).

The Grand Jury identified the La Mesa HOME program as outstanding in its approach to helping the homeless.

The Grand Jury commends the proactive La Mesa HOME program on its organization, transparency, and publicly available information.

Tech & Privacy TF Comments – 2022-05-09

Item 3. General Public Comment

Good evening! My name is **Margaret Baker**. My time is limited so I'll quickly address the topic of **AGENDA-SETTING & PROPER CONSIDERATION OF OUR PROPOSED ORDINANCE:**

- 1) I'd like to reiterate our Ad Hoc group's request to present our proposed ordinance. I hope you have had a chance to read the letter we also presented that was signed by 26 community and civil rights organizations.
- 2) Your time as a TF is also short, and your task is large. The sooner you consider this concrete ordinance, the better able you will be to interrogate the various tech program managers - and assess the policies currently in place in CV.
- 3) A key component of the ordinance is formation of a community-led independent civilian oversight board – which we see as essential. Our presentation will identify important components and functioning of such a body, based on best practices from model ordinances around the country, in particular, in the City of SD.
- 4) So, tonight I also ask that you invite members of TRUST SD coalition to present directly to you regarding their work. The language in the ordinance to establish a community-led privacy advisory board recently adopted by the City was written by SD TRUST coalition members. We are very fortunate that they are close by and can attend in person and serve as a resource for you.
- 5) For future agendas, we have identified several other experts in the field of tech privacy who we would like included.
- 6) In the rest of my prepared remarks, I raise several other issues regarding meaningful public participation: we request that the complete agenda with PPT or other attachments be posted no later than 5 pm on the Wed prior to Monday evening meetings. It is unacceptable to receive it after close of business on a Friday. This does everyone a disservice.
- 7) Also, the first half hour of your first meeting was inaccessible to community members who tried to tune in. Several dropped off because they couldn't make sense of the meeting and there was no indication that the audio would finally be fixed. Also, posting of the audio file in its entirety did not solve the problem because it is too large.
- 8) For the past 1.5 years, our attempts to engage with the City regarding surveillance issues have been thwarted by numerous technical problems (such as the lack of audio for the first half of the very first meeting of the Tech policy TF). And this glaring lack of technological investment that would allow community members to phone-in comments, to actually hear what is being said in public meetings, etc., is a glaring failure, and ironic for a city that claims to be both "Smart" and "Welcoming." I hope that these barriers will prompt you as a TF to demand a) accessibility to all materials and in a timeframe that allows community participation in the entire process, b) improved two-way communication with the general public during your meetings. The "community" should not be used to provide window-dressing or validation of the process. Openness is NOT just a focus group or a couple of community forums. We want to engage in deliberations with you regarding the future of our city. Please immediately remove the arbitrary limits on public comments, and allow us to be partners in the policy development process.

Thank you.

nrelaford@gmail.
com

Chula Vista Privacy Task Force - Nancy Relaford public comments

Second meeting 5/10/22, 6pm

Hello, my name is Nancy Relaford, I'm a member of the Ad Hoc STOP CV Surveillance group and of Showing Up for Racial Justice - SURJ San Diego.

The public opinion survey and presentation at the last task force meeting raised red flags for me about the underlying agenda and direction of this task force effort. The survey was billed as a "scientific" survey of public opinion. I assumed that as a foundation of the TF's work it would be an objective baseline survey of public opinion and community concerns about technology and privacy.

Instead, the actual purpose of the project seems to have been market research and message testing, specifically looking for current approval for the drone and ALPR programs, and testing (and deploying) certain messages and framings meant to increase public approval especially among less informed respondents. This isn't surprising given that the effort is being led by a PR firm, but it is disappointing and makes me worry for future community outreach. I worry that the end product will be a public relations exercise unless Task Force members question information you're given and take control of the agenda.

This marketing purpose was made abundantly clear in the pollster's narrative presentation of the survey findings, where high approval or acceptance of the city's surveillance programs was consistently characterized with words like: "Good news," "Fortunately," and "Over the moon!" Words used to characterize disapproval rates or privacy concerns include: "only 18%," "a mere 7%," and loaded words like "suspicions," "fears," and "police distrusters." Respondents' privacy concerns expressed as "feel you're being watched" are minimized with the gratuitous editorial comment, "Note that this is more an issue of "feel" than losing actual privacy."

Respondents were fed with potential "benefits" of the drone and ALPR programs in the form of contestable or incomplete assertions presented as facts, while potential "concerns" were prefaced with "Some people say" or "Some people worry." It seems apparent that the goal of the survey exercise was not only testing messages but actively pushing them out to the community. And one of the most telling results of this so-called scientific survey is the finding that "Locating Missing Persons Turns Out to be a Big Selling Point." That says it all.

Several members of the task force asked the pollster probing questions about the survey design and wording that spoke to my own concerns, and I appreciate your diligence. I would urge the task force to continue to examine and question this PR and marketing exercise before basing any of your own discussions or decisions on its assertions. Please do not let this survey go into

the public record unchallenged, and please design authentic outreach, listening, and community participation into the future Task Force forums.

REQUEST TO SPEAK | SOLICITUD PARA DAR TESTIMONIO



DR. ROBERT LEE BROWN
Name | Nombre

Date | Fecha

I do not wish to speak; please register my position on an agenda item for the record.
No deseo hablar: por favor registre mi posición en un asunto de la agenda.

LAW ENFORCEMENT
 SUPPORT | En APOYO
TECHNOLOGY
 OPPOSE | En OPOSICIÓN OR | O Item is NOT on the agenda
Agenda Item No. (Business Items ONLY)
El asunto NO está en la agenda

Número de asunto (Asuntos bajo "Business Items" SOLAMENTE)

FOR LAW ENFORCEMENT

Contact Information (optional) | Información de Contacto (opcional)

SAN DIEGO
City of Residence | Ciudad de Residencia

Representing Myself | A mí mismo
Representando Organization | Organización:
NAACP / URBAN LEAGUE / HOME LAND SECURITY

Address | Domicilio

Email | Correo electrónico

Phone Number | Número de teléfono

Subscribe to email agenda publication notifications.
Suscríbese a notificaciones de publicación de agenda por correo electrónico.

Please submit this request to City Clerk Staff prior to the meeting.
Por favor envíe esta solicitud al personal del secretario de la ciudad antes de la reunión

Comments:

AS A NEIGHBORHOOD COLLABORATOR AND MEDIATOR, I WHOLEHEARTEDLY
ENDORSE AND SUPPORT LAW ENFORCEMENT'S USE OF TECHNOLOGY TO ENSURE
THE SAFETY OF ALL SAN DIEGO COUNTY NEIGHBORHOODS
I AM THE VICE PRESIDENT OF THE S.D. NAACP BOARD MEMBER
OF THE URBAN LEAGUE OF SAN DIEGO COUNTY AND RESEARCHER IN SD SU
CRIMINAL HOME LAND SECURITY - THANK YOU!

Jeremy Ogul

From: Jeremy Ogul
Sent: Monday, August 1, 2022 1:14 PM
To: Jeremy Ogul
Subject: FW: Privacy meetings

From: Jorge Marroquin <[REDACTED]>
Sent: Sunday, July 31, 2022 1:50 PM
To: Adrianna Hernandez <adhernandez@chulavistaca.gov>
Subject: Privacy meetings

Warning:
External
Email

I was unable to attend the meeting due to other commitments but I feel you can't be safe without any type of surveillance equipment, why are residents buying home protection equipment alarms or cameras. If you have some problems with privacy stay home but if you have nothing to hide. Enjoy the extra protection,, this is not big brother this is our elected government protecting all of us. I am a retired MTS rail (trolley) accident investigator and at present all public agencies require some type of surveillance equipment to locate and evidence of the 5% of criminals in our communities.

Present, timed out member of the Chula Vista safety commission. [from the all new AOL app for Android](#)

Jeremy Ogul

From: Margaret Baker [REDACTED]
Sent: Monday, August 1, 2022 1:20 PM
To: Privacy Task Force
Cc: Sophia Rodriguez
Subject: Community's proposed ordinances
Attachments: Revised Privacy Advisory Commission Ordinance_2022-07-15.pdf; Revised Surveillance and Community Safety Ordinance_2022-07-15.pdf

**Warning:
 External
 Email**

Dear Privacy Task Force members,
 I am writing to make sure you each have copies of the ATTACHED community's proposed ordinances, and to request that these two documents be posted as attachments for tonight's Task Force meeting so that the general public can access them.

In addition, I am including the [link to our group's PPT presentation](#) that provides a clear outline of some of the major provisions of these ordinances, specifically, community-led oversight commission, and elements of the Surveillance Impact Reports and Surveillance Usage Policy. We hope that you will carefully review these provisions during your deliberations.

As you know, our community groups have worked diligently to research best practices, discuss options with local community members as well as leaders in cities that have already implemented such ordinances regarding what is needed and what works to protect our privacy. All agree that a community-led process is essential. We feel the city needs to establish BOTH a community-led Privacy Advisory Commission and a Usage Ordinance that establishes processes to codify clear usage policies for each type of surveillance, and to lay out processes for initial and ongoing review of impact and privacy protections, as well as regular reporting that includes provisions for robust community review and comment. We encourage you to start with some basic agreements on definitions, a set of guiding principles, and an outline of components of policy provisions before jumping to votes on details that require more research and consultation. The definitions and provisions included in the Surveillance and Community Safety Ordinance will help you to establish a common language.

Finally, I would like to thank you for your time and commitment to this challenging work, and to encourage you to continue to ask tough questions and to bring in concerns of often-marginalized members of our community about the need for enforceable, transparent civil rights protections in our city.

Sincerely,

Margaret A. Baker, DrPH
 [REDACTED]

South Bay People Power promotes social justice through nonpartisan civic engagement.

Privacy Advisory Commission Ordinance

(Revised - July 15, 2022)

ORDINANCE NO. _____

ORDINANCE OF THE CITY OF CHULA VISTA ESTABLISHING THE CHULA VISTA PRIVACY ADVISORY COMMISSION PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, AND DEFINING THE DUTIES AND FUNCTIONS OF SAID COMMISSION

WHEREAS, the Chula Vista City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately monitored and regulated to protect the privacy and other rights of Chula Vista residents and visitors, and

WHEREAS the City of Chula Vista (the City) has been building on a detailed Smart City Strategic Action Plan since 2017 with limited opportunity for community input, oversight or control; and

WHEREAS Chula Vista seeks to maintain its designation by Welcoming America as a certified Welcoming City, City Council strives to comply with the criteria in the Welcoming Standard, in particular, relevant criteria relating to “Safe Communities”, “Equitable Access”, and “Civic Engagement”; and

WHEREAS, the City Council recognizes the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs, both fiscal and civil liberties; and

WHEREAS, the City Council recognizes that surveillance technology may be a valuable tool to support community safety, investigations, and prosecution of crimes, but must be balanced with the individual’s right to privacy, it also; and

WHEREAS, the City Council recognizes that privacy is not just a personal matter; there are societal consequences to privacy degradation over time as well as societal benefits with increased trust and transparency; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, but also may include technology that aggregates publicly-available information, which, in the aggregate or when

pieced together with other information, has the potential to reveal details about a person's familial, political, professional, religious, or intimate associations; and

WHEREAS, the City Council recognizes that government surveillance may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, the City Council finds that safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before City surveillance technology is deployed; and

WHEREAS, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

WHEREAS, on January 18, 2022, City Council unanimously approved creation of a "Technology and Privacy Advisory Task Force" to draft policy and recommendations to be presented to the City Council for consideration, and further requested that the City Administration prepare a "Citywide Technology Oversight Policy"; and

WHEREAS, the said Technology and Privacy Advisory Task Force recommends creation of a new permanent citizen advisory board known as the "Privacy Advisory Commission" to advise the Mayor and City Council on transparency, accountability, and public deliberation in the City's acquisition and usage of surveillance technology and data; and

WHEREAS, Article VI, Section 600 of the City Charter reserves to the City Council the authority to create boards and commissions by ordinance, and to prescribe their function, powers, duties, membership, appointment, terms, qualifications, eligibility, reimbursements for expenses, if any;

NOW THEREFORE the City Council of the City of Chula Vista does hereby ordain as follows:

Section I. Establishment

A. Establishment and Appropriations

Pursuant to Article VI of the Charter of the City of Chula Vista, there is hereby created a Chula Vista Privacy Advisory Commission (hereinafter referred to as the "Privacy Commission" or "Commission"). Appropriations of funds sufficient for the efficient and proper functioning of the Privacy Commission shall be included in the annual budget by the City Council.

B. Purpose and Intent

It is the purpose and intent of the City Council to establish a Privacy Commission to serve as an advisory body to the Mayor and City Council on policies and issues related to privacy and surveillance. The Commission will provide advice intended to ensure transparency, accountability, and public deliberation in the City's acquisition and use of surveillance technology.

C. Definitions

For purposes of this ordinance, all words defined in the CVMC Chapter XXXX, known as the Chula Vista Surveillance and Community Safety Ordinance, have the same meaning herein.

D. Membership

The Privacy Advisory Commission shall consist of nine (9) members, who shall serve without compensation. At least six (6) members shall be Chula Vista residents. Members shall be appointed by the City Council.

E. Qualifications of Members

All members of the Privacy Advisory Commission shall be persons who have a demonstrated interest in privacy rights through work experience, civic participation, and/or political advocacy.

The City Council shall appoint the nine (9) members from the following representative areas of organization interest, expertise, and background:

1. At least one attorney or legal scholar with expertise in privacy or civil rights, or a representative of an organization with expertise in privacy or civil rights;
2. One auditor or certified public accountant;
3. One computer hardware, software, or encryption security professional;
4. One member of an organization that focuses on open government and transparency or an individual, such as a university researcher, with experience working on open government and transparency; and
5. At least four (4) members from equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.

Member qualifications and eligibility shall be in accordance with Chula Vista Charter Article VI, Section 602, and CVCM Section 2.25.030. No member shall have a state law-prohibited financial interest, employment, or policy-making position in any commercial or for-profit facility, research center, or other organization that sells data products, surveillance equipment, or otherwise profits from recommendations made by the Privacy Advisory Commission.

F. Terms

Pursuant to Article VI, Section 602 of the City Charter, members shall be appointed by motion of the City Council adopted by at least three affirmative votes. The members thereof shall serve for a term of four (4) years and until their respective successors are appointed and confirmed. Members shall be limited to a maximum of two (2) consecutive terms and an interval of two (2) years must pass before a person who has served two (2) consecutive terms may be reappointed to the body upon which the member had served.

Initial members shall be appointed in staggered terms by lot. For the initial appointments, three (3) members shall be appointed to an initial term that will expire on June 30, 2023, and two (2) members shall be appointed to an initial term that will expire on June 30 of each subsequent year. Initial appointments to a term of two years or less shall not have the initial term count for purposes of the eight-year term limit.

G. Rules

The Commission shall hold regular meetings as required by ordinance of the City Council, and such special meetings as such commissions may require. All proceedings shall be open to the public.

At the first regular meeting, and subsequently at the first regular meeting of each year following the first day of July of every year, members of the Privacy Advisory Commission shall select a chairperson and a vice chairperson.

The Commission shall adopt rules for the government of its business and procedures in compliance with the law. The Commission rules shall provide that a quorum of the Privacy Advisory Commission is five people.

Pursuant to Article VI, Section 603 of the City Charter, the Commission shall have the same power as the City Council to compel the attendance of witnesses, to examine them under oath and to compel the production of evidence before it.

