THE CITY OF SAN DIEGO

M E M O R A N D U M

DATE: May 25, 2023

TO: David Nisleit, Chief of Police
via Christopher McGrath, Executive Assistant Chief

FROM: Charles Lara, Acting Captain, Special Projects/Legislative Affairs

SUBJECT: The San Diego Police Department's Response to the Privacy Advisory Board's Questions Regarding the Smart Streetlights Program

---

Summary:

The Privacy Advisory Board ("PAB") was created by the Transparent and Responsible use of Surveillance Technology Ordinance ("Surveillance Ordinance") adopted on September 9, 2022. The Surveillance Ordinance mandates a process of community meetings, Use Policies, Impact Reports and reporting out to the PAB and San Diego City Council prior to acquiring or using surveillance technology. On April 27, 2023, the San Diego Police Department reported out on Smart Streetlights to the PAB after having completed community meetings, Impact Reports and Use Policies. Following the presentation, the PAB provided numerous written questions to the Department pertaining to the Smart Streetlight proposal.

This memorandum will outline each PAB question, followed by SDPD's response.

1. **Who is the vendor of the devices? Can we get a description of the specific (systems) and products?**

   Ubicquia is the proposed vendor the San Diego Police Department is working with to restart/refresh Smart Streetlights throughout the City. Product details are listed on SDPD's website and through this link: https://www.ubicquia.com/products/smart-city-platform-UbiHub-APAI. If Ubicquia is selected as the City's vendor, it may subcontract other services, such as automated license plate readers ("ALPR"), wireless connectivity, and installation and maintenance, to vendors that will be disclosed as the contracting process allows.

2. **How and why did the City select this vendor?**

   Ubicquia is capable of bringing video and ALPR under one unique platform, which makes it an ideal technology to enhance the Department's public safety mission. Law enforcement agencies throughout the nation have found video evidence from cameras placed in public spaces, along with ALPR technology, being invaluable to detect, deter, and solve crime and enhance public safety.

3. **I see that GE provided a $30 million loan to the City for the cameras. What is GE's objective with the City? Any relation to the vendor?**

   Any previous loan, and agreement between the City and GE, has no relation to this proposal currently before the Privacy Advisory Board pursuant to the Transparent and Responsible Use of Surveillance Technology Ordinance ("Surveillance Ordinance").

4. **Are there already agreements or MOUs in place with vendor(s)? If so, can the PAB see a copy (to ensure that it aligns with the use policy)?**

   No. Pursuant to the requirements of the Surveillance Ordinance, there is no agreement currently in place.

5. **What is the experience of the vendor? How long has it existed? Is it a private or public company? How many security or privacy breaches has it had in the last 3 years? How many were reportable breaches?**

   Ubicquia has experience with smart lighting, smart electrical grid, and smart city solutions, since 2016. Ubicquia is a private company. They have had zero breaches and zero reportable breaches in the last three years.

6. **Does the vendor have security and privacy certifications or audit reports (e.g., SOC 2, Type 2 reports) to share?**

   Yes. An ISO 27001 certification.

7. **Please describe the vendor (and subprocessor) access to the systems and data, including for routine maintenance.**

   Ubicquia reserves the right to use all data collected by its products and systems solely for the purposes of analyzing, evaluating, supporting, and improving Ubicquia products and services. This data does not identify any individual and is never sold, licensed, or provided to any third party.

8. **Please describe whether and how the vendor (and any subprocessors) can use any data collected.**

   Ubicquia reserves the right to use aggregated statistics, that have been anonymized such that they do not and cannot be used to identify any customer or individual, solely for the analysis, evaluation, and improvement of Ubicquia products. This data is never sold, licensed, or provided to any third party.

9. **Does the vendor sell, license, or otherwise provide any information (including "de-identified" data, aggregated data, and metadata) collected through the units or related to this initiative for any purpose? If so, to whom and for what purposes?**

   No. Aggregated or "de-identified" data is used to continually train the computer vision model, which benefits the customer.

10. **Does the vendor have a documented security policy?**

    Yes, per ISO 27001.

11. **Does the vendor have a documented privacy policy?**

    Yes. https://www.ubicquia.com/privacy-policy

12. **Does the vendor have a documented code review process?**

    Yes, per ISO 27001.

13. **Has the City checked other vendors and compared qualities and pricing?**

    Yes, SDPD has extensively reviewed the capabilities of other vendors and their pricing models including software as a service and considered purchasing the technologies being discussed separately.

14. **Who will be maintaining and operating the cameras and data? Is it the same company that installed them?**

    If selected as the City's vendor, Ubicquia will likely use a subcontractor to install and physically maintain the technology on City infrastructure, in accordance with all applicable contracting and permitting requirements.

15. **Does the vendor contract secure the ownership and use of the data and no other firm/entity has rights to the data?**

    Yes, any contract will identify data associated with this technology, and how it can be used and by whom. Additionally, state law, as well as SDPD's policies and procedures (DP 3.33 (Smart Streetlights), DP 1.51 (ALPR), DP 3.02 (Property and Evidence), provide direction on how data can be used and shared.

