Privacy Protection and Technology Transparency Policy

Presentation to the Chula Vista City Council

Nov. 1, 2022

Selection Process for Task Force

February 2022

- Application live for 30 days
- 57 applications submitted

March 2022

- Committee of three community leaders narrowed applicants down to 21

April 2022

- City Manager interviewed candidates and selected 12 to serve on Task Force

Community Leaders Selection Committee

- **Beatrice Zamora**, former college dean, children's book author and Chula Vista resident
- **Dr. Francisco Escobedo**, Executive Director at the National Center For Urban School Transformation
- **Arnulfo Manriquez**, CEO at MAAC

Technology and Privacy Policy Task Force Members

Sophia Rodriguez, Chair, *Human Services Specialist*

Rafal Jankowski, Co-Chair, *Information Technology and Information Security Expert*

Petrina Branch, *Attorney and Human Relations Commission Representative*

Mae Case, *Non-profit and Community Advocate*

Carlos De La Toba, *Retired Federal Law Enforcement Officer*

Dominic LiMandri, *Small Business Representative*

Lucia Napolez, *Digital Marketing*

Art Pacheco, *Engineering Vice President*

Pedro Rios, *Civil and Human Rights Advocate*

Patricia Ruiz, *Academic Research Scientist*

Charles Walker, *Database Administrator and Information Technology Expert*

Maria Whitehorse, *Social Services Worker*

Technology & Privacy Advisory Task Force

- 12 residents / community members
  - Tech experts, social workers, academic researchers, small business, lawyer, retired law enforcement
- 12 meetings (April – September)
  - 10 open public meetings
  - 2 on-site tours and briefings
  - Briefings from 10 City Departments
  - Presentations from experts and community groups

Thank you to...

Task Force members,
community participants,
City staff,
Executive Team,
City Clerk,
City Attorney and
Madaffer Enterprises!

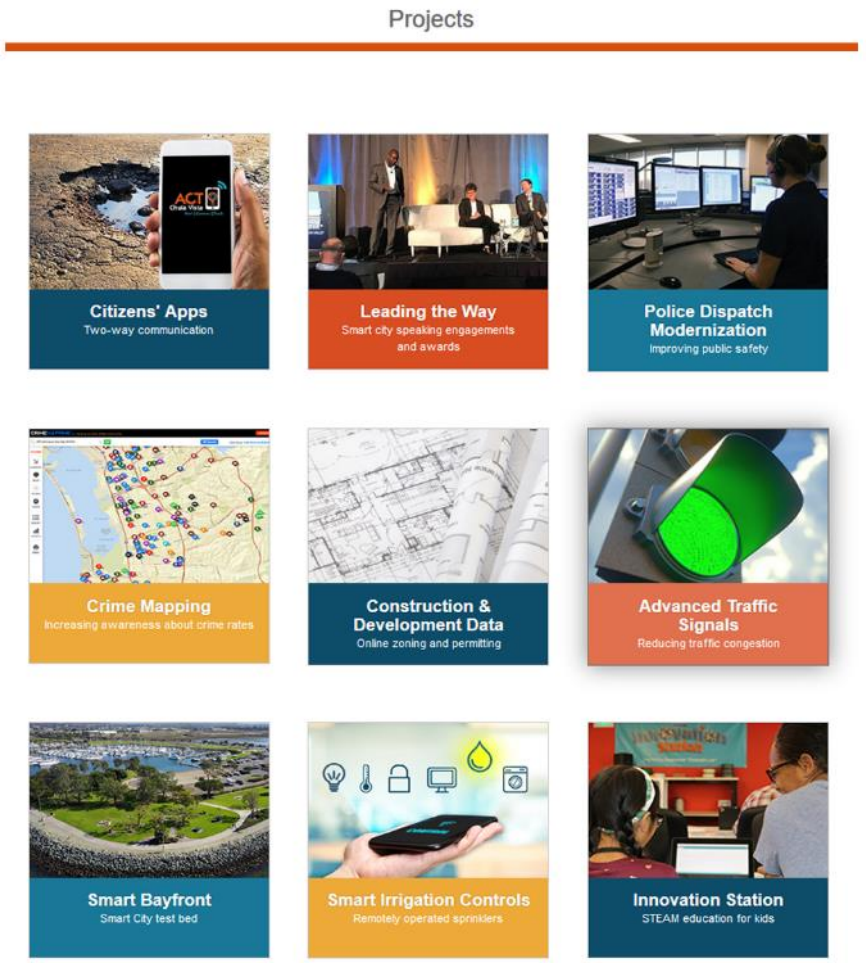
Origin of the policy

2017
- Smart City Strategic Action Plan

2018
- Open Data Policy
- Smart city marketing and communications

2019 - 2020
- Traffic Signals Communications Master Plan
- Citywide Telecommunications Master Plan
- Data Governance Committee and Data Governance Standards
- Digital Equity and Inclusion Plan

