CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

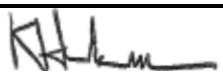
Memorandum

TO: SMART CITIES AND SERVICE IMPROVEMENTS COMMITTEE

FROM: Rob Lloyd

SUBJECT: PRIVACY POLICY UPDATE

DATE: October 29, 2020

Approved  Date 29 October 2020

RECOMMENDATION

a) Accept the written update on the completion of the City's Privacy Policy and roadmap to implementation.
b) Cross-reference this report to the full City Council for approval of the Digital Privacy Policy, to be heard at a City Council meeting in December 2020.

BACKGROUND

In May 2018, the City of San José engaged and received pro-bono guidance from the Harvard Cyberlaw Clinic (Harvard), part of the Berkman Klein Center for Internet and Society, to shape a strong approach to privacy for City services and the adoption of new, data-centric technologies.

Harvard's recommendations were to:

(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 to provide a framework and standards for operationalizing the Privacy Principles in an environment where the still-emerging landscape of technology and data continues to evolve.

These recommendations form the first two of four phases that characterize the City's approach to privacy policy development and implementation:

- Phase 1 – Development of Privacy Principles;
- Phase 2 – Development of Privacy Policy;
- Phase 3 – Implementation of Privacy Policy and associated tools; and
- Phase 4 – Continuous evaluation and input, resulting in policy and process improvements

City Council approved the City's Privacy Principles in September 2019, thereby completing Phase 1. In that same month, as directed, staff presented and the Smart Cities and Service

Improvements Committee approved a workplan for Phase 2 to advance a full Digital Privacy Policy. Core to this workplan was one-time funding in the City's 2019-2020 Fiscal Year Operating Budget for an overstrength Senior Privacy Policy Analyst, who started within the Office of Civic Innovation in November 2019. This funding increased personnel within the City devoted to privacy to approximately 1.25 Full-time Equivalent (FTE). By comparison, Seattle, Washington and Dublin, Ireland, municipal peers with more longstanding privacy programs, have privacy offices of 3.0-4.0 FTE, in addition to information technology and departmental staff to aid implementation. By early 2020, staff funded through the 2019-2020 Fiscal Year had completed several elements of the Phase 2 workplan, including a draft of the Digital Privacy Policy.

In March 2020, work on the Digital Privacy Policy was paused as the City refocused on the COVID-19 pandemic, and staff working on privacy issues were reassigned to that emergency response. In June 2020, due to COVID-1- related budget reduction targets, one-time funding for the 1.0 FTE Senior Privacy Policy Analyst was not continued in the City's 2020-2021 Fiscal Year Operating Budget. Future privacy work was contemplated to be absorbed by remaining staff, all of whom remain assigned to full-time work for the COVID-19 response.

COVID-19 has increased the number of digital tools and platforms in use by the City as work has shifted to be more remote. Greater than 2,400 City employees (approximately 36% of City workforce) are now fully working remotely. The City should expect the number and breadth of City services provided digitally to increase as the Drive to Digital initiative focuses on reimagining City services to be safe and effective in the era of COVID-19. The adoption and new technologies and processes increase the relevance of the City's privacy posture.

ANALYSIS

Advances in technology, corporate globalization, and data valuation are accelerating faster than policy can be written to support human rights and safeguard the public's trust in private and public institutions to protect their privacy and their data. The United States currently does not have a federal strategy or policy related specifically to digital privacy. At the state level, some states, including California, have passed legislation, but that legislation only applies to institutions that monetize data and not to cities like San José who do not. San José's Privacy Principles affirm that privacy is an inherent human right, but currently, the United States lacks a national digital privacy framework, and state-level privacy legislation is not based on a human-rights framework, focusing instead on the potential economic value of personally identifiable information (PII).

Europe, however, has led the world in human rights driven privacy regulations for decades. In May 2016, the European Union adopted the General Data Privacy Regulations (GDPR), crafted through aggregating, normalizing, and "digitizing" the human rights-based privacy policies across the European Union and other progressive countries. GDPR represents the most comprehensive privacy policy in the world, and all of Europe as well as many other countries

have enacted GDPR as privacy legislation applicable to the public and private sector. Additionally, many private sector companies, including Microsoft and Facebook, have formally or informally called for GDPR to be scaled worldwide.

While the future of privacy legislation in the United States is unknown, there are good reasons for San José to adopt GDPR as a guiding framework for its citywide privacy policy and implementation framework:

- **Alignment with San José's Privacy Principles –** implementing a policy framework that protects privacy as a human right;
- **Accelerated policy development and implementation** – leveraging best practices and lessons learned from other leading institutions;
- **Minimized policy rework** – aligning San José's privacy policy with the ongoing evolution of the world's most comprehensive privacy policy; and
- **Leading the nation** - advancing the City of San José's leadership role in smart city policy development including privacy, 5G next generation network deployments, and digital equity.

