



Memorandum

TO: SMART CITIES AND SERVICE
IMPROVEMENTS COMMITTEE

FROM: Rob Lloyd

**SUBJECT: DIGITAL PRIVACY POLICY
IMPLEMENTATION STATUS
REPORT**

DATE: September 2, 2021

Approved 

Date 8/23/2021

RECOMMENDATION

Accept the status report on status Digital Privacy Policy implementation, including review, engagement, and technical protocols.

OUTCOME

Provide an update on the status of Digital Privacy Policy implementation, reviews, engagement, and technical protocols for input.

BACKGROUND

In 2018, the City engaged pro bono services from the Harvard Cyberlaw Clinic (HCC), based at the Berkman Klein Center for Internet & Society, to initiate a strong approach to privacy in the City's adoption of new, data-intensive technologies. Core HCC recommendations were:

- (1) Develop a set of Privacy Principles through a combination of community engagement and subject matter expertise.
- (2) Use the Privacy Principles to develop a Privacy Policy for the City. Said policy would guide emerging uses of identifying technologies and data, providing direction on the City's needs left unaddressed by Federal Government inaction.

The Harvard team noted that the privacy landscape is changing and that no true standard has emerged for communities to follow. The legal team also described that while few Cities in the United States have developed both privacy principles and privacy policy, San José was wise not to wait. Some data use mistakes can have permanent effects.

Privacy Principles

The City applied the HCC recommendation and established a three-part approach to create and scrutinize its Privacy Principles:

- (1) **Creation of a Privacy Working Group.** The Privacy Working Group consists of senior staff from the City departments responsible for implementing the Privacy Principles and Digital Privacy Policy. It receives and integrates operational requirements, legal guidance, input from the Privacy Advisory Taskforce, and input from public forums.
- (2) **Creation of a Privacy Advisory Taskforce.** The Privacy Advisory Taskforce meets quarterly with members with subject matter expertise from industry, nonprofits, and academia. Members provide guidance on the City's approach and the Privacy Principles.
- (3) **Engagement with the Community.** Community input was gathered through a series of stakeholder interviews and public forums conducted in English, Spanish and Vietnamese. The City sees an ongoing need for public engagement as public sentiments and tolerance of uses of personal data continue to evolve.

Upon conclusion of the community and expert input efforts, the City's Privacy Principles were approved by the Smart City and Service Improvements Committee on June 6, 2019¹. The Principles were then adopted by City Council City Council at its September 17, 2019², meeting:

- **We value privacy**— We affirm that privacy is an inherent human right. San Jose commits to fully evaluating risks to your privacy before collecting, using, or sharing your information.
- **We collect only what we need**— We collect only what is required to provide and improve City services and comply with the law. We seek community input about what information is used and collected.
- **We are open and transparent**— We are transparent about what information we collect, why we collect it, and how it is used. We commit to being open about our actions, policies, and procedures related to your data. We make our policy documents publicly available and easy to understand.
- **We give you control over your data**— We will provide you with the information to make an informed decision about sharing your data. We have clear processes that ensure data accuracy and provide you visibility into what data the City has collected from you.
- **We share only what we need**— We anonymize your information before we share it outside the City, except in very limited circumstances. Business partners and contracted vendors who receive or collect personal information from us or for us to deliver City services must agree to our privacy requirements.
- **We design for privacy and security**— we integrate privacy and security into our designs, systems, and processes. We commit to updating our technology and processes to effectively protect your information while under our care. We follow strict protocols in the event your information is compromised.

¹ 6/6/2019 Smart Cities and Service Improvements Committee Meeting, Privacy Policy Update—
<https://sanjose.legistar.com/LegislationDetail.aspx?ID=3947551&GUID=11790DDC-6137-47CC-AF31-7B730A1AE1C2>

² 9/17/2019 City Council Meeting, Privacy Policy Update—
<https://sanjose.legistar.com/LegislationDetail.aspx?ID=4123701&GUID=C04F704C-B022-404D-8836-5DA8B63CCCB9>

Privacy Policy Development

Development of the City's Digital Privacy Policy mapped to three phases, once the Privacy Principles were adopted:

- Phase 1– Development of Digital Privacy Policy;
- Phase 2– Implementation of Digital Privacy Policy and associated tools; and
- Phase 3– Continuous evaluation and input, resulting in policy and process improvements.

With one-time funding in the City's 2019-2020 Adopted Operating Budget, a temporary 1.0 Full-Time Equivalent (FTE) Senior Privacy Policy Analyst was hired into the Office of Civic Innovation in November 2019. Dr. Papazoglakis worked with the Privacy Working Group, Privacy Advisory Taskforce, and leads staff from the Information Technology Department, the Police Department, and the City Manager's Office to assemble and refine a draft Citywide Digital Privacy Policy.