2021 - 2022
- Refining technology privacy & oversight policies



Purpose of the policy

- Safeguard the security, accuracy, and control of access to City data and technology systems
- Protect the civil rights and civil liberties of Chula Vista community members and visitors, including rights to privacy
- Ensure that expert advice and community input are included as part of City decision-making involving the acquisition and use of technology
- Protect against the waste of taxpayer funds
- Promote transparency in the acquisition and use of technology
- Build and maintain public trust in the City and its use of technology

Project scope

January 2022 City Council direction:

- Public opinion survey and focus groups
- Gather information from City staff
- Community meetings and presentations
- Communicate policy development to the public
- Draft a policy

Public input and community engagement

- 36+ hours of open, public meetings
  - Broadcast and archived online
  - Agendas posted 72 hours in advance
- Dedicated website and email inbox
  - chulavistaca.gov/privacytaskforce
  - privacytaskforce@chulavistaca.gov
- Updates sent to City email subscriber lists
- Public updates via social media, City newsletter, news media

Public opinion survey

Sample size: 607 residents

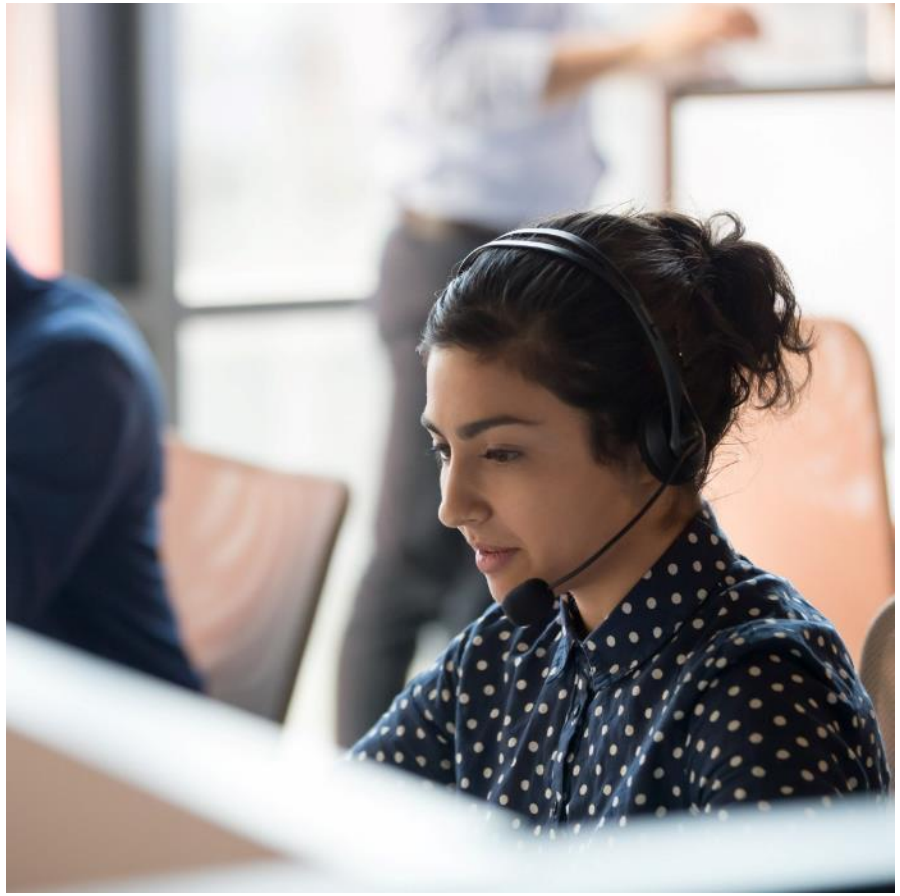
Languages: English, Spanish, Tagalog

Population: All adult residents, including registered voters and non-voters

Modes: Live telephone interview; online survey via email and text message

Margin of error: +/- 4%

Confidence level: 95 percent



Public opinion survey – key findings

- More than half of residents believe things in Chula Vista are “moving in the right direction”
  - 27% say things have “gotten off on the wrong track”
- Residents more confident in City’s ability to protect personal information than in federal government or online businesses
  - 56% express confidence but most residents have some reservations
- 85% of residents said it was important that the City adopt “a new privacy protection policy to make the City’s use of new technologies transparent and efficient”
  - 70% said this was “very” or “extremely” important
- 77% of residents approve of the City using live video cameras on traffic signals to improve traffic flow and safety

Public opinion survey – key findings

- Most residents trust the Chula Vista Police Department “a lot” or “somewhat”
  - 26 percent of residents say they trust CVPD “not much” or “not at all”
- Most residents (77%) approve of the drone program (42% strongly approve)
  - 17% disapprove, many citing privacy concerns, potential for misuse
- Most residents (63%) approve of Automated License Plate Readers
  - 31% disapprove, many citing potential for misuse, privacy concerns

Focus Groups & Community Meetings

- Six focus groups
  - Four in English, two in Spanish
  - 45 participants
  - 90 minutes each
- Two community meetings
  - South Chula Vista Library
  - Otay Ranch Branch Library
  - Over 50 attendees
  - 90 minutes each

Information-gathering and City department briefings

- Briefings from 10 city departments
- On-site tour: Chula Vista Police Department
  - Follow-up conversations and 90 question Q&A document