Section II. Privacy Advisory Commission: Duties and Functions

A. Duties and Functions

The Privacy Advisory Commission shall:

1. Provide advice and technical assistance to the City on best practices to protect resident and visitor privacy rights in connection with the City's acquisition and use of surveillance technology.
2. Conduct meetings and use other public forums to collect and receive public input on the above subject matter.
3. Review Surveillance Impact Reports and Surveillance Use Policies for all existing and new surveillance technology and make recommendations prior to the City seeking solicitation of funds and proposals for surveillance technology.
4. Submit annual reports and recommendations to the City Council regarding:

- a. The City's use of surveillance technology; and
- b. Whether new City surveillance technology privacy and data retention policies should be developed, or existing policies should be amended.
- c. Provide analysis to the City Council of pending federal, state, and local legislation relevant to the City's purchase and/or use of surveillance technology.
- d. The Privacy Advisory Commission shall make reports, findings, and recommendations either to the City Manager or the City Council, as appropriate. The Commission shall present an annual written report to the City Council. The Commission may submit recommendations to the City Council following submission to the City Manager.

B. Meetings and Voting

The Commission shall meet at an established regular interval, day of the week, time, and location suitable for its purpose. Such meetings shall be designated regular meetings. Other meetings scheduled for a time or place other than the regular day, time and location shall be designated special meetings. Written notice of special meetings shall be provided to the Commission members, and all meetings of the Commission shall comport with any City or State open meetings laws, policies, or obligations.

The Commission shall, in consultation with the City Manager, establish bylaws, rules and procedures for the conduct of its business by a majority vote of the members present. Voting shall be required for the adoption of any motion or resolution. Any action by the Commission shall be approved by a majority of members present, provided a quorum exists.

C. Staff

Staff assistance may be provided to the Board as determined by the City Manager, pursuant to his or her authority under the Charter to administer all affairs of the City under his or her jurisdiction.

Section III. Severability

If any portion of this Ordinance, or its application to any person or circumstance, is for any reason held to be invalid, unenforceable or unconstitutional, by a court of competent jurisdiction, that portion shall be deemed severable, and such invalidity, unenforceability or unconstitutionality shall not affect the validity or enforceability of the remaining portions of the Ordinance, or its application to any other person or circumstance. The City Council of the City of Chula Vista hereby declares that it would have adopted each section, sentence, clause or phrase of this Ordinance, irrespective of the fact that any one or more other sections, sentences, clauses or phrases of the Ordinance be declared invalid, unenforceable or unconstitutional.

Section IV. Construction

The City Council of the City of Chula Vista intends this Ordinance to supplement, not to duplicate or contradict, applicable state and federal law and this Ordinance shall be construed in light of that intent.

Section V. Effective Date

This Ordinance shall take effect and be in force on the thirtieth day after its final passage.

Section VI. Publication

The City Clerk shall certify to the passage and adoption of this Ordinance and shall cause the same to be published or posted according to law.

Presented by:

Approved as to form by

Maria Kachadoorian
City Manager

Glen R. Googins
City Attorney

Surveillance & Community Safety Ordinance

(Revised - July 15, 2022)

ORDINANCE ADDING CHAPTER XXXX TO THE CHULA VISTA MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the City of Chula Vista ("City") takes great public pride in its status as a Welcoming City and as a Smart City; and

WHEREAS, smart public safety decisions and the protection of all community members require that municipalities ensure public debate and community involvement in decisions about whether to acquire or use surveillance technology; moreover, that real public safety requires that residents have a voice in these decisions; and

WHEREAS, across the U.S. cities that have adhered to a "privacy bill of rights" approach are able to win public support in implementing the technology with proper safeguards in place to build trust. Alternatively, cities that implement new technology in secrecy, without oversight, without policy, and without broad and inclusive public input have found themselves facing scrutiny, lawsuits, and voter referendums to ban certain technologies.

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City's acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, the City Council of the City of Chula Vista does ordain as follows:

Section I. Establishment

A. This Ordinance shall be known as the *Surveillance and Community Safety Ordinance*.

B. *Chula Vista Municipal Code Chapter XXXX*, is hereby added as set forth below:

Chapter XXXX. REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

C. Definitions

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
 - a. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
 - b. Whether and how often data acquired through the use of the surveillance technology was shared with internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s) except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
 - c. Where applicable, a description of the physical objects to which the surveillance technology hardware was installed without revealing the specific location of such

hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

- d. Where applicable, a description of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
- e. A summary of community complaints or concerns about the surveillance technology, and an analysis of its Surveillance Use Policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals;
- f. The results of any internal audits or investigations relating to surveillance technology, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. To the extent that the public release of such information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law;
- g. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- h. A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- i. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
- j. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates, such as the number of Public Records Act requests on such surveillance technology and the open and close date for each of these Public Records Act requests;
- k. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the surveillance technology in the coming year; and
- l. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "City" means any department, unit, program, and/or subordinate division of the City of Chula Vista as provided by Chapter XXXX of the Chula Vista Municipal Code.
3. "City staff" means City personnel authorized by the City Manager or appropriate City department head to seek City Council Approval of Surveillance Technology in conformance with this Chapter.
4. "Community meeting" means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of surveillance technology on disadvantaged groups.
5. "Continuing agreement" means a written agreement that automatically renews unless terminated by one or more parties.
6. "Exigent circumstances" means a City department's good faith belief that an emergency involving imminent danger of death or serious physical injury to any individual requires the use of surveillance technology that has not received prior approval by City Council.
7. "Facial recognition technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.
8. "Individual" means a natural person.
9. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet-accessing device, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
10. "Police area" refers to each of the geographic districts assigned to a Chula Vista Police Department captain or commander and as such districts are amended from time to time.
11. "Surveillance" (or "spying") means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the individual.
12. "Surveillance technology" means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, or system utilizing an electronic device used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such surveillance technology. Examples of surveillance technology include, but are not limited to the following: cell site simulators (Stingrays); automated license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection;

facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that can record audio or video and transmit or be remotely accessed. It also includes software designed to monitor social media services or forecast and/or predict criminal activity or criminality, and biometric identification hardware or software.

“Surveillance technology” does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology beyond what is set forth below or used beyond a purpose as set forth below:

- a. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any public surveillance or law enforcement functions related to the public;
- b. Parking Ticket Devices (PTDs) used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;
- c. Manually-operated, non-wearable, handheld digital 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;
- d. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- e. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- f. City databases 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;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes;
- h. Police department interview room cameras;
- i. City department case management systems;
- j. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above;

- k. Surveillance technology used by the City solely to monitor and conduct internal investigations involving City employees, contractors, and volunteers; and,
 - l. Systems, software, databases, and data sources used for revenue collection on behalf of the City by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other City department or third-party except as part of efforts to collect revenue that is owed to the City.
14. "Surveillance Impact Report" means a publicly-posted written report including, at a minimum, the following:
- a. Description: Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - b. Purpose: Information on the proposed purposes(s) for the surveillance technology;
 - c. Location: The physical or virtual location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
 - d. Impact: An assessment of the Surveillance Use Policy for the particular technology and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities;
 - e. Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;
 - f. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including open source data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
 - g. Data Security: Information about the controls that will be designed and implemented to ensure that adequate security objectives are achieved to safeguard the data collected or generated by the surveillance technology from unauthorized access or disclosure;
 - h. Fiscal Costs and Sources: The forecasted, prior, and ongoing fiscal costs for the surveillance technology, including initial purchase, personnel, and other ongoing costs, and any past, current or potential sources of funding;

- i. Third-Party Dependence: Whether use or maintenance of the surveillance technology will require data gathered by the surveillance technology to be handled or stored by a third-party vendor at any time;
 - j. Alternatives: A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate;
 - k. Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed surveillance technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the surveillance technology such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the surveillance; and
 - l. Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and City departmental responses given, and City departmental conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of surveillance technology.
15. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- a. Purpose: The specific purpose(s) that the surveillance technology is intended to advance;
 - b. Use: The specific uses that are authorized, and the rules and processes required prior to such use;
 - c. Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the surveillance technology, as well as data that might be inadvertently collected during the authorized uses of the surveillance technology and what measures will be taken to minimize and delete such data. Where applicable, any data sources the surveillance technology will rely upon, including open source data, should be listed;

- d. **Data Access:** The job classification of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e. **Data Protection:** The safeguards that protect information from unauthorized access, including logging, encryption, and access control mechanisms;
- f. **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), 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;
- g. **Public Access:** A description of how collected information can be accessed or used by members of the public, including criminal defendants;
- h. **Third Party Data Sharing:** If and how information obtained from the surveillance technology can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i. **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
- j. **Auditing and Oversight:** The procedures used to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the surveillance technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- k. **Maintenance:** The procedures used to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section II. Privacy Advisory Commission ("Commission") Notification and Review Requirements

A. Commission Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

1. City staff shall notify the Chair of the Commission by written memorandum along with providing a Surveillance Use Policy and a Surveillance Impact Report prior to:

- a. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant;
 - b. Soliciting proposals with any entity to acquire, share or otherwise use surveillance technology including the information it provides; or
 - c. Formally or informally facilitating in a meaningful way or implementing surveillance technology in collaboration with other entities, including City ones.
2. Upon notification by City staff, the Chair of the Commission shall place the item on the agenda at the next Commission meeting for discussion and possible action. At this meeting, City staff shall present the Commission with evidence of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to Section III.
 3. The Commission may make a recommendation to the City Council by voting for approval to proceed, by objecting to the proposal, by recommending that the City staff modify the proposal, or by taking no action.
 4. If the Commission votes to approve, object, or modify the proposal, City staff may proceed and seek City Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section III. City staff shall present to City Council the result of the Commission's review, including any objections to the proposal.
 5. If the Commission does not make its recommendation on the item within 90 calendar days of notification to the Commission Chair, City staff may proceed and seek City Council approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section II.

B. Commission Review and Approval Required for New Surveillance Technology Before City Council Approval

1. Prior to seeking City Council approval under Section III, City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Commission for its review at a publicly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for each document as set forth in Section I.
2. The Commission shall approve, modify, or reject the proposed Surveillance Use Policy. If the Commission proposes that the Surveillance Use Policy be modified, the Commission shall propose such modifications to City staff. City staff shall present such modifications to the Commission for approval before seeking City Council approval under Section III.
3. Prior to submitting the Surveillance Impact Report, City staff shall complete one or more community meetings in each City Council district where the proposed surveillance

technology is deployed, with opportunity for public comment and written response. The City Council may condition its approval of the proposed surveillance technology on City staff conducting additional community engagement before approval, or after approval as a condition of approval.

4. The Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Commission proposes that the Surveillance Use Policy be modified, the Commission shall propose such modifications to City staff. City staff shall present such modifications to City Council when seeking City Council approval under Section III.

5. If the Commission does not make its recommendation on a presented item within 90 days of notification to the Commission Chair pursuant to Section II, City staff may seek City Council approval of the item.

6. City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Use Policy, and include Commission recommendations, at least fifteen (15) days prior to a mandatory, properly noticed, germane public hearing. Approval may only occur at a public hearing.

C. Commission Review Requirements for Existing Surveillance Technology Before Seeking City Council Approval

1. Prior to seeking City Council approval for existing City surveillance technology used by the City under Section III, City staff shall submit a Surveillance Impact Report and Surveillance Use Policy for each existing surveillance technology to the Commission for its review, and for the public's review, at least fifteen (15) days prior to a publicly noticed meeting, so the public can prepare for and participate in the Commission meetings. The Surveillance Impact Report and Surveillance Use Policy shall address the specific subject matters set forth for each document in Section I.

2. Prior to submitting the Surveillance Impact Report, City staff shall complete one or more community meetings in each City Council district where the proposed surveillance technology is deployed with opportunity for public comment and written response. The City Council may condition its approval on City staff conducting additional outreach before approval, or after approval as a condition of approval.

3. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Commission, and for public review, a list of all surveillance technology possessed and/or used by the City.

4. The Commission shall rank the surveillance technology items in order of potential impact to civil liberties to provide a recommended sequence for items to be heard at Commission meetings. The Commission shall take into consideration input from City

staff on the operational importance of the surveillance technology in determining the ranking to allow such matters to be heard in a timely manner.

5. Within sixty (60) days of the Commission's action in Section II(C)(4), and continuing every month thereafter until a Surveillance Impact Report and a Surveillance Use Policy have been submitted for each item of the list, City staff shall submit at least one (1) Surveillance Impact Report and one (1) proposed Surveillance Use Policy per month to the Commission for review, generally beginning with the highest ranking surveillance technology items as determined by the Commission.

6. If the Commission does not make its recommendation on any item within 90 days of submission to the Commission Chair, City staff may proceed to the City Council for approval of the item pursuant to Section III.

Section III. City Council Approval Requirements for New and Existing Surveillance Technology

A. City staff shall obtain City Council approval prior to any of the following:

1. Accepting local, state, or federal funds, or in-kind or other donations for surveillance technology;

x2. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;

3. Using existing surveillance technology, or using new surveillance technology, including the information the surveillance technology provides, for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or

4. Entering into a continuing agreement or written agreement with to acquire, share or otherwise use surveillance technology or the information it provides, including data-sharing agreements.

5. Notwithstanding any other provision of this section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

B. *City Council Approval Process*

1. After the Commission notification and review requirements in Section II have been met, City staff seeking City Council approval shall schedule a date for City Council consideration of the proposed Surveillance Impact Report and proposed Surveillance

Use Policy, and include Commission recommendations, at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.

2. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

3. For Approval of existing surveillance technology for which the Commission does not make its recommendation within ninety (90) days of review as provided for in Section II: if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

C. Surveillance Impact Reports and Surveillance Use Policies as Public Records

1. Unless otherwise provided in this Ordinance, Surveillance Impact Reports and Surveillance Use Policies are public records.
2. City staff shall make all Surveillance Impact Reports and Surveillance Use Policies, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section II.
3. City staff shall post all Surveillance Impact Reports and Surveillance Use Policies to the City's website with an indication of its current approval status and the planned City Council date for action.

Section IV. Use of Unapproved Surveillance Technology during Exigent Circumstances

A. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy only in a situation involving exigent circumstances.

B. If City staff acquires or uses a surveillance technology in a situation involving exigent circumstances, City staff shall:

1. Immediately report in writing the use of the surveillance technology and its justifications to the City Council and the Commission;
2. Use the surveillance technology solely to respond to the exigent circumstances;
3. Cease using the surveillance technology when the exigent circumstances end;

4. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation or the exigent circumstances; and
5. Following the end of the exigent circumstances, report the temporary acquisition or use of the surveillance technology for exigent circumstances to the Commission in accordance with Section II of this ordinance at its next meeting for discussion and possible recommendation to the City Council.

C. Any surveillance technology acquired in accordance with exigent circumstances shall be returned within thirty (30) calendar days following when the exigent circumstances end, unless City staff initiates the process set forth for the use of the surveillance technology by submitting a Surveillance Use Policy and Surveillance Impact Report for Commission review within this 30-day time period. If City staff is unable to meet the 30-day deadline, City staff shall notify the City Council, who may grant an extension. In the event that City staff complies with the 30-day deadline or the deadline as may be extended by the City Council, City staff may retain possession of the surveillance technology, but may only use such surveillance technology consistent with the requirements of this Ordinance.

Section V. Oversight Following City Council Approval

A. Annual Surveillance Report

1. For each approved surveillance technology item, City staff shall present a written Annual Surveillance Report for the Commission to review within one year after the date of City Council final passage of such surveillance technology and annually thereafter as long as the surveillance technology is used.