In March 2020, Digital Privacy efforts were paused as the City focused on COVID-19 pandemic response. Staff were reassigned to the Emergency Operations Center and in June 2020, due to COVID-related budget reductions, the Senior Privacy Policy Analyst position was part of cuts. The Digital Privacy initiative was absorbed by Office of Civic Innovation and Information Technology Department staff, all of whom were assigned fully to COVID-19 response.

Pandemic response efforts have since underscored the importance of privacy. Increases in the number and reach of digital tools and data sources staffs used to address public health, economic, community outreach, education, and staff needs were dramatic. Thus, Civic Innovation and Information Technology staff took time to complete the Digital Privacy Policy in parallel. City Council reviewed and accepted the resulting policy at its December 8, 2020, meeting. Council Policy 0-46³ had an effective date of July 1, 2021. The program was matched with a permanent 1.0 FTE Digital Privacy Officer position (using the Enterprise Technology Manager classification) in the City's 2021-2022 Adopted Operating Budget, allocated to the Information Technology Department.

ANALYSIS

Privacy Policy Development Approach

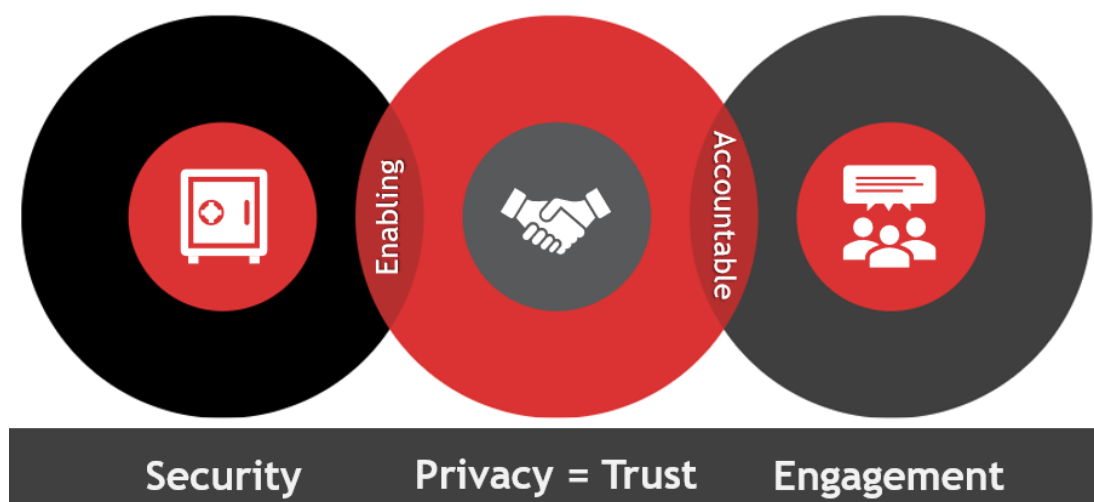
Throughout development work, staff reviewed best practices of other government agencies to create an approach that leverages the lessons learned from privacy policy leaders, and that is tailored to the City of San José's needs. Three cities moved very early on privacy—the City of Seattle, City of New York, and City of Chicago—in addition to two international cities HCC identified. The City of Seattle is considered the early pacesetter in local government privacy efforts in the United States. For comparison, the City of Seattle has a 5-person Privacy Office with significant legal background, that has evolved since 2015. More recently, the team coordinated an equity lens in privacy reviews with their Race and Social Justice Initiative.

³ Council Policy 0-46, Digital Privacy Policy—
<https://www.sanjoseca.gov/home/showpublisheddocument?id=68053>

The City of San José's privacy approach borrows elements of its framework from General Data Privacy Regulations (GDPR) that govern European Union nations and organizations. A team from the City of Dublin, Ireland, worked with City of San José staff—the two are Sister Cities—to evaluate potential practices and applicability in the United States setting.

Privacy Policy Deliverables

The purpose of the City's Privacy Principles and Digital Privacy Policy is to implement and operationalize privacy governance in practice. Staff's approach builds on the concept that the City must maintain the trust of the community it serves in order to be effective in its use of new technologies and data analytics. Improvements in service delivery and the chance to address equity goals through the use of data balance with strong information security controls, transparent policy, and verification reviews. Ultimately, Privacy is a proxy for Trust.