16. **Vendor cameras are not 100% reliable. How is the City planning to protect against false positives? Bias in tying the car to the license plate and to the crime?**

    SDPD's policies and procedures address these issues, for example a "hit" on a license plate read by ALPR technology would require an officer to independently check the license plate via dispatch or their mobile computer terminal prior to making a motor vehicle stop. Please review the draft procedures submitted to the PAB for additional information: https://www.sandiego.gov/sites/default/files/draft-procedure-1.51-lpr.pdf

17. **What due diligence have we done on the vendor to ensure capabilities and ability to uphold the City's privacy requirements?**

    The City and any contracted vendors must comply with all legal requirements. The Department is well aware of community concerns surrounding this technology and is taking great care and effort in developing a program that balances the City's commitment to ensure privacy protections for community members with producing public safety enhancements. Additionally, technology projects such as this are also reviewed by the members of the City's IT Department, including cyber security professionals, and are field tested before implementation.

18. **What inappropriate uses of this technology by police officers, Ubicquia, or others have you considered and what policy, contract, or configuration steps have you taken to mitigate that?**

    Mitigation is achieved by the SDPD developing policies and procedures that provide clear expectations regarding technology use, along with ensuring timely investigations into alleged misuse, and appropriate discipline for any sustained violations. This is followed by the Department limiting access controls to its members and auditing their actions. Additionally, the City will monitor any contract for compliance with all contractual and legal requirements. The agreement will also define the roles and obligations that vendors, and subcontractors, have related to this technology's deployment.

19. **Is there a risk of that vendor outsourcing services to another entity we do not have control over? Is there a risk similar to Jack Teixeira in Washington DC?**

    The parties involved and their services related to the implementation, utilization, and maintenance of any technologies sought by the City will be clearly defined by the conditions and agreed upon contract terms to prevent unapproved outsourcing. Access, supervision, and oversight of this technology would be ensured by the Chief of Police or his designee. Smart Streetlight technology oversight will be the responsibility of the Special Projects Captain to ensure the risks associated with inappropriate use and sharing of confidential data, such as the actions by Air National Guard member Jack Teixeira, are safeguarded.

20. **Will this vendor (or other vendors in the same space) be willing to speak with the public to provide feedback and address community concerns?**

    Any questions for Ubicquia, or any other vendor, may be asked in writing and forwarded to the Mayor's Office for consideration. Please note, there is no requirement under the ordinance for the vendor, or the Department, to answer written questions from the Board.

21. **What is the level of granularity of the videos? Can individuals in the vehicles be detected? Pedestrians? People in buildings? Are they identifiable? Can we see samples?**

    Smart Streetlight cameras have been successfully used to clearly identify persons and vehicles in public places, along with their criminal actions, in numerous investigations. The clarity of the video is directly related to their placement locations in streetlight hardware, with cameras at lower levels, such as the lights in the Gaslamp District, providing greater clarity than those at higher positions on streetlights. Persons in vehicles and buildings, which are also generally masked, were not visible. The Department can provide fliers of wanted subjects that were developed through video images from Smart Streetlights as examples.

22. **Describe the encryption architecture in more detail. Where is the 256-bit AES key stored? Is it stored on the data-gathering device? Does the latter communicate directly with AWS? Or does the device send data to a server, and encryption is done on the server, which holds the key? If so, who runs the server? The key will also need to be stored in any system that uses the data, since the encrypted data will need to be downloaded from AWS and decrypted with the key on the local system. How is the key created and distributed to these systems? How many such systems are there? How is the key protected and accessed on these systems? (For example, password-based access.)**

    Data on the device (at rest) is AES-XTS-256 encrypted with a key that is burned into the device at manufacture, stored on the Trust-M device (crypto chip) and cannot be extracted from it. Data in transit is secured per TLS 1.2. The TLS protocol is supported

by certificates that leverage combinations of public and private keys, generated per session, with a sequence of handshakes. Server side keys are managed by Ubicquia using SSE-KMS, so no other entity (including AWS) has access.

23. AES-256 can be used in many different ways to encrypt data, and the different ways have different security attributes; some are good, some are poor. Exactly what algorithm (sometimes called mode of operation) of AES-256 is used here?

AES-XTS-256.

24. The devices (cameras) will use network access to communicate with AWS, receive maintenance updates and so on. This becomes a path for intruders or hackers to enter the system. Such intruders can read the key directly off the camera memory; encryption is of no help against this threat. At that point hackers can potentially obtain all the data in the clear, opening the door to abuse, blackmail and related risks. What do we know about the security of the camera systems and software against this type of penetration?

It is impossible to read the key directly off the camera because remote access is only possible using a secure SSH connection requiring a rotating, expiring private key, that does not reside on the device and is managed exclusively by Ubicquia. Even if the device is disassembled, accessing the operating system is not possible because the serial port access is disabled at manufacturing.

25. Who is responsible for SDPD's settings within the AWS environment?

Ubicquia manages the AWS environment.