2. If City staff is unable to meet the annual deadline, City staff shall notify the Commission in writing of staff's request to extend this period, and the reasons for that request. The Commission may grant a single extension of up to sixty (60) calendar days to comply with this provision.

3. After review of the Annual Surveillance Report by the Commission, City staff shall submit the Report to the City Council.

4. The Commission shall recommend to the City Council: (a) that the benefits to the community of the surveillance technology in question outweigh the costs and that civil liberties and civil rights are safeguarded; (b) that use of the surveillance technology cease; or (c) propose modifications to the corresponding Surveillance Use Policy that will resolve any identified concerns.

5. If the Commission does not make its recommendation on the item within 90 calendar days of submission of the Annual Surveillance Report to the Commission Chair, City staff may proceed to the City Council for approval of the Annual Surveillance Report.

B. Summary Of All Requests And Recommendations And City Council Determination

1. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section III for that particular surveillance technology and the pertinent Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

2. Based upon information provided in the Annual Surveillance Report and after considering the recommendation of the Commission, the City Council shall revisit its “cost benefit” analysis as provided in Section III(B)(2) and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City’s use of the surveillance technology must cease. Alternatively, City Council may require modifications to a particular Surveillance Use Policy that will resolve any concerns with the use of a particular surveillance technology.

Section VI. Enforcement

A. Violations of this article are subject to the following remedies:

1. Any material violation of this Ordinance, or of a Surveillance Use Policy promulgated pursuant to this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the City of Chula Vista and, if necessary, to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.

2. Any person who has been subjected to the use of surveillance technology in material violation of this Ordinance, or of a material violation of a Surveillance Use Policy, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in the Superior Court of the State of California against the City of Chula Vista and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater).

3. A court may award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A(1) and A(2) under Section VI above.

Section VII. Contract for Surveillance Technology

A. Contracts and agreements for surveillance technology

1. It shall be unlawful for the City to enter into any contract or other agreement for surveillance technology that conflicts with the provisions of this Ordinance. Any conflicting provisions in any such contract or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Any amendment or exercise of any option to any contract to obtain or use surveillance technology shall require City staff to comply with the provisions of this Ordinance.
2. To the extent permitted by law, the City shall publicly disclose all of its surveillance contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

Section VIII. Whistleblower Protections

A. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

1. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
2. The employee or applicant was perceived to, about to, had assisted in or had participated in any proceeding or action to carry out the purposes of this Ordinance.

B. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or administrative instruction promulgated under this Ordinance.

C. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

Section IX. Review of Existing Surveillance Use Policies and Adoption as Ordinances

A. Surveillance technology is considered existing if the City possessed, used, or has a contract in force and effect for the use of surveillance technology, or any resulting data, on the effective date of this Ordinance.

B. The requirement for City staff to present a list of all existing surveillance technology and, once ranked, to seek monthly Commission review and approval for the use of existing surveillance technology shall begin within sixty (60) days after the effective date of this Ordinance.

C. As per Section II, City staff shall return to City Council with an ordinance or ordinances for adoption and codification under the Chula Vista Municipal Code of all Surveillance Use Policies, but only after proper Commission and City Council review of any Surveillance Use Policies for existing surveillance technology, and with a 15-day public notice period in each instance to allow the public to prepare and participate in the meetings.

Section X. Severability

If any portion of this Ordinance, or its application to any person or circumstance, is for any reason held to be invalid, unenforceable or unconstitutional, by a court of competent jurisdiction, that portion shall be deemed severable, and such invalidity, unenforceability or unconstitutionality shall not affect the validity or enforceability of the remaining portions of the Ordinance, or its application to any other person or circumstance. The City Council of the City of Chula Vista hereby declares that it would have adopted each section, sentence, clause or phrase of this Ordinance, irrespective of the fact that any one or more other sections, sentences, clauses or phrases of the Ordinance be declared invalid, unenforceable or unconstitutional.

Section XI. Construction

The City Council of the City of Chula Vista intends this Ordinance to supplement, not to duplicate or contradict, applicable state and federal law and this Ordinance shall be construed in light of that intent.

Section XII. Effective Date

This Ordinance shall take effect and be in force on the thirtieth day after its final passage.

Section XIII. Publication

The City Clerk shall certify to the passage and adoption of this Ordinance and shall cause the same to be published or posted according to law.

Presented by

Approved as to form by

Maria Kachadoorian
City Manager

Glen R. Googins
City Attorney

From: Michael McDonald <[REDACTED]>
Sent: Monday, August 1, 2022 1:21 PM
To: privacytaskforce@chulavistaca.gov
Subject: 7/27 Community Meeting - Technology & Privacy Advisory Task Force

**Warning:
External
Email**

Dear Task Force members,

I attended the community forum on July 27, 2022 and would like to provide my feedback about the meeting for your attention and the record.

I was in Raf's (Rafael?) group and takeaways were as follows:

1. Most of the conversation was dominated by one person in particular who claimed he had prior experience with Chula Vista government and politics. He traded a lot of questions and remarks with the moderator and it appeared that Raf was in a defensive position the whole time instead of taking notes and facilitating a discussion. I'm not sure if there was an overall plan for the discussion groups prior to this meeting, but I did not feel the conversation was productive for all of us and I felt some members did not have a chance to voice their opinions, ideas and experiences. Please be mindful of individuals dominating the conversation and guide the conversation and take notes rather than taking any position that could be perceived as bias towards the City or the police department and allow others to share as well.
2. Based on the results of the survey in the beginning of the meeting, the majority of the attendants were over 40 years of age and were either white or white presenting. This was not representative of the population of Chula Vista or the demographics of the communities where these technologies are used the most. This was apparent in our discussion as all members of my group were concerned with issues surrounding personal property, which limited the scope and reach of these technologies and the broader issues relating to the communities that are most impacted, the unhoused in Chula Vista, young people in underserved communities and so forth. Without adequate representation of residents of Chula Vista at these meetings, including those that were formerly incarcerated, young people of color and those that are most impacted by the use of surveillance technologies is a disservice to this Task Force and will produce inaccurate data that is collected for the purpose of policy making.
3. This leads to my next not which is the discussion question about how to get more people to attend the meetings. As I'm aware, the City may already employ a marketing/PR team that could contract with a consultant or hire more people to figure out ways to attract and incentivize more people, especially from the communities where this technology is most deployed, to attend the meetings. This could mean being more transparent about how this technology is used, how many drones the PD currently deploys to neighborhoods and what is done with the data collected. There could be an outreach team visiting local junior and high schools to talk with students or attend after school programs in the area. These ideas were not discussed because the conversation was only regarding what has already been done and doing more of that ex. sending mailers to homes. I was disappointed that the moderator only shared this idea to the rest of the attendants at the end and not the majority of the conversation about confusion and concerns the group members had.
4. Finally, our group although limited in focus on personal privacy concerns did offer valid questions about past events about how this contract was approved, current data collection and management processes and future use of these technologies. The moderator appeared to take the position of representing the City by trying to answer questions about the contract, police protocols and data collection practices and the policy proposals they came up with. I expected the moderator to ask the questions and take notes about what questions and concerns that were raised. As soon as he tried to answer the initial questions about the contract, the group

assumed that he represented the City and continued to ask questions and this was not a productive conversation.

Thank you for your time and attention to my feedback. I hope to participate in future meetings and events surrounding this topic.

Best,

Michael McDonald

Jeremy Ogul

From: Stacey Uy [REDACTED]
Sent: Monday, August 1, 2022 9:46 AM
To: privacytaskforce@chulavistaca.gov
Subject: Takeaways from 7/27 Public Comment Forum

**Warning:
External
Email**

Dear Privacy Task Force Members,

Thank you for carving out a space for the community to contribute to the conversation on surveillance in Chula Vista. As a member of Adriana's group, I wanted to make sure highlights from our group were put into the record. We had a great discussion. We probably disagreed on many things, but we were in consensus over the following points, and especially for surveillance policies being community-led.

1. Seeking public approval *after* programs are already underway is TOO LATE. The fact that the drone program and automated LPRs are already being used without the public's consent and knowledge is a sign that the city of Chula Vista is failing to protect its citizens' privacy. There needs to be processes in place **before** technology is acquired and used.
2. One of our group members, Sergio, spoke of his personal experience of being overly surveilled, to the point where even his daughter is noticing the drones following them and he's had to file complaints to the DOJ with no response. Safeguards like the Oversight Board and policy safeguards need to be **community-led**. That means, placing the people affected by surveillance the most on the Oversight Board. People like Sergio, Black, Latinx, undocumented, young people, trans and queer folks should be sought after as experts on how surveillance affects our everyday lives and how we can protect privacy while keeping each other safe. Requirements for membership that include bachelor's degrees, clean records, and technology "expertise" are back door attempts to exclude the people who have first hand experience of being overly surveilled in the city.
3. We all identified issues in Chula Vista that needed attention such as homelessness, drug rehabilitation programs, and affordable housing. We ALL agreed the return on investment from surveillance technology to supposedly prevent crime was unacceptable, compared to how that money could have been spent actually helping the people that need it the most. **Providing basic services is where crime prevention happens.**
4. According to our poll, no one under the age of 24 was present. The city of Chula Vista needs to be **actively engaging young people** in the conversation, as these policies will affect them for the rest of their lives. That can look like holding youth-specific forums at schools and publicizing meetings on Tik Tok and IG. If you don't know how to do these things, you should hire (and pay) young people to help you.

As an Asian American, I was also very concerned that the forum audience did not reflect the racial makeup of the city. With the spotlight on anti-Asian violence, people claim we need surveillance to keep us safe, and I disagree. We are just as much at risk of being overly-surveilled and over-policed, and we will not be used as a racial wedge to build more surveillance in the city. Please do a better job of engaging with Black, Latinx, and Asian American communities for these meetings.

Thank you for your attention on this matter. And I hope to engage more in future meetings.

Sincerely,

Stacey Uy (she/hers)

From: Norah Shultz [REDACTED]
Sent: Friday, August 12, 2022 7:12 AM
To: privacytaskforce@chulavistaca.gov
Subject: Concerns about survey conducted for policy consideration

**Warning:
External
Email**

Dear Members of the Chula Vista Privacy Advisory Task Force,

I am a Professor of Sociology at San Diego State University. I have been a professor and a senior administrator in higher education for over thirty years. Since my undergraduate days, one of my core specializations has been in the area of survey research.

I've reviewed the report and the survey and I have a lot of questions. I'm going to write about them in groups and put representative examples for the types of concerns, rather than go through each question and/or finding.

My overall concern is that while this is a well-known firm that has conducted a classic phone/email survey with traditional methodology (and for that there are strengths to what they have presented), it is not getting to the answers that are needed for the questions that a city council should be seeking. What is needed is a study to determine the needs and concerns of all community members, which is different from a study to determine the likelihood of something occurring – a market research study or a political poll, for example. In other words, a more nuanced study and analysis is required for a study of community needs and concerns.

I'm sure the firm can answer a few questions I have about their work, however, as I explained I will list the overall issues with their approach:

(1) It is very reassuring to read the words random sample and statistically significant. This sounds scientific and unbiased. However, a truly random sample is one in which every person has the same chance as any other person to participate in the survey. That means every person in your population – the group you are interested in learning about. I'm assuming that you are all interested in learning about all the residents of Chula Vista. So if this were truly a random sample of the residents of Chula Vista, then that means that each person in Chula Vista had the same chance of ending up in the final group as any other. But this is **not true** because of the following:

- a. The sample was originally constructed from a list. Unless that list was all of the residents (over 18) of Chula Vista, then not everyone has the opportunity to be selected. Where is the list from? Phone directories and car registrations? There is bias there. Voter registration? We know the bias there. I didn't see reported in the materials how the list was generated.
- b. When you generate your random sample from your list, you decide to select every Xth person depending upon how many you need in your sample as you allude to in your notes on effect size. But again, unless every Xth person agrees to participate and complete the survey, bias has crept in again. Do you know how different the participants are from those who do not participate? One way is to try to get non-participants and those who do not complete the survey to provide some demographic information, particularly on relevant variables such as income, or some indicator of

socio-economic status, and ethnic group identity and, in this case, also on perceived knowledge of the technology, so that some comparisons can be made to determine if your final sample is representative of the population and if these changes along the way have not introduced a bias that impacts your study questions. Again, while this check on the representativeness of the sample may be included in the final report, it was hard to find.

c. The easiest way to reassure those reviewing the report would be to take the demographic information from p. 2 and on p. 6 and compare it to the data from the Census Bureau for the city. You explain that you applied weights (and only on four variables from what I can discern) but do not provide detail about the demographic characteristics that were impacted. The weighting statistical technique will not account for missing information from groups. The weighting technique also would not impact the open-ended questions. This is an extremely long questionnaire. We have no idea what percentage of the original group actually completed the questionnaire. Even with the weighting, it makes it very difficult to assess many of the findings - particularly when critical policy issues are being considered.

(2) The questionnaire is extremely long. This in itself is of concern. People who complete a survey of this length are different from those who don't. While there are some very good aspects to the questionnaire, there are some that I find concerning, besides the length. For example, let's look at Q7a. Part of the intro reads, "...where engineers use it to manage traffic signal timing in an effort to improve traffic flow and safety." It is not surprising that 77% of the respondents approved of this. Who is going to say they don't approve of improving safety? If a question has an 80/20 split, it is not differentiating. Now it may be that everyone is okay with this, but the question wording makes me wonder. Were there skip sequences? For example, if I don't know anything about the use of drones, did I answer Q9? After that, Q11 and A12 really start out with sentences that make it pretty hard to answer anything other than beneficial. I actually think it is problematic that those with little or no knowledge seem to be included in the analyses along with those who claim some awareness of the technology or Chula Vista's programs, as well as others who may have actual experience or understanding of the technology use and privacy issues and implications, beyond what is written in this survey as the lead-ins to the questions. That may be one of the most problematic aspects. It is very good that you include the opposite questions, however the language is subtly different, "*Some people worry the drones might,....*" [emphasis mine]. Again, not to throw this out entirely but I think problems with wording and sequencing of questions should be brought to the attention of those who might want to use the reported findings to make policy decisions that impact people's lives.

(3) My last points are about the analysis. The vast number of crosstabs, many with small cell sizes, makes it hard to go back and make any independent judgments. I also did not see any statistical analysis, such as a chi-square, associated with these data. Since chi-square is sensitive to overall sample size and the cell sizes are so variable, a discussion of statistical significance related to this information would, admittedly, be problematic. But there are other ways to address this. You mention sampling error several times in the report, but I haven't been able to find any discussion of effect size. In a study such as this, one that is impacting policy and citizens lives, I'd be curious about meaningful differences rather than statistically significant differences. I did appreciate the explanation of how to properly read a cross tab! I also reviewed the section discussing the multivariate analysis, but would like to have seen the actual analysis in the appendix and not just the cloud replication. What was the overall R^2 ? Was this explaining the outcome in any significant way? It is, as I stated above, important to discuss the **meaning** and not just the statistical significance but the findings are presented in a way that makes it hard to understand overall how much is being explained here. Were all responses put into your model?

Another key concern is that we don't know who is really being represented in this analysis. The very people who may be most impacted by such a policy may be silenced. As I wrote at the beginning, this does not call for a piece of market research. What is needed is a study that looks at the differential impacts on the highly diverse population of Chula Vista. In a situation such as this, I would not have used a random sample. With a simple random sample, you cannot create a stratified random sample, to make sure you are reaching enough of the people who may have particular concerns so that you can adequately analyze their position vis-à-vis the other groups. This requires a more complex sampling design. I realize that important steps were taken to have a Spanish language and a Tagalog version, and to conduct several focus groups drawn again from some lists, but this falls far short of capturing the voices of many others in the community whose opinions and concerns should be a part of the crafting of such a policy.