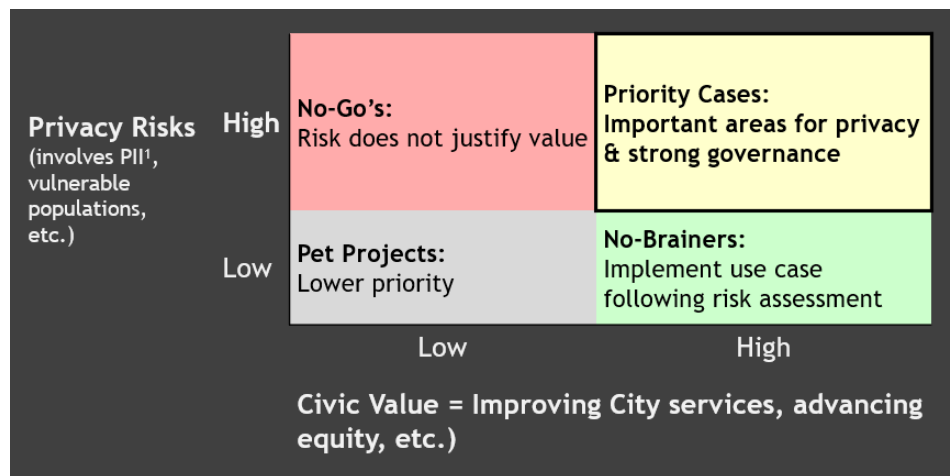


With research and input gathered from stakeholder groups, San José's privacy approvals processes focus on seven policy elements:

- **Notice:** Providing notice about the collection, use, and sharing of personal information at the time such information is collected. The City will make every reasonable effort to provide a privacy notice when basic municipal services are requested or delivered.
- **Retention:** Developing, maintaining, and following the City data retention schedule. Departments must ensure that identifying information is deleted or deidentified after the retention period expires. In the event of a conflict between this Policy and the Public Records Act, Sunshine Act, or other law governing the disclosure of records, the applicable law will determine our obligation in support of open and transparent government.
- **Minimization:** Minimizing the collection and processing of identifying information and limiting collection to only what is necessary to provide services and to conduct business. When personally identifiable data is required to deliver or improve a service, departments must anonymize, de-identify, pseudonymize, or otherwise mask this information.

- **Accountability:** Maintaining documentation, available for public review and third-party monitoring, to demonstrate compliance with our privacy principles and Policy. If any information under our control is compromised or if residents are impacted due to a breach of security or negligent maintenance of information systems, the City will take reasonable steps to investigate the situation and notify those individuals whose information may have been impacted.
- **Accuracy:** Making every reasonable effort to provide the public with information on how predictive or automated systems are used and will institute processes to correct inaccurate information or methodologies in those systems. City Departments may use predictive or automated systems and technologies to support decision making, but some degree of human input and oversight into decision making is also required.
- **Sharing:** Following clear data governance procedures and instituting information sharing agreements when sharing information with outside entities, which shall strive to enable effective information sharing while following the City's Privacy Principles and this Policy. Nothing in this policy shall preclude data sharing with research or other institutions if clear data sharing agreements are in place which govern the use of data pursuant to the standards of this Policy.
- **Equity:** The City is mindful of the populations it serves and how data about members of the public, including vulnerable populations, can and should be used. The City will strive to advance equity in a data-driven way while ensuring that PII is used only in accordance with this policy. The City will work to mitigate the impact of algorithmic and data bias.

Implementation efforts in 2021 are focusing on process levers where Digital Privacy has a connection to administrative routines. Specifically, for any initiative that requires use of Personally Identifiable Information (PII), budget requests, procurement requests, and project initiations cannot occur without analysis and review of how the project or program performs against the seven privacy elements. In three cases, the City declined a major project based on the inability to full address Minimization, Equity, and Retention concerns. The City's rubric ultimately focuses the organization on cases where Civic Value is high, and Privacy Risk is low.



Long-term, staff has a more robust implementation work plan. The approach will be updated when the Digital Privacy and Surveillance Ordinance initiatives rise to the City Roadmap's active priorities.

Prioritized Backlog FY 2021-2022		
No.	Initiative/Policy Name (by points and alphabetized)	Points
1	Boost San José's Retail Sector (D1)	7
2	Update Council's Wage Theft Prevention Policy	7
3	Anti-Displacement Preference Ordinance	6
4	Local Hiring/Business/Apprentice Utilization Program	6
5	San José Surveillance Ordinance (D2) + Digital Privacy Policy Implementation	6
6	Traffic Calming Policy for Residential Neighborhoods	6
7	Urban Greening Implementation Plan	6
8	Universal Preschool Policy (D5)	5
9	Staffing Analysis (D7)	4
10	Universal Development Fee	4
11	Affordable Housing Construction Policy on City Land (D9)	3
12	Citywide Goals + KPI Dashboard (D10)	3
13	Private Percent for Art	3
14	Transit First Policy Framework	3

