Chula Vista Technology and Privacy Advisory Task Force
Summary of Policy Recommendations
DRAFT VERSION – September 23, 2022

Guiding Principles

Guiding Principle 1: Protecting the privacy and safety of Chula Vistans via **enforceable law.**

- The task force intends that ordinances should be passed by the Chula Vista City Council to regulate the acquisition, deployment, use and expansion of new or existing technology designed to monitor or capture personal identifying information (sensitive or surveillance) by the City of Chula Vista.
- The task force urges the Chula Vista City Council to align all future decisions regarding technology designed to monitor or capture personal identifying information (sensitive or surveillance) with the principles of ensuring Chula Vistans receive maximum awareness, that any such technologies provide defined and verifiable benefits for Chula Vistans.
- The task force intends that the fully advised and informed elected members of Chula Vista City Council should be the only body that can authorize new acquisition of, or continuing use of, technology designed to monitor or capture personal identifying information (sensitive or surveillance). There should be no automatic exemption from this approval process for technologies currently in use.

Guiding Principle 2: Providing the communities of Chula Vista with a **permanent, empowered board or commission.**

- The task force intends that a board or commission of independent community members that are affected by technology and or who are most knowledgeable of the risks of surveillance technology, will be created by Chula Vista City Council.
- The task force intends that the board/commission should be empowered by Chula Vista City Council to ensure the community is fully informed and provided with sufficient time and opportunities for meaningful engagement.
- The task force believes local communities and their elected officials should be empowered to make determinations about the use of existing and new technology. We do not intend for department heads or department staff to be empowered to make these determinations without transparency.
- It is the communities most affected that are most in need of an empowered platform, and whose advice can be most meaningful to creating a trusted process. The task force intends that the City select its board/commission members accordingly.

Guiding Principle 3: Protecting **taxpayer funds and City operations** from waste, fraud and abuse.

- The task force intends that the proposed acquisition and/or use of technology only be consented to by the Chula Vista City Council under defined conditions, which are enforced by City Council during the approval process.
- The task force intends that city departments 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.

- The task force intends that any program designed to monitor or capture personal identifying information (sensitive or surveillance) being considered for approval should demonstrate written policies and operational controls that are commensurate with the impacts and risks of harms that will be placed on the communities of Chula Vista.
- Any eligible technology operated by the City should be periodically required to demonstrate to the community and City Council the technology's costs and effectiveness at achieving its intended purpose, and its compliance with all privacy requirements.

Guiding Principle 4: Protecting Chula Vistans' **civil rights and civil liberties**

- The task force intends that technologies designed to monitor or capture personal identifying information (sensitive or surveillance) should not be funded, acquired, or used without studying and addressing their potential impact on civil rights and civil liberties.
- The task force intends that city departments seeking to fund, acquire, or use a technology designed to monitor or capture personal identifying information (sensitive or surveillance) 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. This information should serve as the basis for all public hearings regarding the proposed technology.

Based on the guiding principles outlined above, the task force has developed the following specific recommendations:

Privacy Advisory Board

1. The City should establish a permanent Privacy Advisory Board responsible for carrying out a broad range of advisory duties.
    a. The Privacy Advisory Board should be established as soon as possible, as it is key to implementing many of the recommendations in this document and conducting further public discussion on important issues related to privacy and City technology.
    b. 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 leaders, 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.

    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
            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. Sharing of sensitive personal data 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 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.
    b. This recommendation does not apply to the sharing of standard business data or other operational information between departments. It does apply to data that can be used to identify a person.

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.

Transparency and Oversight

18. City staff should provide annual reports to the Privacy Advisory Board on the use of selected privacy-impacting technologies. These reports should include the following information:
    a. A description of how and where the technology was used
    b. A description of the type and quantity of data gathered or analyzed by the technology
    c. Information about how the data was shared with internal or external entities, including the names of any recipient entity, the type of data shared, and the justification for the sharing

19. 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.

20. 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.

21. 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.

22. Data breaches should be disclosed to affected individuals as soon as possible, pursuant to all applicable state and federal laws, and the City should provide a general notification to the public once the issue has been fully resolved.
    a. Notification to the general public should occur through a wide range of communications channels, including social media, news media, and the City website. To protect the City's information security, only limited information should be released to the general public.

23. 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.

24. The City should establish strong whistleblower protections for any employee who reports a suspected violation of the City's privacy or technology policies or any use of City technology that could violate an individual's privacy.

Procurement

25. 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.

26. At least one month prior to a City Council decision to acquire new privacy-impacting technology or to adopt new policies around the use of privacy-impacting technology, the City should hold public meetings to solicit community input on the proposed policies associated with the technology.
    a. Meetings should be held in locations on both the West and East sides in locations such as public libraries.
    b. These public meetings should include a presentation by City staff outlining how the technology would work, types of data to be collected, how the data would be protected, etc.
    c. These meetings should be recorded and made available on the City's website and/or social media channels such as YouTube, and links to the video should be promoted through City communications channels in the weeks prior to a City Council decision.

27. Following the public meetings and prior to seeking City Council approval for a new privacy-impacting technology, City staff should create a Technology Impact Report that identifies the following:
    a. Potential impacts to the City's budget, including the cost of acquisition and cost of anticipated ongoing operations and maintenance
    b. Potential impacts on the City's information security, and proposed strategies to mitigate those impacts
    c. Potential impacts on the civil rights and civil liberties of community members, and proposed strategies to mitigate those impacts

28. 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.

29. Public disclosures should follow a process similar to that outlined in Appendix C, in which City staff first provides draft impact reports and use policies to the Privacy Advisory Board, then receives feedback and a recommendation from the Privacy Advisory Board, then provides public notice at least two weeks in advance of a City Council meeting, and then holds a public hearing at a City Council meeting.

30. As a strategy to mitigate risks to the City's information security, the City should establish a preference for acquiring technology that is developed and sold by companies that are owned and based in the United States.

31. Prior to agreeing to acquire new privacy-impacting technology, the City Council should make a determination that the following conditions have been met:

a. The collection and use of personal information is reasonably necessary and proportionate for one of the following purposes, and that this purpose outweighs the risks and costs to the civil rights and civil liberties of Chula Vista community members:
    i. The vital interest of the individual
    ii. The public interest
    iii. Contractual necessity
    iv. Compliance with legal obligations
    v. Unambiguous consent of the individual
    vi. Legitimate interest of the City
b. City staff have provided an adequate justification for the stated purposes, retention periods, and impacts of the technology.
c. The public has been notified at least 30 days prior to the City Council decision.
d. The Privacy Advisory Board has reviewed and provided a recommendation as part of the City's due diligence and risk assessment process, and this recommendation has been documented and provided to the City Council.
e. The City will follow best practices — including, but not limited to, anonymization, encryption, and least privilege access — to safeguard data.
f. The City will govern the use of surveillance data and biometric data in a manner similar to the California Privacy Rights Act (CPRA) requirements for "sensitive data."

32. 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.

33. 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 or otherwise violates individual privacy protections.

34. 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.

35. 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.

36. 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.

Information Security

37. 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

1. 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.

2. Some of the recommendations in this document can be achieved through voluntary changes to the City's operating policies and processes, but for some recommendations, an ordinance may be required to implement. The Task Force urges the City to adopt ordinances to provide greater structure and accountability to these recommendations.

3. While the Task Force understands it is the City's prerogative to accept only some of the recommendations in this document, the Task Force urges the City to treat these recommendations as a unified whole and implement all recommendations.