26. The impact report states that audio capability (as well as facial recognition, wifi capabilities, Edge I, gunshot detection, lighting control, etc) is included in the technology but will not be activated. What steps would be involved in activating any of these capabilities? Other than assurances from the vendor and SDPD, what checks and balances are in place to prevent activation of audio (or any of the other capabilities) and how would the community know if it has been activated?

For clarity, the following functions: noise/audio detection and/or recording, the counting of vehicles or pedestrians impacting traffic conditions, documenting near collision hits, illegal dumping or geo-fencing, and monitoring of unusual behaviors, are not capabilities desired or sought from this technology by the City, or its departments, and are not being configured by the vendor for the City. Any contract would make this clear as a check and balance. If the City changed its position and wished to activate these functions, the City would have to formally request these changes, and then these functions would have to be introduced pursuant to all applicable regulations and ordinances, meaning SDPD would have to come back to the PAB for its review and recommendation. Facial recognition functions are not included in this technology proposal.

27. Provide more information as to why the City chose 500 cameras and the locations it did. I do not see a direct correlation to "crime location" and camera location. Please describe your methodology for choosing proposed smart streetlights location, not just statistically but why those specific points on a street and in neighborhoods. Discuss the angles and ranges of cameras, like at an intersection, can they see 360-degrees or in some particular direction?

The proposed Smart Streetlights with embedded ALPR technology will be deployed citywide in all council districts. The locations selected were tied to several factors – analysis of violent crime locations (particularly areas with a strong nexus to gun violence) conducted by our Crime Analysis Unit, input from our centralized investigative units (e.g., Homicide, Robbery & Sex Crimes), and the final input from the commanding officers of every patrol division in the City.

This is detailed in the impact report provided to PAB:

https://www.sandiego.gov/sites/default/files/smart-streetlights-impact-report.pdf

Additionally, when reviewing the impact report, attention should be given to Tables 6 and 7 which breakdown the beats where firearms are seized during stops and used to commit violent crimes. Two of the top five beats involving gun crimes, 512 and 712, are located in Council District 8 and contributed to the resources proposed there.

28. Is past crime statistics the best indicator for camera location? It seems the cameras are positioned in relation to the freeways. Can you specify if the intent is to know who is entering/exiting freeways? What would this be used for?

As stated, crime statistics were not the only factor that led to the selection of camera locations, which also included input from commanding officers, and from investigators throughout SDPD. Many of the cameras are positioned in relation to freeways since overwhelmingly vehicles are used in the commission of crimes, and then freeways are used to quickly flee the area undetected. The deployment of this technology at these locations is to detect, deter, and hold persons accountable for their criminal actions.

29. Is there a .csv file of latitudes and longitudes for locations? Also questions related to directionality and positioning?

Yes.

30. Were communities consulted in selecting the locations? Please describe.

Locations were selected as previously described and shared with communities during outreach meetings for their feedback and input. Additional outreach was conducted by

liaison officers, community resource officers and command staff to answer questions from community members.

31. From past deployments and other cities' experiences, how many people's information was collected? For example, how many license plates were read each day? How does this compare to number of criminal investigations that are aided by the technology?

When SDPD deployed Smart Streetlights previously it was accessed in approximately 400 cases where the investigations demonstrated public safety impacts which were significant, and evidence was located in public view near the deployed cameras. In roughly half or 50% of the cases, the cameras provided video evidence that were critical to solving the reported crimes or enhanced the investigation in a meaningful way. Next, neither video cameras nor ALPR collect "people's information," otherwise known as personal identifying information such as driver's licenses, home addresses, social security information, dates of birth, etc. Video cameras collect images of persons and their actions, and ALPR technology captures the unique features of vehicles and their license plates through Optical Character Recognition (OCR) software. The limited collection of images of persons and vehicles in public spaces, where there is no legitimate expectation of privacy, often provides invaluable leads for investigators in criminal investigations. Next, SDPD has not used ALPR technology in several years, only used it as mobile devices attached to police vehicles, and did not keep records associated with license plates and investigations. In terms of other cities experiences, many agencies maintain transparency portals which described the number of vehicles viewed, "hits" on wanted vehicles, and the number of inquiries conducted by investigators. For example, see: https://transparency.flocksafety.com/san-jose-ca-pd

32. Does the City have other cameras in public places in San Diego? If so, where?

This question appears to be beyond the scope of the proposal being discussed for the PAB, and SDPD does not maintain records of cameras placed throughout the City and is unable to fully answer this question. The Department does maintain cameras to protect its police facilities, as well to ensure the safety of its employees and community members in public meeting places such as the City Administration Building (CAB) where the Privacy Advisory Board conducts its meetings.

33. What other government entities/law enforcement agencies/public organizations have ALPRs in San Diego? Where are those located?

SDPD does not possess records of where other agencies or organizations may have placed security/surveillance cameras in San Diego.

34. What other government entities/law enforcement agencies/public organizations have security/surveillance cameras in San Diego? Where are those located?