For reference, full Privacy Program deliverables include:

- *Citywide Privacy Policy* document providing clear direction and requirements to departments, private sector partners and the community regarding the collection and management of personally identifying information. (Done)
- *Citywide Data Retention Schedule* outlining a data retention and disposal schedule for various public records created or received by the City.
- *Privacy Impact Assessment Toolkit* creating a new review process called a Privacy Impact Assessment to identify and evaluate potential public privacy impacts of proposed partnerships and/or technologies, and ways to mitigate those impacts as appropriate.
- *Training Framework for City Departments* to provide guidance to City staff to ensure broad understanding and application of privacy framework.
- *Master List of Sensing Technologies* compiling a list of sensing technologies (including audio and video) used by department and with descriptions to ensure proper handling.
- *Sustainable Privacy Governance Model* establishing the responsible groups and/or individuals who must review new and existing projects using the privacy impact assessment process, along with authorities.
- *Stakeholder Engagement for Guidance and Feedback* to be conducted through periodic meetings, and will include the community, the external Advisory Taskforce, and the internal Privacy Working Group. (In Process)

CONCLUSION

Base privacy practices are in place to operationalize the core parts of the City's Digital Privacy Policy, which was effective July 1, 2021. Where Personally Identifiable Information is to be

used, budget requests, procurement requests, and project charters require a full analysis of how data use will properly administer Notice, Retention, Minimization, Accountability, Accuracy, Sharing, and Equity requirements. Where privacy cannot be fully addressed and/or proper controls cannot be implemented, the projects and purchases are not executed. City contracts now have standard language addressing privacy controls and minimum expectations.

Once the City's new Digital Privacy Officer is hired, staff will identify tools and improvements to augment the administrative processes now in place, and to deliver the full Privacy Program work plan through 2022 and 2023. Educational programs, cataloging of privacy-impacting assets, public engagement efforts, refining contract language, and continuous improvement routines will require time and contributions from many stakeholders.

Of special note, the City of San José is teaming with the Center for Digital Government (CDG) to create a baseline package of principles, policies, job descriptions, privacy content for an online research library, and Privacy Framework coordination with the National Institute of Standards and Technology. This will allow peer governments to accelerate their adoption of digital privacy and will grow the national community of practice. CDG noted few governments have made progress on the topic, but have identified the clear importance in local and state government.

EVALUATION AND FOLLOW-UP

Moving from Privacy Principles to Privacy Policy and Implementation

The Privacy Advisory Task Force communicated clearly three themes in its August 2021 meeting: (1) The need to take concrete steps now, as data privacy emerges as a concern in new technologies, surveillance, and public health/safety uses; (2) the importance of building privacy knowledge and practices across in the City; and (3) the role of Task Force members to challenge the City to maintain the highest levels of public responsibility. The Task Force's bias towards action and the deep expertise of members is an asset to the San José community.

At its August 2021 meeting, the internal Privacy Working Group communicated its recognition of the importance of Digital Privacy, the effective date of the policy, and requirements to address the Digital Privacy Policy's seven elements in future requests. The group expects to improve the practices through 2021.

The Digital Privacy Officer (DPO) and Chief Information Security Officer (CISO) will refresh the larger Privacy implementation plan, slated for the four months following the hiring of the DPO. Collaboration between the DPO and CISO is key, as the City matches security controls with privacy practices. The team will identify the go-forward approach for reviewing a sample of existing City programs that use PII in that planning work.

Staff will return to the Smart Cities and Services Improvements Committee in 2022 to update Committee Members on status and initial program metrics.

CLIMATE SMART SAN JOSE

The recommendation in this memo has no effect on Climate Smart San José energy, water, or mobility goals.

COMMISSION RECOMMENDATION/INPUT

This report was not presented at a Commission.

CEQA

Not a Project, File No. PP17-009, Staff Reports, Assessments, Annual Reports, and Informational Memos that involve no approvals of any City action. (Information Technology)

PUBLIC OUTREACH

Privacy Policy Public Engagement

Similar to the public engagement performed to evaluate the Privacy Principles, the Privacy Development Team will engage the community using public forum meetings and surveys as needed. Public engagement will pivot to input on Privacy Impact Assessments in the future. Public forums will be conducted in English, Spanish, and Vietnamese and may utilize online feedback mechanisms for collecting comments.

COORDINATION

This memorandum has been coordinated with the City Attorney's Office, the City Manager's Office of Civic Innovation, and the City Manager's Budget Office.

/s/
ROB LLOYD
CHIEF INFORMATION OFFICER
Information Technology Department

For questions, please contact Rob Lloyd, Chief Information Officer, at (408) 535-3566.