Finally, I also would add that the survey report is incredibly long, just like the survey, and very difficult for any lay person to digest. I spend a lot of time teaching students not only how to work on surveys but how to prepare their reports for their audience. Ultimately, as decision makers, the city council has the moral obligation to be sure they understand the information that they are given and to be able to interpret it properly.

I pose these questions with respect for the work done; but also with great respect for all of the residents of Chula Vista.

Sincerely,

Norah P. Shultz, Ph.D.

--

Norah P. Shultz, Ph.D.

Pronouns: She / Her

Professor of Sociology

College of Arts & Letters

Doctoral Faculty

Edd Educational Leadership Community College

& Post-Secondary Education Program

College of Education

Director of Inclusive Curriculum

Division of Student Affairs & Campus Diversity

Nasatir Hall 210

San Diego State University

SDSU



SafeZones@SDSU Ally. Military Ally. Ability Ally.

Indigenous hostlands: Birthplace: Lenapehoking; Residence: Kumeyaay





Jeremy Ogul

From: [REDACTED]
Sent: Monday, August 15, 2022 7:21 PM
To: privacytaskforce@chulavistaca.gov
Subject: Recommendations

**Warning:
External
Email**

Dear Members of the Chula Vista Privacy Advisory Task Force,

As a Chula Vista resident, I would like to make some recommendations that can be part of this discussion.

1. Accountability for Breached Data

I would recommend that the task force come up with a fair punishment when a breach occurs. Usually, the punishment for allowing a breach is a light slap on the wrist. More often than not, there is none.

"We will never have true data security until we start holding companies/governments and their executives/leaders legally and financially accountable for the security of any kind of consumer data they possess."

Basically, we need to hold the vendors and city leaders financially accountable.

2. Children Data

I would like to recommend that ALL data be removed after captured.

3. Right of Citizen's to OPT-OUT

Recommend that each Chula Vista resident have the option to request to review their data and request to have the city erase/delete all data.

Roman Covarrubias

Jeremy Ogul

From: Seth Hall [REDACTED]
Sent: Sunday, August 14, 2022 8:32 PM
To: privacytaskforce@chulavistaca.gov
Subject: Items to consider regarding August 15 Subcommittee reports
Attachments: 2208 Tech Lead SD - Consideration Items RE Subcommittee Reports.pdf

**Warning:
External
Email**

Distinguished task force members,

Please see the attached document regarding items for your consideration as you continue to discuss your recommendations. I would appreciate a confirmation that this email has been received and distributed appropriately.

Thank you all for your continued work on this important topic.

Seth Hall, techleadsd.org
[REDACTED]



“Technologists Tending the Grass Roots”

August 14, 2022

Dear distinguished task force members,

Please consider the attached suggestions as you deliberate regarding your final recommendations.

Chula Vista residents deserve to determine for themselves how they will leverage new technology while protecting themselves from its many potential harms. The attached suggestions are sent in the spirit of collaboration among neighbors who are both actively working to answer similar questions, while also striving for the safest and healthiest city we can create.

Sincerely and with respect,

Seth Hall

Tech Lead San Diego (member of the TRUST SD Coalition)

Items for Consideration Regarding August 15 Subcommittee Reports

Items regarding the Procurement Subcommittee Report

1. The task force should consider making clear its intentions behind any exception to its recommendation prohibiting nondisclosure agreements, so that subsequent city attorneys reviewing the recommendation can provide proper guidance on how such an ordinance would be drafted.

Many NDAs can be argued to contain “proprietary information,” and I don’t believe it is the desire of the task force to incentivize vendors to include proprietary information in the contract for the specific purpose of making contracts undisclosed under the task force’s recommended exception. In my experience, such tactics, while reprehensible from a public perspective, are entirely common in the for-profit vendor context.

2. The task force recommends that a convenience termination clause be added into vendor contracts for cases when a vendor requires their contract be placed under a NDA. If the task force chooses to recommend this, they may wish to further clarify what the task force believes the correct conditions are that would satisfy your intentions for convenience termination.

For example, without additional guidance, convenience termination could be offered by a vendor, but only under the condition the City pays penalty fees that could equal the buyout cost of the contract. I don’t believe that the intention of the task force is to allow vendors to force the City to buy out the entire contract term in exchange for convenience termination in the case of an undisclosed NDA, because that does not protect Chula Vista taxpayers from predatory practices by vendors, and wouldn’t achieve any meaningful options or protection for the City.

If the task force’s intention is that the city can terminate a vendor contract for convenience without any penalty whatsoever imposed by the vendor, the task force should make that intention clear in its recommendation.

3. The task force should reconsider its recommendation that allows for NDAs on vendor contracts in cases of proprietary information. Other subcommittee recommendations (PO&T) require vendor contracts to be posted publicly, and those recommendations do not provide for any exceptions. Upon

further deliberation, the task force may find that hiding vendor contracts from the public is always harmful to public interests and only serves the interests of private parties.

Items regarding the Privacy Advisory Board Subcommittee Report

1. Each restriction placed on board membership carries a risk the board will not be able to be fully populated, which raises the risk of not achieving quorums, or that a minority of members could control the board's decisions. The current recommendation potentially restricts 6 of the 9 seats, and does so in 3 different ways (residency, district residency, professional background). A minimum of 3 board members would have no restrictions whatsoever, beyond applicable law, which gives significant power to an individual who can appoint to those seats.

Consider issues such as redistricting, as well as the ability of council members to interfere with the board's functions by withholding nominations in their district. The task force should deliberate regarding the risks of board membership they are trying to mitigate, and ensure their final recommendation addresses the risks the task force believes are the highest and most likely risks.

2. Prior to making final recommendations, the task force should receive advice from city attorneys regarding the creation of boards and commissions, if the task force has not already received such advice. Existing limitations within the charter or municipal code could have the effect of substantially changing the task force's recommendations if, for example, the task force's preferred appointment process does not comply with current municipal code.
3. The task force is undecided on whether a seat on the board should be reserved for a past member of law enforcement. The task force should consider the option of neither reserving a seat for police, nor prohibiting police from the board. This model leaves the decision up to those responsible for appointments, who may have contemporary insights on the appropriateness of police membership on the board, at the time vacancies occur. If a seat is reserved for police, future appointees supported by the community may be ineligible for appointment, due to the strict requirement recommended by this task force.

4. The task force should consider whether it wants to recommend that a future privacy board be allowed to assemble via virtual meeting in addition to in-person meetings. Virtual meetings can be helpful to ensure quorums are achieved, and virtual meetings can also be helpful with increasing public participation. If the task force does not recommend the accommodation of virtual meetings, the city may not consider supporting that capability.

Items regarding the Use Policies Subcommittee Report

1. The task force recommends allowing the city to prioritize the surveillance technologies that should be reviewed by the board. Consider that the task force is recommending a board of community members, and that the community members are being carefully selected for residency and professional qualifications to ensure they provide trustworthy recommendations.

Considering the careful requirements placed on board membership, the task force should consider capturing those board members' input on the prioritization of technology to be reviewed. Appointed board members' qualifications hopefully indicate a deeper knowledge of what technology is sensitive than what city staff may be aware of. Current task force recommendations cut board members entirely out of the prioritization process and put city staff in the driver's seat.

Items regarding the Data Subcommittee Report

1. Regarding data minimization, the task force should consider adding a recommendation that sensitive personal information in particular be specially handled and retained for only the minimum amount of time necessary to accomplish the most immediate and pressing goal of data collection. See later recommendation that "sensitive personal information" be defined as a term.
2. When the task force makes recommendations that items (such as sale of the public's information) should not occur without "sign off," the task force should consider being more specific with regard to its intention on the process of those approvals. For example, does the task force advise that the sale of public information should require a majority vote of city council, or merely the approval of a particular individual within City staff?

3. Because the City’s Data Governance Committee is made up of only City staff, which varies with turnover, and is not structured by municipal code governing the City’s boards and commissions, the task force may want to consider removing references to the Data Governance Committee from the recommendations. The current recommendation attempts to incorporate the Data Governance Committee into the new privacy process, which may create conflicts of authority and process.
4. The task force should consider incorporating the term “Sensitive Personal Information” into the terms in need of definition, and the task force should consider recommending that the definition of the term permanently track the definition of Sensitive Personal Information as it is defined in the California Privacy Rights Act. See above #1 for recommendation on using this term to apply stronger protections for the public’s most sensitive data.

*Items regarding the **Privacy Oversight & Transparency Subcommittee Report***

1. Nowhere in the subcommittee report are public meetings, community forums, or other live community education offered by City staff recommended. The task force should deliberate on whether posting signs, or posting links on the city website, is sufficient to ensure Chula Vista residents receive an acceptable level of awareness regarding the technology being deployed in their neighborhoods.

*Items regarding the **Information Security Subcommittee Report***

1. The task force includes activity covered by a NDA to be “Confidential Data” and undisclosable to the public. This is very broad because the task force does not know what data could be considered to be “covered” by any given future NDA, since NDAs are negotiable and generally favorable to the non-city party. The task force should deliberate on whether this definition of Confidential Data is too favorable to vendors and poses unquantifiable risks to the public.
2. The task force includes in its definition of confidential data “information related to an allegation or investigation of misconduct.” This recommendation pulls the task force and privacy board into the controversy around public records controversies and California laws governing misconduct, such as SB 1421. The task force should deliberate on whether they believe a privacy ordinance is the proper

venue to engage those controversies or whether the task force's recommendation should instead lean on existing laws and public records processes and policies that already exist within the city.



CAMPAIGN ZERO



FIGHT FOR THE FUTURE



DEMAND PROGRESS



National Network for Arab American Communities



MILLIONHOODIES MOVEMENT FOR JUSTICE



Community Control Over Police Surveillance – Guiding Principles

The Community Control Over Police Surveillance effort, including the legislation being sponsored in connection with it, is guided by the below principles. Legislation may vary from city to city to reflect local concerns and circumstances.

Surveillance technologies should not be funded, acquired, or used without express city council approval: Surveillance technologies should not be funded, acquired or used without the knowledge of the public and the approval of their elected representatives on the city council. Agencies seeking to use a previously acquired surveillance technology in a new manner must also receive specific city council approval of the new use(s).

Local communities should play a significant and meaningful role in determining if and how surveillance technologies are funded, acquired, or used: When used indiscriminately, surveillance technologies create oppressive, stigmatizing environments, especially for communities that are disproportionately targeted by their use, such as communities of color, low income communities, and politically active communities. Rather than allowing the police to unilaterally decide if and how surveillance technologies may be acquired and used, we believe local communities and their elected officials should be empowered to make those determinations.

The process for considering the use of surveillance technologies should be transparent and well-informed: The city council should not approve the funding (including submitting applications), acquisition, or deployment of any surveillance technologies without holding a public hearing. To facilitate a well-informed public debate, far in advance of the hearing, the police or other agency seeking to use the surveillance technology shall publically report on, among other things, the technology to be acquired, its capabilities, how precisely it would be used, how its data would be preserved and protected, its acquisition and operational costs, and how potential adverse impacts on civil rights and civil liberties will be prevented.

The use of surveillance technologies should not be approved generally; approvals, if provided, should be for specific technologies and specific, limited uses: Prior to the public hearing, the police or other agency seeking to acquire and/or use a surveillance technology must identify the technology and its proposed uses with specificity, so they can be debated with specificity. It should be unlawful for the police or any other agency to use a

surveillance technology that has not been expressly approved, or to deploy an approved surveillance technology in a manner that has not been expressly and precisely approved.

Surveillance technologies should not be funded, acquired, or used without addressing their potential impact on civil rights and civil liberties: Historically, government surveillance has had a significant, detrimental impact on civil rights and civil liberties, including those guaranteed by the First, Fourth and Fourteenth Amendments to the United States Constitution. In recognition of this fact, prior to holding a public hearing, the police or other agency seeking to fund, acquire, or use a surveillance technology should expressly identify the potential adverse impacts the technology may have on civil rights and civil liberties and what specific measures it will undertake to prevent such adverse impacts.

Surveillance technologies should not be funded, acquired, or used without considering their financial impact: Prior to holding a public hearing, the police or other agency seeking to fund, acquire, and/or use a surveillance technology should provide information on the surveillance technology's financial benefits and costs, including its acquisition and annual operational costs.

To verify legal compliance, surveillance technology use and deployment data should be reported publically on an annual basis: A public approval process for the acquisition and use of surveillance technology will be of limited value unless the city council and public can verify the legal requirements pertaining to its use, including those regarding the protection of civil rights and civil liberties, have been adhered to. Annual reporting requirements will empower the city council and public to monitor the use and deployment of approved surveillance technologies.

City council approval should be required for all surveillance technologies and uses; there should be no "grandfathering" for technologies currently in use: The same public approval process for the acquisition and use of new surveillance technologies should be applied to surveillance technologies that are currently in use. Any technologies and existing uses that are not expressly approved pursuant to a transparent, community-focused process should have to be discontinued.

Jeremy Ogul

From: Margaret Bake [REDACTED]
Sent: Thursday, September 22, 2022 2:52 PM
To: Privacy Task Force
Subject: Please post attached Privacy Advisory Commission Ordinance with Privacy Task Force meeting agenda
Attachments: Revised Privacy Advisory Commission Ordinance_2022-07-15.pdf

**Warning:
External
Email**

Margaret A. Baker, DrPH
[REDACTED]

South Bay People Power promotes social justice through nonpartisan civic engagement.

Jeremy Ogul

From: Jason Essex [REDACTED]
Sent: Friday, September 2, 2022 10:08 AM
To: privacytaskforce@chulavistaca.gov
Subject: New Chula Vista Privacy Policy Reply

**Warning:
External
Email**

Greetings,

I have had any number of issues for over ten years as it pertains to privacy.

The root cause also always lead back to lawyers, attorneys, law firms, groups, organizations and company who do honor their oath, do do not state discovery, disclose why they are doing so as well as ignoring Caliofnria Consumer Protection Act.

Each needs to be held accountable for not having a business listing it with the city and or state but a listing with the California State Bar. ANY *website* that ends in : .com is a business. In many cases they do not have a Privacy or Terms of Use page(s).

I have to wonder how many data mining tools they use to capture your IP Address, Email information and the like. A Credential check needs to be run whenever a case is brought to the court as it pertains to these listings. If you can sight said legal entities ongoing failure to state Disclosure and Discovery they need to be penalized and this should count towards the opposing party.

I also have to wonder why said entities that have my Social Security number have shared it with such legal sources and not been accountable. Monies have changed hands for the purpose of earning monies from said information. Does this not fall squarely under the California Consumer Protection Act as well as Disclosures and Discovery laws in addition to Business and Professional Ethics laws?

To review these ongoing concerns please review my cases in the San Diego County Court House / Hall of Justice.

* I have not been paid fro any of my Intellectual Properties dating back to 2014 as of today. The courts have repeatedly frozen my assets without ever stating who the asset manager(s) are. With of twenty (20) such items for sale under the author names of By Jason Douglas Essex, By Jason Essex as well as the bulk being under By Jason D. Essex the sales platforms have never provided me with earnings information.

As such this is identity, time and wage theft that has caused endless forced labor and costs in addition to endless stress.