- On-site tour: Traffic Management Center
- Special presentation by Pegah Parsi, Chief Privacy Officer at UC San Diego
- Educational presentations by Madaffer Enterprises
- Special presentation by ad-hoc community coalition

Summary of 37 Task Force Recommendations

- Establish a Privacy Advisory Board
- Hire a Chief Privacy Officer
- Provide enhanced privacy training for City staff
- Require City Council review of privacy-related contracts
- Create written Use Policies to govern the use of technology
- Prepare impact reports for technologies with privacy impacts
- Provide annual reports on the use of technology with privacy impacts
- Prohibit the sale of data and limit data sharing with third parties
- Establish a strong information security policy

Privacy Protection and Technology Transparency Policy

- Privacy and Technology Advisory Commission
- Support from Privacy and Technology Experts
- Use Policies
- Surveillance Technology Impact Reports (STIR)
- Surveillance Technology Acquisition Process
- Transparency in the Use of Sensitive and Surveillance Technology
- Data Collection, Retention, Sharing and Management
- Information Security
- Exceptions
- Training, Compliance and Enforcement of the Policy and Compliance with Laws

Key definitions

1.4. **Sensitive Personal Information**: Information that reveals a person's social security number, driver's license information, state identification card, passport number, military identification number, financial account numbers, debit card number, credit card number, account log-in credentials, IP address, email address, phone number, home address, precise geolocation at a given time, biometric information, contents of email, contents of mail, contents of text messages, ethnic origin, racial origin, genetic data, medical information, health information, immigration status, philosophical beliefs, political opinions, religious beliefs, sexual orientation, union membership, or membership in any other private organization, in each case to which a person has a reasonable expectation of confidentiality or privacy. For purposes of this definition and this policy, Sensitive Personal Information **does not include** information recorded, obtained or disclosed as a part of an active criminal investigation, a lawful judicial hearing or process, or in accordance with other legal or statutory requirements.

Key definitions

1.6. **Surveillance** or **surveil:** To observe the movements, behavior, or actions of identifiable individuals, or to gather information that can readily be connected to identifiable individuals (for example, an automated license plate reader program), for purposes of analysis in accordance with a program or plan, without the knowledge and consent of the observed individuals. Observations that are incidental or part of a focused, ongoing investigation shall not be considered surveillance for the purposes of this definition and this policy.

Key definitions

1.5. **Sensitive Technology**: Any electronic device, software program, or hosted software solution owned or operated by the City that generates or collects Sensitive Personal Information, but which is not designed or intended to be used for surveillance.