SDPD does not possess records of where the organizations mentioned have positioned security/surveillance cameras technology in San Diego.

35. Will these locations be secure from someone hacking the system or stealing the camera and getting sensitive information? SDPD will take necessary steps to secure its surveillance technologies from hacking and theft.

SDPD does not possess the information requested in items 33 and 34. SDPD will take necessary steps to secure its surveillance technologies from hacking and theft. Additionally, when utilized previously, SDPD did not record vandalism, thefts, or hacking of Smart Streetlights.

36. Where would cameras be mounted (how high off the ground) to scan and capture license plates?

ALPR cameras will be positioned on City streetlights in locations that allow this technology to function as intended, and their heights may vary to ensure unobstructed views of traffic lanes that can be negatively impacted by signs, tree branches, etc.

37. What expansions of locations, capabilities, or uses are anticipated over the next 5 years?

SDPD is already receiving requests to expand the deployment of these technologies from entities throughout the City into areas that were not originally included in the initial proposal, but any expansion of locations would need to fit the public safety mission of the Department and City, along with complying with the provisions outlined in the Surveillance Ordinance and budgeting priorities of the City.

38. How will the City account for healthcare facilities? Reproductive services providers? Please highlight these locations on the map shown in Table 1 of the impact report.

The City and SDPD will continue to follow all applicable laws related to healthcare facilities and reproductive service providers. This starts with FACE Act compliance, otherwise known as the Freedom of Access to Clinical Entrances Act, which makes it a crime to injure, intimidate, or interfere with someone seeking or performing reproductive health care services. Next, the Department never used cameras or video footage from Smart Streetlights that identified healthcare facilities in its investigations when they were active, nor does it intend to if reactivated. State law also prohibits the sharing of ALPR data outside California, and limits the sharing of this data within the state and its uses. Lastly, the Department declines to share the locations of these facilities on a singular map

to protect the privacy and security of these facilities and those who exercise their lawful right to their services.

39. Where do most protest activities occur in San Diego? Please highlight these locations on the map shown in Table 1 of the impact report.

Most protests occur in the City's downtown, but in recent years protest activities have occurred throughout the City over labor disputes, social movements, legal and legislative decisions, access to healthcare, visits from elected officials and police uses of force. They take place with regular frequency, often starting in one area and finishing miles from their origin, and SDPD does not maintain exhaustive records of these events to accurately document their occurrence on a map. In many instances, SDPD does not even deploy resources to them unless public safety is threatened or complaints are received from community members.

40. Which houses of worship will be in view or within two blocks of the units? Please highlight these locations on the map shown in Table 1 of the impact report.

When Smart Streetlights were used previously, Muslim community members were the only religious group to express concerns. To alleviate future criticism, SDPD tasked its community liaison officers to meet with Muslim leaders, review the proposed placement of new Smart Streetlights, and provide feedback regarding their locations and any request to move them. In one instance, a request was made and the camera will be moved from its original location to accommodate the request of a local Imam. The California FACE Act is defined by Penal Code sections 423-423.6, also provides for freedom of access to church entrances, well as reproductive centers. The Department declines to highlight their locations on a singular map and bring unwarranted attention to them or those exercising their legal right to enjoy their services.

41. The information given says no face-recognition will be used, and no AI beyond what the license-plate readers use. However, these tools seem readily available and could be turned on. The information given indicates that if this is desired, it would be brought before the PAB. But how is one to know if these tools are turned on and used? Who monitors what tools are being used? Is this covered by the audits by the Special Projects Unit? But what is this unit? Is it a police unit? A city unit?

Please refer to the previous answers under the tech specifications section. The Chief of Police, and his designee, is responsible for oversight regarding what technology is possessed by the Department and how the technology is accessed and used, along with how data is maintained and shared. SDPD's procedures require the Special Projects Captain, and personnel assigned to this command, to maintain internal audits of this technology.

42. **Can you please explain the added benefit of the Smart SLs plus ALPR, instead of just using ALPRs like other cities? It wasn't entirely clear from the documentation why the City isn't just installing ALPRs instead of using both.**

    Recorded video of criminal activity has continuously been shown to be the most compelling evidence in trials, and in many cases, jurors have come to expect it, especially since SDPD transitioned to body worn cameras in 2016.

43. **Do any other government entities/task forces/units ever have access to this information, either directly or through a request process? If so, please describe. What are the processes and policies for other agencies access the data, such as through SDLECC fusion centers?**

    Requests and releases of ALPR data are described in SDPD's draft procedure which can be reviewed here: https://www.sandiego.gov/sites/default/files/draft-procedure-1.51-lpr.pdf

44. **Does the SDPD use or access any other databases for ALPR information (including private companies with ALPRs)?**

    Currently, SDPD does not operate its own ALPR technology, but does have a contract for limited services with Vigilant Solutions.