Here is a direct link to some of my content:

<https://www.facebook.com/ByJasonDEssexLocalAuthor>

<https://books.apple.com/us/book/red-tape/id1529009437>

<https://books.apple.com/us/book/a-valentines-day-event-for-you-to-enjoy-too/id1571539079>

This appears to be the data mining and redirection robot that is preventing me from having any such information or earnings on this sales platform:

<https://books.apple.com/us/book/living-the-dream/id437205980>

Thank you for your time today.

By Jason D. Essex

[REDACTED]

Chula Vista, CA 91914

Jeremy Ogul

From: Steve Goldkrantz [REDACTED]
Sent: Tuesday, September 6, 2022 12:50 PM
To: Adrianna Hernandez
Cc: Privacy Task Force
Subject: Re: Share your thoughts on privacy guidelines for the City of Chula Vista

**Warning:
External
Email**

Ms. Hernandez,

Thank you for the opportunity to provide comment and feedback. The draft is very well organized and written. As for the formation of a new Board including non-Chula Vista residents, I defer to the current regulations on the books concerning such a matter.

It seems that there are four overarching issues at hand:

(1) Cybersecurity - how the City of CV information is secured once collected - be it City Hall offices, the library, the Police Department, etc. This involves technical systems security matters, user procedures, and insider threat detection/mitigation.

(2) Information Sharing Externally - this always presents a cybersecurity challenge, and again covers information technology transmissions from the technical level to the user level. Essentially, how information can technically be shared externally - legally and appropriately - while remaining secure.

(3) Privacy - what information is deemed Private and [Sensitive] Personally Identifying Information under various laws and rules such as the Privacy Act, 28 CFR 23, etc. and what are the regulations/rules guiding both the technology and end user applications.

(4) Enforcement Technologies - with the rapid expansion of the City of Chula Vista, the Public Security Sector is challenged in meeting the demand for increased patrols, call responses, crime prevention, victim handling, etc. Technology is a force multiplier for deterring crime, responding to crimes, enabling community assistance, investigations, prosecution. Technology is critical to the entire law enforcement cycle needed to protect the residents of the City and those who are non-residents but work, attend school, shop, or have businesses here. Enforcement technologies are a force multiplier for public protection and the officers and first responders working it.

All the above needs to be wrapped up with incident detection, response, mitigation, resolution. It might not be bad for a "Red Team" to challenge some of the existing processes as well as the gaps/concerns identified by the Privacy Task Force.

Again, thank you for the opportunity to comment. The Mayor's Office and the Privacy Task Force are more than welcome to reach back to me for any further questions, comments via this email or my phone: 619-823-3383.

Thank you and have a great afternoon.

Steve Goldkrantz

[Sent from Yahoo Mail for iPad](#)

Jeremy Ogul

From: Seth Hall [REDACTED]
Sent: Tuesday, September 6, 2022 4:23 PM
To: privacytaskforce@chulavistaca.gov
Subject: Suggestions for Draft Recommendations
Attachments: 2209 Tech Lead SD - Suggestions RE Draft Recommendations.pdf

**Warning:
External
Email**

Task Force members,

Please find attached a review of the draft recommendations and additional items for your consideration. Please confirm your receipt and distribution. Thank you!

-Seth Hall, Tech Lead San Diego
[REDACTED]

September 6, 2022

Dear distinguished task force members,

Congratulations on reaching an important milestone in your work. The Task Force's proposed draft of recommendations contains many important improvements, which will benefit the residents and visitors of Chula Vista.

My below review expresses suggestions for 11 potential improvements to your draft recommendations. Among those 11 suggestions, I believe suggestions that are related to 4 items in particular would have the most significant impact on your recommendations.

1. The Task Force's draft recommendations do not include a requirement that any specific approvals be required, prior to acquiring or using surveillance technology. My below Recommendation 2 strongly suggests adding that as a Task Force recommendation.
2. The Task Force is not currently recommending the use of impact reports as a tool to discover and mitigate potential harms caused by surveillance technology. My below Recommendation 3 suggests adding that as a Task Force recommendation.
3. The Task Force is not currently recommending any educational meetings with the public be held prior to acquisition or use of surveillance technology. My below Recommendation 6 suggests adding that as a Task Force recommendation.
4. The Task Force is not currently recommending the use of annual surveillance reports as a primary tool to achieve meaningful, ongoing oversight. My below Recommendation 11 suggests adding that as a Task Force recommendation. I suggest adding that as a Task Force recommendation.

In addition, I suggest the Task Force create a Guiding Principles document to make clear the principles that the Task Force suggests be followed after the Task Force has finished its work, and the City attempts to translate Task Force recommendations into actions or law.

Thank you for your continued work on this important topic.

Seth Hall
Tech Lead San Diego (member of the TRUST SD Coalition)
seth@s3th.com

Suggestions for the Chula Vista Privacy Task Force

Recommendation 1: Statement of Guiding Principles

The Task force should consider adding a statement of principles that can guide City staff on the Task Force's intentions once the Task Force has completed its work.

- Currently, the Task Force's recommendations are highly detailed. Any City staff that attempts to translate Task Force items into municipal code may be forced to make assumptions about the values and principles that guided the Task Force's recommendations.
- For example, the Task Force could state that all its recommendations are based in principles of public awareness, public benefit and public consent, and urge that any subsequent City efforts should strictly align to such principles.
- Any such statement would help ensure that the Task Force's detailed recommendations are not misconstrued to justify outcomes that the Task Force did not intend.

Recommendation 2: Approval for Acquisition and Use of Surveillance Technology

The Task Force should consider recommending that the City's proposed use policies be required to undergo advisory board review, and subsequent City Council approval, prior to acquiring or using surveillance technology. This requirement should be encountered at the earliest stages of surveillance technology acquisition or use.

- Currently, the Task Force recommendations do not require City Council approval prior to acquiring or using surveillance technology. The suggested requirements are only that contracts be presented and use policies be created and reviewed. No time frame or sequence for these presentations, creations and reviews is currently specified. No mechanism for rejection of a problematic technology is proposed by the Task Force.
- Without further requiring the City to achieve explicit City Council approval, City departments may continue to acquire and use technology without the knowledge of the public and City Council. All acquisitions and uses could be documented after-the-fact, after an undefined period of time, under the Task Force's current recommendations.

Additionally, unrecognized or obfuscated surveillance features of non-surveillance products could operate indefinitely without review, without consequences.

- This requirement for approval would ideally be encountered by the City prior to the phase of City staff seeking any funding for the acquisition or use.

Recommendation 3: Requirement of Impact Reports

The Task Force should consider recommending that the city be required to provide an impact report alongside any proposed use policy.

- Currently, the Task Force recommendations only require a Use Policy to be created for each surveillance technology. No impact reports are recommended.
- An impact report is a document that indicates the City has diligently investigated the impact its acquisition and use of technology will have on the public. The results discovered through the process of creating the impact report should heavily inform the City department's proposed use policy.
- Without requiring an impact report, City departments could draft a use policy without considering whether that use policy successfully reduces the threat of harm to the community, or whether the use policy successfully mitigates other risks created by the introduction of the surveillance technology.
- Impact reports are included as a definition in the Task Force's document, but they are not recommended.

Recommendation 4: Advisory Board's Conclusive Recommendation

The Task Force should consider recommending that the advisory board conclude its advisory work in each case by advising council members to approve, reject, or modify the proposed use policy.

- Currently, the Task Force recommendations only cover the advisory board reviewing and suggesting changes to use policies brought by the City. Rejection of use policies is not mentioned.
- For the advisory board to have maximum usefulness to council members, the advisory board should be required to make clear a recommendation that the proposal be accepted, modified, or rejected.

- In the case of the advisory board evaluating contracts with privacy implications, the

Recommendation 5: Advisory Board Evaluations

The Task Force should consider changing its draft recommendation to instead reflect that the advisory board drafts its own evaluation, independent of City staff.

- Currently, the Task Force recommendations state that any evaluations of contracts be written by a combination of City staff and the advisory board. *Procurement: 24.*
- Under the Task Force’s current recommendation, council members would be unable to determine if evaluations were the product of employed City staff, or if they were the product of independent community experts.
- The advisory board should author its own evaluations so that council members can benefit from knowing the evaluations originate from a board of independent community experts. Since City staff will be presenting final proposals to City Council, City staff already have ample opportunity to document and voice their own evaluations.

Recommendation 6: Educational Community Meetings Prior to Surveillance

The Task Force should consider recommending that the city hold public educational meetings prior to submitting the documents for review or approval.

- Currently, the Task Force is not recommending the City hold any public meetings prior to drafting the technology’s use policy, or prior to acquiring or using surveillance technology. *“Transparency and Oversight: 18(d)”*
- The City may benefit greatly from increased public trust, if it makes the effort to hold public meetings to present surveillance proposals prior to writing documents and acquiring or using technology.

Recommendation 7: Inventory of Existing Surveillance

The Task Force should consider recommending that all currently used surveillance technology be inventoried, and that list be provided to the advisory board as a public document as the first order of business for the advisor board.

Recommendation 8: City Council Approval Guidelines

The Task Force should consider recommending the conditions under which council members can determine a surveillance technology is eligible for City Council approval.

- Currently, the Task Force does not recommend the City obtain City Council approval prior to acquisition or use of surveillance technology. If such a recommendation was added, the Task Force should provide guidance to council members on the minimum circumstances that should be present before City Council gives approval for a surveillance technology.
- The Task Force should consider suggesting minimum, non-controversial preconditions for City Council's approval, such as requiring that the City Council judge that the technology's benefits outweigh its costs, or requiring City Council to judge that no better alternative exists.

Recommendation 9: Public Records

The Task force should consider recommending that any use policies (and impact reports, if the Task Force chooses to add a recommendation for them) created in this process be explicitly defined as public documents, regularly maintained and well-presented to the public.

Recommendation 10: Annual Surveillance Reports

The Task Force should recommend that annual reports be required for all surveillance technologies. The reports should review the ongoing cost, usefulness, and integrity of any approved surveillance technology.

- Currently, the Task Force does not recommend annual reports.
- Annual reports form the basis of ongoing oversight. They provide the advisory board and the City Council with opportunities to safeguard the rights of the public and to maximize budget efficiency, by identifying technologies that are not producing expected results. Annual reports also help the public understand how surveillance technology is benefiting public goals.

- The definition for Annual Reports is already included in the Task Force’s recommendation, but the Task Force does not currently have a recommendation that aligns with the definition.

Recommendation 11: Whistleblower Protections

The Task Force should consider that any non-compliant use of surveillance technology will be observed first by City staff. Encouraging those staff to report the non-compliant use to their supervisors is the most efficient and most desirable way to handle any such issues. If the Task Force agrees, then it should consider recommending the City adopt specific whistleblower protections, to ensure City staff feels they can safely report non-compliant activity, without risk of retaliation.

September 3, 2022

Adrianna Hernandez

Special Projects Manager | Office of the City Manager

City of Chula Vista | 276 Fourth Avenue, Chula Vista, CA 91910

619-691-5254 | ADHernandez@chulavistaca.gov

Let me preface my remarks by thanking you for the opportunity to comment on the proposed Summary of Policy Recommendations.

My comments are limited to the application of these recommendations as they impact law enforcement and more specifically the CVPD, Sheriff and National City.

I speak from a background in law and law enforcement having been a sworn member of the CVPD and SDSO and a licensed attorney representing clients in the area of civil litigation. I served on the 2021-22 County Grand Jury where my Law and Justice committee examined and extensively studied the issue of privacy rights and the impact of surveillance and modern technology on the public. The 2021-2022 Grand Jury published our findings and recommendations which can be found at: <http://www.sdcounty.ca.gov/grandjury>.

That being said, the recommendations being proposed are, I believe, incomplete and present potential serious issues concerning public welfare and safety.

2. “The Privacy Advisory Board should have nine members, at least two-thirds of whom are Chula Vista residents.”

It is no surprise that the authors specifically left out inclusion of representatives from law enforcement and victim’s rights advocates. The special interest groups, working under the guise of the San Diego TRUST coalition, drafted and presented the exact same recommendations for the City of San Diego. One only need look at the composition of that group to understand the real purpose behind their agenda. Best practices studies show that “city council decisions are more likely to be seen as fair and considerate if all people having a stake in the outcome” are involved. Asking nine people, none of whom have any experience in law enforcement, to make recommendations on what is acceptable use of a piece of modern technology is like asking a jury of nine to determine guilt or innocents after hearing testimony and seeing evidence from only one party to a case. At the August meeting of the Advisory group, a member of TRUST stated they were only interested in being sure that all members of the community were represented. It appears TRUST does not view law enforcement or victims of crime to be part of the Chula Vista community.

Using that as background, the recommendations fail to address serious concerns unique to law enforcement.

The CVPD works closely with the SDSO, which serves the unincorporated area of Bonita, and with the NCPD. The departments are often called upon to assist each other. This close symbiotic working relationship often requires sharing of information by each organization. That need for sharing must be recognized and incorporated in the guidelines the advisory board works and collaboration with outside agencies must be considered when recommending any rules on surveillance or use of equipment such as drones.

Along the same lines, the use of surveillance technology as it specifically applies to law enforcement cannot be adequately explained by a non-law enforcement lay person. Hence, any recommendations concerning use of technology must include specific and articulable rationale from the CVPD (or other L.E. sources) as to the appropriateness of the board's recommendation. If necessary, provisions should be included allowing such presentation to be made in a closed door session.

In addition, the CVPD has officers assigned to various state and federal task forces. In their roles, secret and sensitive information must be shared. Any attempt to quash that sharing might jeopardize further participation by CVPD personnel and affect public safety. Clarification with regard to sharing of such data should be included. Once again, this will require input from high level members of the CVPD.

Finally, I see no provision for discussion of sensitive material among the advisory board members. Secrecy should be addressed and violations should be subject to criminal and/or administrative sanctions.

Once again, I thank you for providing the opportunity to address these issues.

Jeremy Ogul

From: Robert Johnson <[REDACTED]>
Sent: Thursday, August 25, 2022 6:19 PM
To: privacytaskforce@chulavistaca.gov
Subject: Fwd: Some of my concerns.

Warning:
External
Email

Sent from my T-Mobile 5G Device
Get [Outlook for Android](#)

From: Robert Johnson <[REDACTED]>
Sent: Thursday, August 25, 2022 6:18:50 PM
To: adhernandez@chulavistaca.gov <adhernandez@chulavistaca.gov>
Subject: Some of my concerns.

Some of the paper I've been looking at is call for service. In the data case numbers and many thing are identifiers and can be cross referenced with identifying data in call for service fire department. If they are public records that's the thing it's more detailed on the fire department. I think a standardized version should be ready available to both like the police already have. It's in power bi updates automatically and is very easy to get to. If privacy is a concern sending out city votes for another city to count let alone in machines not made in America. The dod has many hundreds of documents assessments of how nation security risks and what systems are a threat to have a secure election yet mail in ballots remain high risk and you embrace it. If privacy is a concern why are you all talking about noncitizen privacy. And not our privacy. I see a lack of knowledge and leadership thinking they know what makes America safe. Bet you can even fix ur own cell phone.. If u want threat assessment maybe go to the foia web search and read on past elections. We could hold 1000person in person ballots one day and everyone could feel safer about voting. He let's have voter ID so non citizens can't vote.