For the purposes of this definition and this policy, Sensitive Technology **does not include** the following:

- Standard office technology such as email systems, copy machines, telephone networking systems, or broadly available consumer software such as Microsoft Office applications
- IT infrastructure only intended to manage backend or operational data.
- Technology solely intended to manage the Sensitive Personal Information of City employees, such as payroll, employment applications, health and retirement benefits.
- Technology solely intended to manage the internal administrative functions of the City, such as case management systems and revenue collection and billing systems.

Key definitions

1.7. **Surveillance Technology:** Any electronic device, software program, or hosted software solution owned or operated by the City that is designed or primarily intended to be used for the purpose of Surveillance.

For the purposes of this definition and this policy, Surveillance Technology **does not include** the following:

- Cameras installed on City property solely for the purpose of maintaining the security of that property.
- Cameras installed solely to protect the physical integrity of City infrastructure, such as sewers and storm drains.
- Technology that monitors only City employees in the performance of their City functions.
- Public safety officer body-worn cameras.

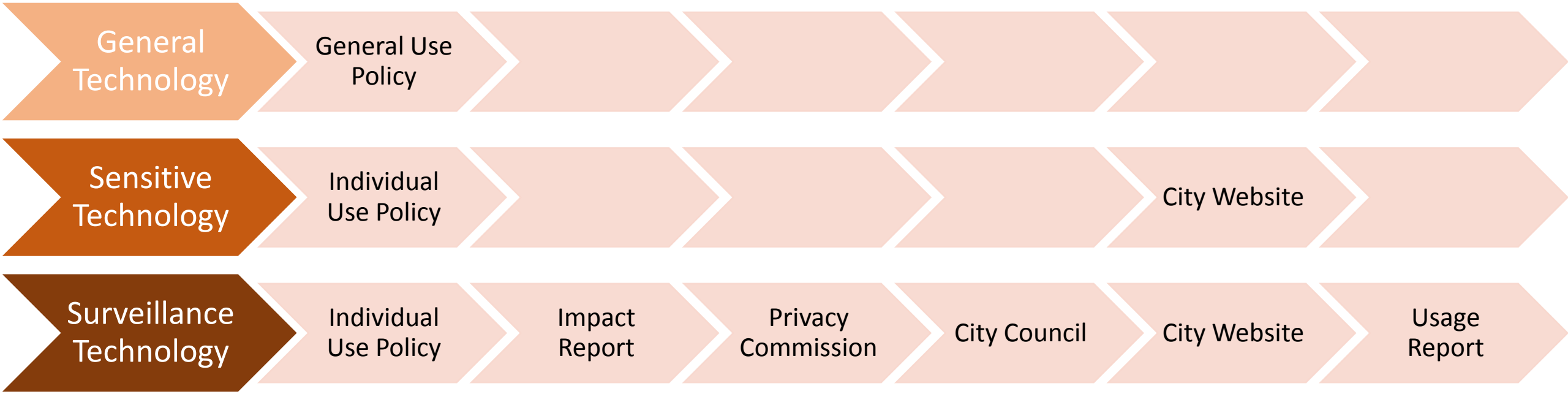
Types of technology used by the City

General Technology	Sensitive Technology	Surveillance Technology

• Minimal privacy concerns
• *Examples:*
  • *Standard business technology (email, mobile devices, etc.)*
	• Involves sensitive personal information, but not used for surveillance
	• *Examples:*
	  • *Drones in engineering*
	  • *Traffic signal cameras*
	  • *Drone as first responder**
		• Specifically used for surveillance
		• *Examples:*
		  • *Automated license plate reader systems (ALPR)*

*Staff intends to process as "surveillance technology" in the interest of transparency

Technology acquisition & review processes



Increased oversight and transparency

- Prohibition of sale of City data
- Establishing a Council Privacy and Technology Advisory Commission
- Providing a privacy advisor to assist City staff and the Commission
- Report every 2 years on surveillance technology usage
- Post information (use policies, impact reports, usage reports) on City website
- City Council approval for all surveillance technology acquisitions

Exceptions

- Waiver by City Manager or City Council
  - Only when circumstances make compliance impossible or infeasible
- Interagency task force activities
  - Only to the extent of work on the interagency task force
- Exigent circumstance
  - Must be authorized by City Manager or designee
  - Must be reported to City Council

Next steps

- Council to establish Privacy and Technology Advisory Commission
- City Manager to establish internal Technology Governance Committee
  - Establish internal process for classifying technology
- City Manager and Commission to elaborate on requirements for video feed access