45. **Are data collected through Smart SLs or ALPRs checked against other databases (city, state, federal, private, etc.)? Which ones?**

    Video collected from Smart Streetlights is not used with additional databases, unless it captured a license plate of a vehicle wanted in connection with a criminal investigation. DMV data bases could be used by investigators to gain additional leads. License plate images are commonly checked against the following data bases: NCIC - National Crime and Information Center, CA SVS - California Stolen Vehicle System, NCMEC -National Center for Missing and Exploited Children, and Amber and Silver Alert for missing children and seniors.

46. **Who will be selecting and implementing the "privacy blocks" on the videos? What is that decision based on? How much time would that process take? How do residents and workers in the city request to see and ensure that private locations they occupy have been masked off?**

    SDPD works with the vendor to identify areas that should be blocked from view, and blocks are used in locations where persons have a legitimate expectation of privacy. SDPD inspects camera images and viewpoints to ensure these locations were properly masked. The Department has never received a request for specific information but would respond to such a request in accordance with all existing City and legal procedures and requirements.

47. The use policy states that videos will be deleted after 15 days. Can you please provide details of how synthesized data, metadata, or other raw data will be handled?

Video data to include meta data, is overwritten (effectively destroyed) every 15 days on a rolling (FIFO) basis. Ubicquia delivers the video hardware (source) and the video archive (edge storage). The automatic deletion of stored files is handled by Ubicquia.

48. Please detail policies for accessing data to monitor civilians engaged in protected First Amendment activity, prior to, during, and after events?

The procedures can be viewed these links:

https://www.sandiego.gov/sites/default/files/draft-procedure-1.51-lpr.pdf
https://www.sandiego.gov/sites/default/files/draft-procedure-3.33-smart-streetlights-investigations.pdf
https://www.sandiego.gov/sites/default/files/cpp-4.17-aafm.pdf
https://www.sandiego.gov/sites/default/files/completedepartmentpolicymanual.pdf
Policy 9.31 - Non-Bias Based Policing

49. What is the purpose of flagging dirty license plates? What data would be captured when the system scans a dirty license plate?

Automatic License Plate Recognition Technology (ALPR) is a component of the San Diego Police Department's crime-fighting strategy and its purpose involves the identification of vehicles associated with suspects, witnesses, or victims. ALPR enhances the Department's ability to focus its investigative resources, deter the occurrence of crime, and enhance public safety of the community. Please refer to the following document to understand how ALPR technology works: https://majorcitieschiefs.com/wp-content/uploads/2023/02/MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf

50. Is there risk of "Mission Scope Creep" and adding features and data to the systems?

This question has been asked and answered above as to how different functions and capabilities could be added to this requested technology. Refer to those answers to determine how risk is mitigated.

51. The use policy says "the primary purpose of the SSLs is to facilitate investigations of violent crimes and traffic offenses that result in the loss of life, significant destruction of property, and erode the public safety of community members." Please explain what would constitute a crime that "erodes the public safety of community members." Please also explain what secondary uses of the data will be made.

Please refer to the Department's presentation on this technology to see how it was used in the past to investigate matters the Department considers as “eroding public safety.” A secondary use of data considered would be to work with the City's traffic engineering team to review locations where fatal and serious collisions have occurred to determine if they could be engineered differently to prevent repeat occurrences.

52. What would be released as part of a public record request? How will the City ensure confidentiality of residents when the public requests information related to these data?

The information and data released via a California Public Records Act (CPRA) request depends on the request received and the legal requirements to release specific information. The Department has trained and dedicated personnel to answer requests, supervisory oversight, and legal advisors to assist them. When the Department releases video pursuant to a CPRA request, it has the capability to redact video images as necessary to ensure privacy. The California Supreme Court has considered and decided to allow agencies to exempt raw automated license plate recognition data from disclosure under CPRA provisions.

53. The survey is of a sample size of only 900+ and fully online. That excludes a large number of the population that will be impacted by the cameras. What efforts has the City taken to conduct a robust survey, including with translation services, of communities that will be impacted?

A 914 person sample survey is more than sufficient to provide accurate and reliable statistical measures for the City of San Diego. A San Diego Union-Tribune poll, published on the front page of that newspaper, sampled 547 voters to produce an accurate and publishable poll of San Diego residents. The poll was used in an October 6, 2020 article which gauged support for mayoral candidates, Barbara Bry and Todd Gloria. The Zencity survey was significantly larger in sample size. Furthermore, the survey referenced was conducted in both English and Spanish.

54. Survey methodologies are not appropriate for deliberation on complex problems where constituents lack important information to consider tradeoffs. When the ZenCity survey asked people if they were comfortable with ALPR, were they told that license plate data can build location profiles of their movements? Were they informed of the types of investigations that would be aided by this? Were they informed of the success rates of the program? Were they asked to select among various options for uses of the funds? Were they asked to select among various options for improving community safety?

The complete survey questionnaire text is available on the Department's website at www.sandiego.gov/police/technology. Any survey, to be broadly accessible, must be limited in length. The survey did pose various questions about comfort and perceived effectiveness of the use of technology. It used different scenarios in a methodologically sound manner. In fact, San Diego residents did express a wide range of opinions on these matters, which is reflected in the results. The survey also solicited and presented analysis of open-ended concerns about license plate readers.