Sent from my T-Mobile 5G Device
Get [Outlook for Android](#)

Jeremy Ogul

From: John Richeson <[REDACTED]>
Sent: Saturday, August 27, 2022 12:13 PM
To: Adrianna Hernandez
Cc: Privacy Task Force
Subject: Re: Share your thoughts on privacy guidelines for the City of Chula Vista

**Warning:
External
Email**

The foundational recommendation that "The City should create written Use Policies that govern the use of each privacy-impacting technology and the data generated by those technologies" is so general and vague (with should meaning compliance is voluntary) as to be meaningless.

The duties of the Chief Privacy Officer should be:

1. Prepare and maintain an inventory of data systems within the City that collect, retain, and/or exchange citizen information with outside entities including, but not limited to: the DMV, County Assessor, State and Federal Government agencies, SDG&E, Republic Services, Community Power, telecommunication providers, credit agencies, law enforcement, and the courts.
2. Periodically assess, or have to be assessed, the justification for collecting, retaining and/or sharing of citizen information, and the vulnerabilities of departmental data systems to the release of citizen information without their consent to third parties.
3. Require data system owners and administrators to develop and enforce citizen data security using the latest available encryption and network protection technologies, together with administrative procedures to minimize human error.
4. Annually report to the City Council on the status of data systems within the City.

Respectfully,

John Richeson

"If it is worth doing, it is worth doing right"

On 08/25/2022 5:34 PM PDT Adrianna Hernandez <adhernandez@chulavistaca.gov> wrote:

Greetings,

After many meetings and many hours of work, the Chula Vista Technology and Privacy Advisory Task Force<<https://www.chulavistaca.gov/businesses/smart-city/projects/privacytaskforce>> has developed a draft set of policy recommendations for the City Manager.

Now it's your turn. The task force is looking for feedback from the public. A full draft of the policy recommendations<<https://www.chulavistaca.gov/home/showpublisheddocument/25071>> has been posted online, and community members are encouraged to provide comments in writing to privacytaskforce@chulavistaca.gov<mailto:privacytaskforce@chulavistaca.gov>.

Please send in your thoughts no later than Tuesday, Sept. 6 so they can be compiled and shared with task force members before their next meeting.

Additionally, you are welcome to attend and speak during the public comment session at the upcoming task force meeting on Monday, Sept. 12 or Monday, Sept. 26. Public comment is open from 6 to 6:20

p.m. and at the end of each meeting. There will be further opportunities to comment when a final report and policies are presented to the City Council in November.

Please feel free to share this information with anyone who may be interested. Thank you!

Sincerely,

Aдриanna Hernandez

Special Projects Manager | Office of the City Manager

City of Chula Vista | 276 Fourth Avenue, Chula Vista, CA 91910

619-691-5254 | ADHernandez@chulavistaca.gov<mailto:ADHernandez@chulavistaca.gov>

Jeremy Ogul

From: David Stucky [REDACTED]
Sent: Saturday, August 27, 2022 12:58 PM
To: privacytaskforce@chulavistaca.gov
Subject: Task Force Recommendations
Attachments: Summary of Policy Recommendations with comments.pdf

**Warning:
External
Email**

Attached is the task force document with comments and observations. Please feel free to contact me for any needed explanations or clarifications.

David Stucky
[REDACTED]

Notes

[Empty box for notes]

Chula Vista Technology and Privacy Advisory Task Force
Summary of Policy Recommendations
DRAFT VERSION – August 25, 2022

Note: To facilitate discussion and review, the policy recommendations are numbered in this document. There is no particular order or significance to the numbering scheme or the section headings in this draft.

Privacy Advisory Board

1. The City should establish a Privacy Advisory Board responsible for carrying out a broad range of advisory duties.
 - a. The Board’s duties are described throughout this document, including:
 - i. Holding regular meetings that are open to the public, including opportunities for public comment in English and other languages.
 - ii. Reviewing Use Policies for privacy-impacting technologies and making recommendations on changes
 - iii. Reviewing data sharing agreements.
 - iv. Reviewing new technology-related contracts.
2. The Privacy Advisory Board should have nine members, at least two-thirds of whom are Chula Vista residents.
 - a. Chula Vista residents should comprise a super-majority of Board members because residents experience the impacts of City decisions on privacy and technology to a much greater degree than non-residents do.
 - b. The purpose of allowing non-residents to serve on the Board is to recognize that non-residents also experience the impacts of City decisions on privacy and technology, especially if they work, own a business, or attend school in Chula Vista. Additionally, non-residents may have valuable expertise or perspectives that should be included on the Board.
 - c. There is no requirement to include non-residents on the Board.
3. Privacy Advisory Board members will be selected through a combination of City staff review, community review, and City Council review.
 - a. Members of the Board should be selected through a process that includes review and vetting by both City staff and by community leader similar to the process used to appoint members of the Technology and Privacy Advisory Task Force.
 - b. All members of the Board must be approved by a majority vote of the City Council pursuant to the City Charter.
 - c. The purpose of involving community leaders in the selection process for some members is to ensure that Board membership is not exclusively determined by City staff or elected officials.
4. Selections to the Board should reflect the City’s diversity in terms of race, gender, and age.

| | | |
|---|------|---------------------|
| 1 | Dave | 08/27/2022 12:14:58 |
| This should be the only criterion for including non-residents | | |
| 2 | Dave | 08/27/2022 12:16:10 |
| Define community leader. | | |

Notes

Empty box for notes.

All Board members shall be persons who have an interest in privacy rights as demonstrated by work experience, civic participation, and/or political advocacy.

No member may be an elected official.

No member may have a financial interest, employment, or policy-making position in any commercial or for-profit facility, research center, or other organization that sells surveillance equipment or profits from decisions made by the Board.

Each of the following perspectives should be represented by at least one member of the Board:

- a. A resident of Council District 1
- b. A resident of Council District 2
- c. A resident of Council District 3
- d. A resident of Council District 4
- e. A technology professional with expertise in emerging technologies and systems (this perspective should be represented by three members of the board)
- f. A professional financial auditor or Certified Public Accountant (CPA)
- g. An attorney, legal scholar, or recognized academic with expertise in privacy and/or civil rights
- h. A member of an organization that focuses on government transparency or individual privacy
- i. A representative from an equity-based organization or a member of the Human Relations Commission.
- j. A former member of the Technology and Privacy Advisory Task Force (only applies to the first year of appointments)

Chief Privacy Officer

- 5. The City should hire a full-time Chief Privacy Officer responsible for carrying out a broad range of duties related to privacy.
 - a. Until a full-time Chief Privacy Officer can be budgeted and hired, the duties of the Chief Privacy Officer should be carried out by the Chief Information Security Officer.
 - b. The Chief Privacy Officer should report to the City Manager to ensure they are accountable to City Council and the voters of Chula Vista.
 - i. A minority of task force members believes the Chief Privacy Officer should report to the City Attorney to ensure they are accountable to the voters of Chula Vista.
 - c. The Chief Privacy Officer's responsibilities include, but are not limited to:
 - i. Provide regular training sessions and guidance to City staff on privacy issues.
 - ii. Serve as the primary City staff liaison to the Privacy Advisory Board, including:
 - 1. Managing agendas and coordinating meetings

| | | |
|--|------|---------------------|
| 1 | Dave | 08/27/2022 12:20:04 |
| Don't forget the need for an appropriate level of support staff. | | |

| | | |
|--|------|---------------------|
| 2 | Dave | 08/27/2022 12:13:14 |
| In a representative democracy, the City Council are the representatives of the voters. | | |

Notes

Empty box for notes.

- 2. Managing the selection process for Privacy Advisory Board members
- 3. Assisting in the preparation and presentation of technology Use Policies for Board review
- iii. Performing internal audits and ensuring compliance with data retention standards and use policies, and coordinating with external privacy auditors when applicable
- iv. Evaluating new technology acquisitions for potential privacy issues

Use Policies

- 6. The City should create written Use Policies that govern the use of each privacy-impacting technology and the data generated by those technologies.
 - a. Each policy should clearly state the purpose of the technology, who will be allowed to access the technology, how the technology can be used, what kind of data the technology generates, how that data can be used, how that data is protected, and the retention period for that data.
- 7. Use Policies should be drafted by the applicable department in consultation with the Chief Privacy Officer, then reviewed by the Privacy Advisory Board.
 - a. Departments will use a template created by the Chief Privacy Officer.
- 8. Use Policies should be reviewed annually and updated if necessary. Use policies should also be reviewed and updated any time there is a significant change in the function or purpose of the technology.
- 9. Due to the large number of use policies that may need to be created or updated, the Chief Privacy Officer and Privacy Advisory Board will perform an analysis that prioritizes current and future technologies based on the impact and risks to individual privacy. Based on the results of this analysis, use policies will be reviewed for the highest-ranked technologies first.
 - a. Facial recognition technology, other biometric systems, surveillance systems, and systems that use machine learning algorithms should be a top priority for Board review.

Data Retention and Data Sharing

- 10. The City should never sell the data it collects nor allow third parties working on behalf of the City to sell or use data owned by the City except as necessary to provide the contracted service to the City.
- 11. Internal data-sharing between City Departments should be subject to a review process that includes approval by the City Manager and periodic review by the Chief Privacy Officer and Privacy Advisory Board.
 - a. The purpose of this policy recommendation is to ensure there is a clear understanding of how data is being used and shared between departments, and to

Notes

prevent situations where there is uncertainty around how data is being used, such as in the case of the informal data-sharing that occurred between Engineering and the Police Department regarding traffic signal camera feeds.

12. External data-sharing between the City and third parties must be approved through a formal, auditable process that includes the Chief Privacy Officer and Privacy Advisory Board.
 - a. The purpose of this policy recommendation is to prevent situations like the sharing of ALPR data with law enforcement agencies that should not have had access to it.
 - b. The review should ensure that personal information is not being shared and that the data has been repackaged and de-identified to minimize the possibility of privacy violations.
13. The City Records Retention Schedule should be re-organized and expanded to include information on what personal data is collected and when that data will be deleted.
 - a. As part of these updates, the Records Retention schedule should be presented in a format that provides a category for data type in addition to the existing categories.
 - b. The Chief Privacy Officer should collaborate with the City Clerk to lead this process.
14. The City should establish a more formal process for ensuring that personal data is being deleted according to the Use Policies established for that data.
15. The City should establish a policy that it will not collect personal data unless it is absolutely necessary to provide the core service.
 - a. The Chula Vista Public Library's approach to personal data is a model that should be followed citywide. Personal data is only collected and retained for the period necessary to provide the service. For example, the library keeps a record of an item checked out by an individual borrower only until that item is returned, at which point data related to that transaction is deleted.
 - b. To ensure compliance with this policy, the Chief Privacy Officer should randomly sample Departments or data sets to review on a periodic basis.
16. Where possible, the City should anonymize, remove, or de-identify data that relates to a person.
 - a. It must be understood and acknowledged that anonymization strategies will not completely protect individuals from having their identities reverse-engineered from otherwise anonymized datasets, but these strategies are still valuable in mitigating risks to individual privacy.
17. The role of the City's Data Governance Committee should be more clearly defined and communicated to the public.
 - a. The City should ensure that the work of the Data Governance Committee is consistent with the City's adopted privacy policies and with the role or recommendations of the Privacy Advisory Board.

Notes

Transparency and Oversight

- 18. City staff should provide the public with full disclosures about what technologies have been acquired, what data is being collected, and how that data is being used.
 - a. These disclosures should happen in a variety of ways, including on the City’s website, through email newsletters, social media, and in printed communications mailed to residents.
 - b. These disclosures should address what data is being collected, what department is collecting it, how it is being used, who has access to it, how long it is retained, etc.
 - c. Where feasible, signs should be posted to notify and disclose surveillance technology. For example, if surveillance cameras are added to parks, signs should be posted notifying visitors that they are under video surveillance.
 - d. The City should hold public forums, educational seminars, and other types of community events to ensure the public is informed and has an opportunity to hold the City accountable for how privacy-impacting technologies are being used.
 - e. All public disclosures related to technology, data, and privacy should be provided with adequate time for public review before any meeting. The 72-hour standard is not sufficient for the public to review and consider new information, especially when that time period coincides with weekends and holidays.

- 19. Information about privacy and technology that is provided on the City website should be easy to find and easy to understand.
 - a. Links to disclosures should be provided on each Department’s page within the City website.
 - b. The City’s “smart city” webpages should have their own navigational tab or section on the City website, rather than being contained under the Business / Economic Development section.

- 20. Contracts with technology vendors should be easy for the public to find and review.
 - a. This should include information about the status of existing contracts, including upcoming renewal or termination dates.

- 21. Data breaches should be publicly disclosed as soon as possible.
 - a. Notification should happen within 24 hours of the data breach being confirmed.
 - b. Notification should occur through a wide range of communications channels, including social media, news media, and the City website.

- 22. Residents should have the opportunity to opt-out or have their data deleted if it was provided voluntarily to the City and is not needed for City operations.
 - a. It is understood that individuals will not be able to opt-out of certain types of data collection, such as a drone responding to 9-1-1 calls, or medical data being retained following a emergency medical service call.

1 | Dave | 08/27/2022 12:30:38
 Contracts with technology vendors should be subject to the same disclosure standards as those of any other vendor contracts.

2 | Dave | 08/27/2022 12:33:34
 "Voluntarily" provided data implies the option to decline to provide in the first place. And if it not needed for City operations, it probably should not have been collected in the first place.

Notes

Procurement

- 23. All contracts with privacy implications  must be presented to the City Council, regardless of whether they meet standard purchasing  and contracting thresholds that typically trigger City Council review.
- 24. Prior to City Council presentation, contracts with privacy implications must be reviewed by the Chief Privacy Officer and the Privacy Advisory Board. The evaluation provided by the Chief Privacy Officer and the Privacy Advisory Board must be included as part of the report presented to City Council.
- 25. When acquiring new technology systems, the Chief Information Security Officer and Chief Privacy Officer should prepare an assessment of the technology's potential impact on the City's information security and detail any mitigation strategies. This assessment should be provided to the Privacy Advisory Board and the City Council at the same time as any other documents provided for review, such as the contract for the technology (Item 24) and the technology's proposed Use Policy (Item 7).
- 26. The City may not enter into any agreement that prohibits the City from publicly  acknowledging that it has acquired or is using a particular technology. Nondisclosure  agreements are acceptable only to extent that they protect a vendor's proprietary information without prohibiting the City's acknowledgement of a relationship with the vendor.
- 27. Contracts should include a clause of convenience that allows the City to terminate the  agreement in the event the vendor violates any restriction on the sale or sharing of data  otherwise violates individual privacy protections.
- 28. Technology contracts should require that vendors provide the City with the capability to audit or review who has accessed what information.
 - a. These access reports should be provided at pre-designated intervals to City staff or third-party auditors.
- 29. City staff should be provided with additional training to assist in recognizing potential data privacy issues in contracts.
 - a. Key staff to receive additional training includes the Chief Privacy Officer, Chief Information Security Officer, City Attorney staff, and purchasing and contracting staff.
- 30. Changes in the ownership of a privacy-impacting technology that has already been reviewed by the Privacy Advisory Board should trigger a new review by the Privacy Advisory Board.

- 1 | Dave 08/27/2022 12:36:17
"Privacy implications" is too broad a term. The standard needs to be more narrowly defined.
- 2 | Dave 08/27/2022 12:38:59
It is not inconceivable that an agreement with, for example, a federal agency could reasonably prohibit public disclosure.
- 3 | Dave 08/27/2022 12:40:15
Virtually all municipal contracts should already include the right to terminate for convenience.

Notes

Information Security

31. Establish a comprehensive information security policy that addresses procedures for maintaining and controlling access to data and articulates the roles and responsibilities of data stewards and data custodians.
 - a. An outline of such a policy has been developed by the Information Security subcommittee of this Task Force and will be submitted as part of this recommendation.
 - b. The policy should make clear that only City-owned mobile equipment using two-factor authentication should be allowed to connect to the City's primary network. Any personal devices connecting to the City's network must use restricted "guest" access.
 - c. The policy should provide for audits of all City-owned equipment to protect against unauthorized storage of regulated data.
 - d. The policy should require data security breaches to be reviewed and addressed by an established panel that includes the Director of Information Technology Services, the Chief Information Security Officer, the Chief of Police, the City Attorney, and the Chief Privacy Officer.
 - e. The policy should require that data is stored and transmitted in encrypted formats whenever possible and prohibit the communication of confidential data through end-user messaging technologies such as email, instant messaging, chat, or other communication methods.
 - f. The policy should specifically address mobile computing devices, including recovery of data in the event a mobile computing device is lost or stolen.

Additional Comments

The Task Force has received multiple public comments regarding the methodology used to conduct the public opinion survey and focus groups. The Task Force encourages City staff and City Councilmembers to consider the potential for bias in the results of the public opinion research, particularly as described in the letter from Dr. Norah Shultz of San Diego State University, which was provided as part of the August 15 Task Force meeting agenda.

Notes

Empty box for notes.

Appendix A: Definitions
DRAFT – August 25, 2022

1 “Annual Surveillance Report” means a written report concerning a specific surveillance technology that includes all the following:

- a. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
- b. Whether and how often data acquired through the use of the surveillance technology was shared with internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s) except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- c. Where applicable, a description of the physical objects to which the surveillance technology hardware was installed without revealing the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
- d. Where applicable, a description of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
- e. A summary of community complaints or concerns about the surveillance technology, and an analysis of its Surveillance Use Policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals;
- f. The results of any internal audits or investigations relating to surveillance technology, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. To the extent that the public release of such information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law;
- g. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- h. A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate

| | | |
|--|------|---------------------|
| 1 | Dave | 08/27/2022 12:52:45 |
| Nowhere in this report is surveillance mentioned until now. Where does this come from and how does this fit into the overall scheme of the report? Who is responsible for the creation of this "Annual Surveillance Report" and to whom is it presented? | | |

Notes

Empty box for notes.

security interests of the City;

I. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;

i. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates, such as the number of Public Records Act requests on such surveillance technology and the open and close date for each of these Public Records Act requests;

j. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the surveillance technology in the coming year; and

k. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "City" means any department, unit, program, and/or subordinate division of the City of Chula Vista as provided by Chapter XXXX of the Chula Vista Municipal Code.

3. "City staff" means City personnel authorized by the City Manager or appropriate City department head to seek City Council Approval of Surveillance Technology in conformance with this Chapter.

4. "Community meeting" means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of surveillance technology on disadvantaged groups.

5. "Continuing agreement" means a written agreement that automatically renews unless terminated by one or more parties.

6. "Exigent circumstances" means a City department's good faith belief that an emergency involving imminent danger of death or serious physical injury to any individual requires the use of surveillance technology that has not received prior approval by City Council.

7. "Facial recognition technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.

8. "Individual" means a natural person.

9. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet-accessing device, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.

Notes

10. "Police area" refers to each of the geographic districts assigned to a Chula Vista Police Department captain or commander and as such districts are amended from time to time.

11. "Sensitive personal information" will reflect the California Privacy Rights Act (CPRA) definition of personal information which defines the term to include:

- (1) personal information that reveals:
 - (A) a consumer's social security, driver's license, state identification card, or passport number;
 - (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
 - (C) a consumer's precise geolocation;
 - (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
 - (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
 - (F) a consumer's genetic data; and
- (2)
 - (A) the processing of biometric information for the purpose of uniquely identifying a consumer;
 - (B) personal information collected and analyzed concerning a consumer's health; or
 - (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

12. "Surveillance" (or "spying") means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the individual.

13. "Surveillance technology" means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, or system utilizing an electronic device used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such surveillance technology. Examples of surveillance technology include, but are not limited to the following: cell site simulators (Stingrays); automated license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that can record audio or video and transmit or be remotely accessed. It also includes software designed to monitor social media services or forecast and/or predict criminal activity or criminality, and biometric identification hardware or software. "Surveillance technology" does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology beyond what is set forth below or used beyond a purpose as set forth below:

Notes

- a. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any public surveillance or law enforcement functions related to the public;
- b. Parking Ticket Devices (PTDs) used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;
- c. Manually-operated, non-wearable, handheld digital 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;
- d. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- e. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- f. City databases 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;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes;
- h. Police department interview room cameras;
- i. City department case management systems;
- j. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above;
- k. Surveillance technology used by the City solely to monitor and conduct internal investigations involving City employees, contractors, and volunteers; and,
- l. Systems, software, databases, and data sources used for revenue collection on behalf of the City by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other City department or third-party except as part of efforts to collect revenue that is owed to the City.

14. "Surveillance Impact Report" means a publicly-posted written report including, at a minimum, the following:

- a. Description: Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

Notes

- b. Purpose: Information on the proposed purposes(s) for the surveillance technology;
- c. Location: The physical or virtual location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
- d. Impact: An assessment of the Surveillance Use Policy for the particular technology and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities;
- e. Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;
- f. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including open source data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
- g. Data Security: Information about the controls that will be designed and implemented to ensure that adequate security objectives are achieved to safeguard the data collected or generated by the surveillance technology from unauthorized access or disclosure;
- h. Fiscal Costs and Sources: The forecasted, prior, and ongoing fiscal costs for the surveillance technology, including initial purchase, personnel, and other ongoing costs, and any past, current or potential sources of funding;
- i. Third-Party Dependence: Whether use or maintenance of the surveillance technology will require data gathered by the surveillance technology to be handled or stored by a third-party vendor at any time;
- j. Alternatives: A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate;
- k. Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed surveillance technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the surveillance technology such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the surveillance; and
- l. Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and City departmental responses given, and City departmental

Notes

conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of surveillance technology.

15. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:

- a. Purpose: The specific purpose(s) that the surveillance technology is intended to advance;
- b. Use: The specific uses that are authorized, and the rules and processes required prior to such use;
- c. Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the surveillance technology, as well as data that might be inadvertently collected during the authorized uses of the surveillance technology and what measures will be taken to minimize and delete such data. Where applicable, any data sources the surveillance technology will rely upon, including open source data, should be listed;
- d. Data Access: The job classification of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e. Data Protection: The safeguards that protect information from unauthorized access, including logging, encryption, and access control mechanisms;
- f. Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), 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;
- g. Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants;
- h. Third Party Data Sharing: If and how information obtained from the surveillance technology can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i. Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
- j. Auditing and Oversight: The procedures used to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the surveillance technology or access to information

Notes

collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and

k. Maintenance: The procedures used to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Notes

Information Security Subcommittee Report
 August 15, 2022
 Members: Charles Walker and Carlos De La Toba

Recommended City Information Security Policies

PURPOSE: To provide guidelines with regard to the responsibility of every City of Chula Vista (City) employee who accesses Data and information in electronic formats and to provide for the security of that Data and to restrict unauthorized access to such information.

POLICY: Electronic Data is important to the City assets that must be protected by appropriate safeguards and managed with respect to Data stewardship. This policy defines the required Electronic Data management environment and classifications of Data, and assigns responsibility for ensuring Data and information privacy and security at each level of access and control.

SCOPE AND APPLICABILITY: This policy applies to all City personnel and affiliated users with access to City Data.

DEFINITIONS:

Affiliated Users: Vendors and guests who have a relationship to the City and need access to City systems.

Application or App: A software program run on a computer or mobile device for the purpose of providing a business/academic/social function.

Cloud: An on-demand availability, geographically dispersed infrastructure of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the end user. Clouds may be limited to a single organization (Private Cloud), or be available to many organizations (Public Cloud). Cloud-computing providers offer their “services” according to three standard models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Confidential Data: Data that are specifically restricted from open disclosure to the public by law are classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Confidential Data include, but are not limited to:

- Medical Data, such as Electronic Protected Health Information and Data protected by the Health Insurance Portability and Accountability Act (HIPAA);
- Investigation. Only investigation data and information within the following broad categories is to be considered Confidential Data:
 - Active Investigations;
 - Activity that is covered by a fully executed non-disclosure agreement (NDA);
 - Information, data, etc., that is proprietary or confidential (whether it belongs to an internal investigator or an outside collaborator), regardless of whether it is subject to an NDA;
 - Information or data that is required to be deemed confidential by state or federal law (e.g., personally identifying information about research subjects, HIPAA or FERPA protected information, etc.); and
 - Information related to an allegation or investigation into misconduct.
- Information access security, such as login passwords, Personal Identification Numbers (PINS), logs with personally identifiable Data, digitized signatures, and encryption keys;

Notes

- Primary account numbers, cardholder Data, credit card numbers, payment card information, banking information, employer or taxpayer identification number, demand deposit account number, savings account number, financial transaction device account number, account password, stock or other security certificate or account number (such as Data protected by the Payment Card Industry Data Security Standard) ;
- Personnel file, including Social Security Numbers;
- Library records;
- Driver’s license numbers, state personal identification card numbers, Social Security Numbers, employee identification numbers, government passport numbers, and other personal information that is protected from disclosure by state and federal identity theft laws and regulations.

Data Classifications: All Electronic Data covered by this policy are assigned one of three classifications:

- Confidential
- Operation Critical
- Unrestricted

Data Custodian: Persons or departments providing operational support for an information system and having responsibility for implementing the Data Maintenance and Control Method defined by the Data Steward.

Data Maintenance and Control Method: The process defined and approved by the Data Steward to handle the following tasks:

- Definition of access controls with assigned access, privilege enablement, and documented management approval, based on job functions and requirements.
- Identification of valid Data sources
- Acceptable methods for receiving Data from identified sources
- Process for the verification of received Data
- Rules, standards and guidelines for the entry of new Data, change of existing Data or deletion of Data
- Rules, standards and guidelines for controlled access to Data
- Process for Data integrity verification
- Acceptable methods for distributing, releasing, sharing, storing or transferring Data
- Acceptable Data locations
- Providing for the security of Confidential Data and Operation Critical Data
- Assuring sound methods for handling, processing, security and disaster recovery of Data
- Assuring that Data are gathered, processed, shared and stored in accordance with the City privacy statement **(to be written)**.

Data Steward: The persons responsible for City functions and who determine Data Maintenance and Control Methods are Data Stewards.

Electronic Data/Data: Distinct pieces of information, intentionally or unintentionally provided to the City in a variety of administrative, academic and business processes. This policy covers all Data stored on any electronic media, and within any computer systems defined as a City information technology resource.

Mobile Computing Devices: Information technology resources of such devices include, but are not limited to, laptops, tablets, cell phones, smart phones, and other portable devices.

Operation Critical Data: Data determined to be critical and essential to the successful operation of the City as a whole, and whose loss or corruption would cause a severe detrimental impact to continued operations.

Notes

Data receiving this classification require a high level of protection against accidental distribution, exposure or destruction, and must be covered by high quality disaster recovery and business continuity measures. Data in this category include Data stored on Enterprise Systems such as Data passed through networked communications systems. Such Data may be released or shared under defined, specific procedures for disclosure, such as departmental guidelines, documented procedures or policies.

City Provided Data Systems: Information technology resources, as defined and described by the City and used for the storage, maintenance and processing of City Data.

Unrestricted Data: Information that may be released or shared as needed.

Usage/Data Use: Usage and Data Use are used interchangeably and are defined as gathering, viewing, storing, sharing, transferring, distributing, modifying, printing and otherwise acting to provide a Data maintenance environment.

PROCEDURES:

1. Data Stewardship

Data Stewards are expected to create, communicate and enforce Data Maintenance and Control Methods. Data Stewards are also expected to have knowledge of functions in their areas and the Data and information used in support of those functions. The Chief Information Officer(CIO) is ultimately accountable for the Data management and stewardship of all the City data. The CIO may appoint others in their respective areas of responsibility.

2. Data Maintenance and Control Method

Data Stewards will develop and maintain Data Maintenance and Control Methods for their assigned systems.

When authorizing and assigning access controls defined in the Data Maintenance and Control Methods involving Confidential Data and Operation Critical Data, Data Stewards will restrict user privileges to the least access necessary to perform job functions based on job role and responsibility.

If the system is a City Provided Data System, City Technology Services will provide, upon request, guidance and services for the tasks identified in the Data Maintenance and Control Method.

If the system is provided by a Public Cloud, the Data Steward must still verify that the Data Maintenance and Control Method used by the Public Cloud provider meets current City technology standards **(to be written)?**. Further, ongoing provisions for meeting current City technology and security standards **(to be written)?** must be included in the service contract.

Review of Public Cloud solutions must include City Technology Services and City Attorney prior to final solution selection and purchase.

Use of personal equipment to conduct City business must comply with all guidance provided by City policies **(to be written)?**.

3. Data Custodianship

Data Custodians will use Data in compliance with the established Data Maintenance and Control Method. Failure to process or handle Data in compliance with the established method for a system will be considered a violation of the City policies.

Notes

4. Data Usage

In all cases, Data provided to the City will be used in accordance with the Privacy Statement **(to be written)** Software solutions, including SaaS solutions, are selected to manage Data and are procured, purchased and installed in conjunction with City (to be written)

Data will be released in accordance with City (to be written). Requests for information from external agencies (such as Freedom of Information Act requests, subpoenas, law enforcement agency requests, or any other request for Data from an external source) must be directed to the City Attorney and processed in accordance with existing policies.

Standards for secure file transmissions, or Data exchanges, must be evaluated by the CIO when a system other than a City Provided Data System is selected or when a Public Cloud is utilized. Specific contract language may be required. The City Attorney must be consulted regarding such language.

Unencrypted authorization and Data transmission are not acceptable.

Communication of Confidential Data via end-user messaging technologies (i.e., email, instant messaging, chat or other communication methods) is prohibited

5. Storing Data

Data cannot be stored on a system other than a City Provided Data System without the advance permission of the Data Steward and demonstrated legitimate need.

Data should be stored in encrypted formats whenever possible. Confidential Data **must** be stored in encrypted formats. Encryption strategies should be reviewed with City Technology Services in advance to avoid accidental Data lockouts.

Data cannot be stored on a City-provided Computing Device unless the device is encrypted without the advance permission of the Data Steward and demonstrated legitimate need.

Data must be stored on devices and at locations approved by Data Stewards. If information technology resources (computers, printers and other items) are stored at an off-campus location, the location must be approved by Data Stewards prior to using such resources to store City Data.

Technology enables the storage of Data on fax machines, copiers, cell phones, point-of-sale devices and other electronic equipment. Data Stewards are responsible for discovery of stored Data and removal of the Data prior to release of the equipment.

When approving Mobile Computing Device Usage, Data Stewards must verify that those using Mobile Computing Devices can provide information about what Data was stored on the device (such as a copy of the last backup) in the event the device is lost or stolen.

In all cases, Data storage must comply with City retention policies. Data Usage in a Public Cloud system must have specific retention standards**(to be written)?** written in the service contract. The City Attorney must be consulted regarding such language.

Provisions for the return of all City Data in the event of contract termination must be included in the contract, when Data is stored on a Public Cloud. The City Attorney must be consulted regarding such language. Current

Notes

Empty box for notes.

security standards **(to be written)?** (such as controlled access, personal firewalls, antivirus, fully updated and patched operating systems, etc.) will be evaluated when a system other than a City Provided Data System is selected and must be covered in contract language. The City Attorney must be consulted regarding such language.