55. The survey does not really get at people's preferences because they are not comparing surveillance to other things they are also familiar with and may prefer. For example, they couldn't choose between ALPRs and other government services, for example. Who designed the survey methodology in the City? Was anyone with advanced training in social science, such as a MS or PhD involved to identify these methods issues?

The survey was designed and supervised by Dr. Rachel Levenstein, who holds a PhD in Survey Research and Data Science from the University of Michigan. Dr. Levenstein has taught courses on survey research methodology and has nearly two decades of experience designing and leading large-scale public-sector research projects across the United States.

56. Has the City conducted any studies, broken down by city district and race/ethnicity, on perspectives regarding these technologies? Can we see the breakdown?

The City and Department sought to learn more about community perspectives regarding these technologies through community meetings, input provided through the Department website, and in the survey responses provided by Zencity. This information has been provided to the PAB in the Community Impact Report, the survey from Zencity, and by answering the Board's questions.

57. Can you provide us with the survey design and complete response data set so we can ask our questions of the data?

Survey design has already been provided in publicly available summary materials. Respondent-Level data is not provided to the City or Department in order to respect respondent privacy. This was promised to respondents in the disclosure at the initiation of

the survey. This is a standard best practice in survey research, and not unique to this survey.

58. Has the City made any direct changes to its plans based on community feedback? What specifically?

Yes, changes are being made based on feedback. For instance, the Department community liaison officers have met with religious leaders who requested that cameras near a parking lot be moved to alleviate fears they could record someone attending services and SDPD will accommodate this request.

59. How can someone exercise their data subject rights to access or correct their own data collected by these systems? (not a public records question, but an information practices and privacy rights question)

SDPD believes the data collected by these systems should be confidential, and not shared or open to the public for review except as permitted by applicable law, but is open to considering PAB recommendation for the Department in this area.

60. What does Council District 8 feel about the number of cameras proposed for that district? Have their questions about collaborations with ICE and CBP with this data been addressed? If so, how?

Some members from Council District 8 sought to understand the methodology used to designate the number of cameras proposed in this district, and other members indicated they would like as many as possible, particularly around shopping centers and business districts.

Concerns and questions about law enforcement partnerships with ICE and CBP are continually addressed by citing the Department's commitment to the California's Values Act, SB 54, and explaining that the Department does not conduct immigration enforcement, but rather continually works with these agencies to address criminal actions like those exposed through Operation Better Pathways related to human trafficking.

61. Referring to Table 8 of the impact report, what vendors do the other cities use?

The primary vendors that provide services and similar technologies to cities include: Axis Communications, Genetec, Flock Safety, Motorola Solutions, and Rekor Systems.

62. What outreach has the City done to learn from the other Cities that have completed and experienced the installations? What pros and cons? What changes did the city make to address these findings?

SDPD personnel participate in monthly meetings with county, state, and federal law enforcement partners, as well as quarterly meetings with agencies throughout the nation

to discuss the benefits and challenges of using evolving technologies. Many also attend and teach classes related to technology, and the need to balance its use to enhance public safety with privacy protections. Many of the lessons it has learned were published by the Major Cities Chiefs Association and provided to the PAB already, along with incorporating these lessons into the Department's draft procedures.

63. What has been the success rate of other cities using these technologies? Specifically for Seattle, which is the only one using both technologies.

Seattle documented their experiences with these technologies in impact reports which are provided for your review:

https://www.seattle.gov/documents/Departments/Tech/Privacy/SPD%20ALPR%20%28Patrol%29%20-%20Final%20SIR.pdf

https://www.seattle.gov/documents/Departments/Tech/Privacy/Situational%20Awareness%20Cameras%20WG%20SIR.pdf

64. What is this initial cost breakdown?

The impact reports provided to the PAB provide a breakdown of anticipated costs and funding sources, refer to them for detailed information:

https://www.sandiego.gov/sites/default/files/alpr-impact-report.pdf and
https://www.sandiego.gov/sites/default/files/smart-streetlights-impact-report.pdf

For the camera hardware, software, and connectivity there is a $4,000 per unit charge resulting in a total cost of $2,000,000 cost for 500 units to install.

65. What are the ongoing hardware maintenance costs?

The impact reports provided to the PAB provide a breakdown of anticipated costs and funding sources, refer to them for detailed information:

https://www.sandiego.gov/sites/default/files/alpr-impact-report.pdf
https://www.sandiego.gov/sites/default/files/smart-streetlights-impact-report.pdf

There is a one-time installation and maintenance cost of $1,500,000 for units installed and utilized during the proposed contract term.

66. What are the data storage costs?

If the Department determines it needs to store data from these technologies associated with a criminal investigation it can be done using existing video management services possessed by the Department which are already being used and funded.

67. What are the ongoing software maintenance costs?

The impact reports provided to the PAB provide a breakdown of anticipated costs and funding sources, refer to them for detailed information:

https://www.sandiego.gov/sites/default/files/alpr-impact-report.pdf
https://www.sandiego.gov/sites/default/file

This was answered in the initial cost breakdown.