Data stored on Mobile Computing Devices must be protected by current security standard methods (such as controlled access, firewalls, antivirus, fully updated and patched operating systems, etc.). City standard procedures **(to be written)** for the protection and safeguarding of Confidential Data and Operation Critical Data must be applied equally and without exception to City Provided Data Systems, Mobile Computing Devices and systems other than City Provided Data Systems, such as Public Cloud solution.

6. Systems and network Data

Systems and network Data, generated through systems or network administration, logs or other system recording activities, cannot be used, or captured, gathered, analyzed or disseminated, without the advance permission of the Chief Information Officer.

7. Value of Data

In all cases where Data are to be processed through a Public Cloud, the following assessment must be done: The value of the Data must be determined in some tangible way. Signature approval from the Data Steward’s division vice president or appropriate party with the ability to authorize activity at the level of the value of the Data must be obtained.

8. Sanctions

Failure to follow the guidelines contained in this document will be considered inappropriate use of a City information technology resource and therefore a violation of the City policy**(to be written)**.

9. Data Security Breach Review Panel

A Data Security Breach Review Panel (Panel) comprised of the following members will be established:

- Chief Information Officer
- Chief of Police
- City Attorney
- Chief Privacy Officer

10. Data Loss Prevention Software

Define granular access rights for removable devices and peripheral ports and establish policies for users, computers and groups, maintaining productivity while enforcing device security

11. Audits

All City owned equipment is subject to audit for unauthorized storage of regulated data. Devices authorized to store regulated data are subject to audits as deemed necessary by the CIO. Reasonable prior notification of an audit will be provided. Audit results are handled confidentially by Information Security staff and are reported to the CIO in aggregate.

12. Mobile Devices

City owned mobile equipment will be exclusively allowed on the City’s primary network and use two factor authentication. All personal devices must use “guest” access if provided.

Notes

Jeremy Ogul

From: [REDACTED]
Sent: Tuesday, September 6, 2022 2:09 PM
To: privacytaskforce@chulavistaca.gov
Subject: Community input

Warning: External Email

To whom it may concern,

I am a Chula Vista resident, home owner in Otay Ranch community since 2008, a working RN, married with 3 children. Me and my husband both support the increased monitoring in our city/community. We are happy that our hard earned tax dollars were spent to provide the drone first responder service to our CVPD. In my opinion the more eyes we have on our community the better, the safer our city community our neighborhoods will be. I do not care if I have camera's on my house, drones flying over my backyard ext. That makes me and my children feel safer. Our neighborhood so far has been a very safe and family welcoming neighborhood- with kids walking and riding bike independently, seniors walking there dogs, parks without issues of homelessness or petty crime, absence of graffiti ext. So I trust our CVPD to use the monitor technology at there will- whatever they have been doing so far has been working great. Keep up the good work for people like me and my family CVPD!

Gina Velasco
Zip 91913

From: Eric Wood [REDACTED]
Sent: Sunday, August 28, 2022 10:03 PM
To: privacytaskforce@chulavistaca.gov
Subject: Feedback on DRAFT Policy Recommendations

**Warning:
External
Email**

Hello,

My name is Eric Wood and I am a resident of Chula Vista. In the past, I was the Police Technology Manager and Smart Technology Officer for the City of Chula Vista. I currently have no official or formal relationship or role with the city aside from being a resident and former employee. I have spent over 20 years as a technology consultant, much of that was under the employment of Microsoft. I have also worked in the public sector driving technology innovation, security and compliance. I hold CISSP and CCSP credentials for information system security. I'm currently employed by a private sector firm which helps law enforcement gain insights from their existing data systems; which are often separated in vendor, departmental or technology silos. I'm accustomed to dealing with very sensitive data sets and security compliance that must meet FBI standards (CJIS) and NIST:800-53.

I have attended several of the task force meetings at the Council Chambers and the public engagement event at the Otay Ranch Library.

With that background, let me offer you some of my feedback after reviewing the DRAFT Policy Recommendations that the task force has published for comment.

General Feedback:

As a whole, I believe that the task force is misguided with their approach in several aspects. It is my opinion that the purpose of the task force was to propose policies or practices for the purpose of establishing safe and reasonable protections against the misuse or abuse of Personally Identifiable Information within the city. However, what I notice in the discussions at meetings and within the proposed policies and practices is a much more controlling or gating role in city operations born from a foundation of mistrust. I will provide some specific examples to support this observation.

This DRAFT policy recommendations document reads as if this was a Surveillance Task Force. There are 68 occurrences of the word 'Surveillance' in the document. Please consider the impression that your language will leave on the public and be leveraged by the media to create negative connotations that are unwarranted in my opinion. The focus should be on data privacy protections...yes surveillance systems are an element of privacy protections but the systems this task force is aware of and have described as surveillance systems include the Police Drones and LPR cameras, neither of which collect identifiable information...you would have to take information from those and have **access and cause** to search another system in order to make any identification....and that's not identifying the occupants...just the registered owner. My ask here is for the task force to rebalance the language used with the purpose and real risk that exists today to privacy. An ongoing PAB would keep those in check down the road...but I believe this heavy lean on the use of surveillance is not warranted and does not serve the city or the citizens. It's unnecessarily alarming and if you outline these to the average citizen, as has been done for each of you, they would agree that it's been overblown.

Specific Points of Feedback:

Section 1.A.II through 1.A.IV – The language used here implies (based on other language and open discussion at the task force meetings) that the Policy Advisory Board (will review Use Policies, Data Sharing Agreements and new technology-related contracts) in a gating function...meaning if the outcome of the review is not satisfactory then some delay or denial will occur as a result. In reality, Use Policies, Data Sharing Agreements and Contracts are all discoverable and there's no need to include this within the recommendations unless the intent is for the PAB to act as a gating function. The PAB should absolutely review those and provide any recommended changes to the city manager's office

and the CISO. The PAB will not have the requisite background and training in Federal, State and Local laws on contracting, interagency collaboration, mutual-aid and jurisdiction. I recommend clarifying that these types of documents may be reviewed along with other established (not proposed, planned or work-in-progress) policies, practices and contracts, just as any member of the public is able to.

Section 5 – I strongly disagree with the recommendation for a Chief Privacy Officer. Managing and being accountable for data privacy is included in the discipline and profession of a Chief Information Security Officer. Data is both an asset and a liability. If PII data is not adequately protected against misuse, abuse, manipulation, denial of access or unwanted disclosure then this is an Information Security problem. How many other cities that are comparable to Chula Vista do you see with a Chief Privacy Officer? This would be an anomaly and it's poorly envisioned in my opinion. I would not be surprised if this recommendation was not supported by the City Manager. If what you are concerned about is that there is clear accountability and job focus, then a more preferred approach in my opinion would be to recommend that the CISO must personally report progress/challenges regarding Data Privacy to the City Attorney and Risk Management Officer and in order to conduct the desired level of internal audits, investigations of practices not aligned with policy, then an analyst position should be created to perform the discovery, monitoring and reporting of data privacy related activities, developments, areas of non-compliance to the CISO. The CISO must be capable of managing the city's cybersecurity posture and strike a balance between usability for city functions and security and compliance for risk management. The CISO should have direct oversight of external audits or vendors which may periodically augment the data privacy or cyber security functions.

Section 11 – Internal data sharing between city departments should be encouraged. This is actually a core competency that underpins smart-cities and more effective/efficient government services. The Data owner is ultimately the department head that is deciding the if, who, what, where, when, how and why they would share their departments data with another city department. Are there concerns about oversharing or how the information will be utilized by the other city department, absolutely. But I guarantee that those city department heads and their senior managers will work through those details. I know this because I was involved in the example used by the task force. The 'informal sharing agreement' between Traffic Engineering and the Police Department. I directly led this effort from the PD by requesting access from Traffic Engineering. The Distinguished Traffic Engineer went directly to the department head to seek authorization. We outlined use cases, permissions, authorized personnel, etc. This was handled in email, phone calls and face-to-face meetings. To what degree of formality does the task force desire department heads to work together to save the taxpayer money while also improving service delivery? The video management system that enabled this sharing was under the control of the Data Owner and the permissions and audit logs assured that only the agreed upon people and permissions were utilized. This is another area where the Task Force is over-stepping what is being asked....describe the safe-guards you would like to see, don't inject a review process and a board that bogs down good public service leaders making responsible decisions. Please focus on transparency and trust....let periodic audits by the CISO verify that the safety measures are having the desired effect.

Section 12 – External data sharing between the city and third parties must be approved through a formal, auditable process that includes the PAB? Data is shared with 3rd party agencies and entities on a regular basis and cannot be gated by the PAB who doesn't meet often enough or have a working understanding of the nature of the data sharing. The Police Department shares data with investigators from other agencies in the region and with the District Attorney's office. Traffic engineering collect non-identifiable data on traffic flow and patterns based on cell phones passing by various points on surface streets and that data can be shared with 3rd parties to help inform commuters where there is congestion so that they can choose an alternate/faster route. This section of your recommendations needs significant revision in my opinion and frankly, I would focus on requiring that the data owners document the current practices sharing of identifiable data to 3rd parties, rather than submitting all data sharing to 3rd parties for review. I would also like to add some insight to the example the task force used in section 12 with regard to the sharing of LPR data with law enforcement agencies that should not have had access to it. I suspect the task force is not aware that this was a result of a software user interface design flaw which I, as the Police Technology Manager at the time, had reported to the vendor. The vendor said it was not a bug and it was by design. If so, it was a design to trick people into clicking a 'Yes' button about data sharing broadly right after a typical prompt appears during user login where clicking 'Yes' is necessary to continue into the platform. The look and feel between the two dialogs was nearly identical yet the impact of clicking

the second 'Yes' button was dramatically different than the first. We had no leverage to force the vendor to change the behavior and it was inevitable that a user would Click 'Yes' twice in order to get into the platform to do their job. There was no alert email to indicate that this sharing was enabled. It was a horrible design but it is not a reason to throw shame on the city and employ some level of oversight that wouldn't have prevented the sharing or detected in for perhaps months. Allowing the city to have legal language in the contract to terminate at our convenience if the vendor is putting our data privacy/sharing policies in jeopardy would have resolved this. I defer to the City attorney's office for the best way to proceed.

Section 22 – In general, I agree with this section as it's also already supported by California Privacy laws and is therefore redundant and unnecessary to include in your recommendations. This section should be more about tracking and reporting on compliance with existing applicable laws and statutes and less about trying to implement what you believed to be new technical controls. I also wanted to take a moment to highlight that last sentence of 22.a which should include LPR data as a type of data collection that a person cannot reasonably opt-out of. And for the same reason, why signage of 'surveillance cameras in use' should not be posted as it gives an improper expectation that if they are nowhere near one of those signs, they are not subject to LPR cameras which would generate plate reads that are available to the city (which I believe is the intent based on conversation at a public meeting of the task force). Commercial vehicles such as tow trucks, garbage trucks and HOA owned LPR cameras are everywhere and moving constantly. That's technically where most of the license plate reads come from that all law enforcement agencies utilize to investigate crimes that have occurred. A reasonable control to request for LPR systems is that whenever a search of LPR data is done by authorized personnel, the reason for the search must include a CAD incident number or a crime case number. This would make audits of the approved use of LPR data much more usable in terms of finding abuses/misuses.

I am happy to take calls and meetings to respond to any of my comments here. But I also know that each of you are also very busy and so I understand that I will likely hear nothing in response. I do empathize with each of you. You have volunteered to do a job that you only discover the challenges in doing it well once you're already in the midst of it. I know that you all have great intentions but I do encourage you to take a trust but verify approach rather than mistrust and review approach. The city has done nothing to deserve that posture.

Best Regards,
Eric Wood

From: Jim Zuffoletto <[REDACTED]>
Sent: Sunday, September 18, 2022 11:07 AM
To: privacytaskforce@chulavistaca.gov
Cc: Rkennedy@chulavistapd.org; pcollum@chulavistapd.org
Subject: Summary of Policy Recommendations

**Warning:
External
Email**

Members of the Privacy Task Force

Let me preface my remarks by thanking you for the opportunity to comment on the proposed Summary of Policy Recommendations.

My comments are limited to the application of these recommendations as they impact law enforcement and more specifically the CVPD, Sheriff and National City.

I speak from a background in law and law enforcement having been a sworn member of the CVPD and SDCSO and a licensed attorney representing clients in various area of civil litigation. I served on the 2021-22 County Grand Jury where my Law and Justice committee examined and extensively studied the issue of privacy rights and the impact of surveillance and modern technology on the public. The 2021-2022 Grand Jury published its findings and recommendations which can be found at: <http://www.sdcounty.ca.gov/grandjury>.

That being said, the recommendations being proposed are, I believe, incomplete and present potential serious issues concerning public welfare and safety.

“The Privacy Advisory Board should have nine members, at least two-thirds of whom are Chula Vista residents.”

It is no surprise that the authors specifically left out inclusion of representatives from law enforcement and victim’s rights advocates. The special interest groups, working under the guise of the San Diego TRUST coalition, drafted and presented the exact same recommendations for the City of San Diego. One only need look at the composition of that group to understand the real purpose behind their agenda. Best practices studies show that “city council decisions are more likely to be seen as fair and considerate if all people having a stake in the outcome” are involved. Asking nine people, none of whom have any experience in law enforcement, to make recommendations on what is acceptable use of a piece of modern technology is like asking a jury of nine to determine guilt or innocents after hearing testimony and seeing evidence from only one party to a case. At the August meeting of the Advisory group, a member of TRUST stated they were only interested in being sure that all members of the community were represented. That being said, it appears TRUST does not view law enforcement or victims of crime to be part of the Chula Vista community.

Using that as background, and as mentioned earlier, it is my opinion the recommendations fail to address serious concerns unique to law enforcement.

Sharing of information with neighboring law enforcement agencies

The CVPD works closely with the SDSO, which serves the unincorporated area of Bonita, and with the NCPD. The departments are often called upon to assist each other. This close symbiotic working relationship often requires sharing of information by each organization. That need for sharing must be recognized and incorporated within the guidelines the advisory board works with and in collaboration with outside agencies and must be considered when recommending any rules on sharing surveillance or the use of equipment, i.e.; drones.

Law Enforcement Consultation and Contribution

Along the same lines, often, the use of surveillance technology as it specifically applies to law enforcement cannot be adequately explained by a non-law enforcement lay person. Hence, any recommendations concerning use of technology must include specific and articulable rationale from the CVPD (or other L.E. sources) as to the appropriateness of the board's recommendation. If necessary, provisions should be included allowing such presentation to be made in a closed-door session with city council, city attorney, city manager, mayor, and privacy director.

Cooperation and contribution with State and Federal Authorities

In addition, the CVPD has officers assigned to, and cross-sworn with, various state and federal agencies and task forces such as FBI, DEA, HSA, etc. In their roles, secret and sensitive information must be shared. Any attempt to quash that sharing might jeopardize further participation by CVPD personnel and affect public safety. Clarification with regard to sharing of such data should be included. Once again, this will require input from high level members of the city administration and the CVPD,

Secrecy and Confidentiality

Finally, I see no provision for discussion of sensitive material among the advisory board members. Secrecy should be addressed and required as it is with the members of the grand jury. All members must be held to a strict level of confidentiality and subject to fines or prosecution for violating their oath.

I would like to present further discussion at the upcoming meeting and will request the same in a separate writing.

Thank you again,

James M. Zuffoletto, Esq. (Ret)



Virus-free www.avast.com