68. What is the software and hardware upgrade schedule?

Ubicquia continuously and remotely deploys software upgrades to devices to improve performance and reliability. The hardware is intended to last the life of the contract and would only be replaced with like hardware in the event of failure.

69. What does the Support Model look like in cases of failure?

The customer will initiate a support request to Ubicquia by emailing support@ubicquia.com. Ubicquia will then assess the reported issue and respond in conformance to its SLA based on severity of the reported issue.

70. The police presentation said the cameras helped in 100 cases out of about 1 million, which is only 0.1%. Is this significant enough to warrant the expense and the potential risks?

That is not what the Department represented in its presentation. Specifically, the Department receives approximately 1 million calls for services a year, most do not require a criminal investigation, or investigative resources, and the Department has purposely restricted the use of Smart Streetlight technology to matters that threaten public safety and are broadly supported by community members.

In the 400 cases where it was used, in about 100 cases the technology was critical to investigate crimes like homicide, sexual and aggravated assault, and robbery. By "critical," the Department means the case would likely not have been solved without the availability and use of this technology. In another 100 instances, the cameras facilitated the investigation in a meaningful way.

By way of analogy, matters that can be framed as statistically insignificant often have the most impact. For instance, according to data from the Racial and Identity Profiling Act (RIPA), law enforcement stops of persons that result in officers using deadly force takes place at a rate of .00004 annually, meaning that 99.99996% take place without deadly forced being used. However, when multiplying .00004 by the 4 million stops made in

California, it produces roughly 160 stops where deadly force was used. While the use of deadly force could be described as statistically insignificant, the impact it has at every level of government and discussion related to police reform, training, operations, policy, and legal decisions, not to mention the officers and community members involved in these interactions, cannot be overstated.

Smart Streetlights and their use could also be framed as statistically insignificant, but crime victims and their families, along with the members of law enforcement and elected officials that seek to provide justice to them and the safety of their communities, should support the expense and minimal risks associated with their use. Lastly, understanding the cost of crime, which has been presented in many research studies, more than justifies the use of this technology if it even deters one homicide from happening every few years, see Hidden in Plain Sight here:
https://www.rand.org/pubs/occasional_papers/OP279.html

71. What would happen if this technology were not approved by the City?

The Department would continue operating without it, and in all likelihood, there will be some violent crimes that occur that will go unsolved without this technology being available. As stated, the Department documented approximately 100 crimes investigated with Smart Streetlight technology that were critical to the identification of suspects and their prosecution.

72. You mentioned that there were nearly 1 million 911 calls in the two years the system was in place but that the technology resulted in only 400 investigations and 100 convictions. How does this compare to results without the system? There is annual variability in crime statistics. Is the two year "reduction" in crime really a result of the cameras?

The statements in the question misstates SDPD's presentation before PAB. First, SDPD receives approximately 1 million calls for service a year. Next, Smart Streetlight technology was used in 100 investigations where the video evidence was critical in solving the crime being investigated, and in another 100 cases where it facilitated the investigation in a meaningful way. Again, the technology had a positive impact in 50% of the cases where SDPD chose to employ it. If Smart Streetlights had been unavailable, there would be 100 significant crimes which most likely would have gone unsolved including those involving murder and sexual assault.

While there are many variables related to crime statistics, and causal relationships are difficult to prove, SDPD's use of video evidence from Smart Streetlights benefitted case clearance rates and allowed it solve cases that it would not have been able to solve without it. This will most likely remain true if this technology remains unavailable to the Department and without useful leads generated by the proposed technology SDPD will solve less violent crimes (like murder, sexual and aggravated assault and robbery). Cases that go unsolved reduces confidence in the Department and causes community members to view the Department as ineffective. It also creates unwillingness by some to assist

with investigations, because they don't believe it will benefit the communities where they live.

73. There are other ALPR vendors that might be more affordable. Has the city evaluated a standalone ALPR system? Why or why not? If so, which ones? How do these compare with what other cities are using?

This question was previously answered. Yes, the Department is very familiar with the capabilities and pricing of numerous camera and ALPR systems being utilized by cities in San Diego County and in cities throughout our state and nation. SDPD believes that Ubicquia offers a product that best fits the needs of our organization and the City's public safety goals. Existing City procedures and contract requirements ensure SDPD has done its due diligence in regard to evaluating technologies it seeks to purchase.

74. Has the City or its vendor ever considered monetizing data from its Smart SL systems?

No. SDPD has not considered monetizing data from Smart Streetlights.

75. What were the constitutionality arguments raised by cities that passed ALPR technology such as Seattle?

Legal arguments and concerns over the use of ALPR technology in Seattle, and elsewhere, typically center on the following topics: reasonable privacy expectations of those in vehicles on public roadways, persistent tracking and the nature of ALPR technology, the nexus between license plates and personally identifiable information, collecting and sharing ALPR data, and the degree of intrusion authorized by ALPR hotplate detection.

See https://majorcitieschiefs.com/wp-content/uploads/2023/02/MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf

76. Someone from Alliance SD did a public report on SB-54. What is SDPD's track record of compliance?

Alliance SD referenced a report that was written by the San Diego Immigrant Rights Consortium in 2021. The report highlighted law enforcement agencies in San Diego County that have incorporated the requirements of SB-54 into their written policies, which is not required by the law. As stated by Ern Tsurumoto from Alliance San Diego, "There are some departments that are probably fully in compliance with SB 54, but they don't have it written in their policy."

SDPD believes it is in compliance with SB 54 but has initiated a review to see if any of its policies and procedure should be further updated to reflect its commitment to following this important legislative act.

77. Checks and balances are important in government, particularly when considering new technology and data uses. Why does the use policy not require a warrant to access camera data?

Video evidence from Smart Streetlights in San Diego has routinely been used, and allowed by the courts, to prosecute persons suspected of violent crimes without a warrant being required to obtain it. The San Diego Police Department, in partnership with prosecuting agencies, will continue to follow all statutory and constitutional law regarding the Fourth Amendment.

78. The police presentation said the cameras are in public places where there is no reasonable expectation of privacy. This is arguable. People have some knowledge of their environment and a corresponding expectation; for example, that their neighbors or other people living or driving there will see them. Moreover, this will only be when these people look; they are not recorded. With cameras, there is constant recording and no indication of who will see the data. How would you respond to issues about surveillance cameras raised by the EFF?

The article by Electronic Frontier Foundation on Street Level Surveillance largely describes different types of surveillance technologies, real time crime centers, and data sharing. The issues highlighted are primarily related to facial recognition, which the Department has not requested, and the threat from hacking surveillance technologies. In response, the Department, and the City are always concerned about computer hacking and its serious impact. A number of safeguards are currently in place to protect all City data and computer systems.

79. The police presentation says that there is no personally identifiable information collected. However, video, photos, and information collected through an ALPR are clearly categorized as "personal data" by California law. Why does the SDPD not feel this is personal information?

A license plate number is an anonymous code unless combined with other registration information containing owner/operator information (i.e., a department of motor vehicles database). The Department must access a separate database (DMV database) to draw specific information about the registered owner of the vehicle, after having a “need to know and a right to know.” This would be after a crime has already occurred (e.g., a stolen vehicle creates a “hit,” or a vehicle is associated with a qualifying crime). Thus, an ALPR record is generated from publicly available data and corresponds with detecting a vehicle, not an individual, at a specific location and time.

80. The doctrine that there is no reasonable expectation of privacy in public spaces is shifting rapidly. Even as far back as the 70s, the Supreme Court said that "an individual operating or traveling in an automobile does not lose all reasonable

expectation of privacy simply because the automobile and its use are subject to government regulation." The Court also distinguished between limited monitoring and 24-7 surveillance of the community. Smart SLs and ALPRs collect (and analyze) information in a detailed, indiscriminate, encyclopedic, and systematic way, allowing municipalities to collect information about an individual's detailed movements in space and time. Courts have increasingly declined to treat 4th Amendment protections in a rigid way, particularly in response to rapid advances of technology. For example, the Massachusetts Supreme Court has stated that "with enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and constitute a search for constitutional purposes." How does the SDPD address this? How would the impact report be edited to account for this nuance?

SDPD disagrees with the characterization that Smart Streetlight and ALPR technology, particularly in this proposal, possess the substantial capabilities, described in the statement from the PAB. GPS tracking technology and cell-site location information, the subjects of prior court decisions, enable persistent automated tracking in a singular device capable of following an individual's activity with such detail and scope that the techniques constitute a search. It is not possible for Smart Streetlights or ALPR to accomplish the type of tracking allowed by GPS and CSLI technologies, unless they were installed on virtually every corner of the City. SDPD further addresses this concern of persistent and automatic tracking through a very limited deployment of Smart Streetlights and ALPR technology throughout the City's 350 square mile jurisdiction. The Department does not feel its impact reports require editing. SDPD remains committed to staying abreast of any developments in this area of law.

Conclusion:

The San Diego Police Department has carefully considered all questions about the Smart Streetlights program put forth by the Privacy Advisory Board. In total, SDPD reviewed and responded to 80 questions.

The San Diego Police Department will comply with the Surveillance Ordinance. The PAB is a new processes of technology vetting added to a system of pre-existing City vetting processes. Smart Streetlights are both information technology and surveillance technology as defined by the Surveillance Ordinance. Information technology is already subject to vetting at the Department through our own IT processes, and through the City's IT Governance Processes. The Department and the City work tirelessly to ensure our information technology systems are sound, protected from malicious intrusions and protect the civil liberties and data of San Diegans. The process of complying with the Surveillance Ordinance is unprecedented, uniquely challenging, and all parties are learning their roles and responsibilities. The Department protects public safety while simultaneously protecting civil liberties. Our responsiveness to the PAB and its questions is the newest aspect of vetting surveillance technology.

Respectfully,

Acting Captain Charles Lara
Special Projects/Legislative Affairs