Given these benefits, staff used GDPR as a guiding framework for developing a Digital Privacy Policy recommended for City Council approval. The remainder of this memo provides additional detail on the Digital Privacy Policy development process and next steps for implementation.

Privacy Policy Development Process
The City's privacy policy development process was primarily informed by input from three sources:

(1) **Case studies** of other cities who have modeled privacy programs on GDPR;
(2) The City's **Privacy Advisory Task Force**, comprised of community leaders on privacy from the nonprofit, technology, academic, law enforcement, and government sectors;
(3) **Stakeholder engagement**, including community input, gathered via public forums in three languages as part of the development of the Privacy Principles, and guidance from the City's Departmental Privacy Working Group, comprised of representatives from departments throughout the City, including the Fire Department, Library Department, Environmental Services Department, Department of Transportation, Parks, Recreation and Neighborhood Services Department, Police Department, and Housing Department.

Staff review of case studies and best practices across government agencies identified Seattle and Dublin as pacesetters in local government privacy. Seattle launched their privacy program in 2015, and their comprehensive program includes an explicit focus on embedding an equity lens in their adoption of evolving Smart City technologies. Dublin launched their privacy program in 2018. Though each take distinct approaches, both structured their privacy program around the core elements of GDPR: (i) Risk Assessments, which assigns the degree of privacy risk for projects, systems, and technologies that use PII; and (ii) Data Protection Impact Assessments

(DPIA), which identify corrective actions for projects with a high risk to the individual rights of the data subject or where new technologies are used.

In crafting the Digital Privacy Policy, staff adapted lessons learned from Seattle and Dublin, as well as feedback from the City's Privacy Advisory Task Force and stakeholders throughout City departments. San José's Digital Privacy Policy would accomplish four goals:

(1) Define clear categories of personally identifiable information (PII) covered by the policy;
(2) Create standards to assess privacy risk across City departments, offices, and vendors;
(3) Direct creation of GDPR-based procedures for assessing privacy risk; and
(4) Create initial privacy governance and authority within the City Manager's Office to carry out Council direction.

The Digital Privacy Policy, if approved by City Council, would provide standards and an operational framework for implementation of the City's Privacy Principles to guide City projects, services, and security practices.

Implementation Considerations and Next Steps

The key takeaway from case studies of the European Union, Seattle, and Dublin is that the implementation of a privacy policy is a heavy lift that must be planned and budgeted by any City undertaking a comprehensive privacy policy. Seattle and Dublin have committed to implementation through dedicated ongoing funding and staffing over several years. Seattle started with a dedicated office of 3.0 FTE, which has now grown to 4.0 FTE in its fifth year of operation. Dublin has a dedicated office of similar size, and both cities have identified additional staff within departments as necessary to implement their privacy policies citywide. Dublin estimates that it will take approximately 8 years to be fully compliant with GDPR:

- Year 1 - learning and planning;
- Year 2 - evidence of risk assessments and impact assessments;
- Year 3 - begin compliance and highest priority impact assessments; and
- Years 4-8 - full compliance with GDPR and impact assessments.

Currently, the City lacks this level of ongoing funding commitment to privacy policy implementation. Therefore, staff recommends that implementation of the privacy policy begin with a planning process to take place through the remainder of 2020-2021, which will inform City Council funding decisions for 2021-2022. This timing will also position the City to observe and adapt to potential changes on the Federal level, as the current status quo of inaction on digital privacy may change in a new presidential administration, and the City should prepare for this scenario and the need to increase investment in privacy for 2021-2022. Staff plans to present funding options for further implementation as part of the 2021-2022 budget process.

For the remainder of 2020-2021, staff will be focusing on Phase 2 deliverables, including:

1. Initial planning and design of Risk Assessments and Data Privacy Impact Assessments;

2. Initial design of clear privacy governance to enable clear decisions and action based on GDPR assessment processes; and
3. Community outreach and education in three languages to more deeply educate residents, understand community concerns, and inform design of future implementation. This effort is already funded as part of the remaining $99,000 budgeted for privacy work in 2020-2021 (see Budget Reference section) and will be a continuation of work with nonprofit partner CivicMakers already started in March 2020 and then paused due to COVID-19.

Implementation of this policy citywide beyond a minimal and reactive posture will require additional funding. The examples of Seattle and Dublin are instructive to understand the level of investment required for full privacy policy implementation. The implementation scenarios outlined below illustrate the outcomes at different levels of ongoing funding. No budget action is requested in this memo; these scenarios are presented for informational purposes only, and as a precursor to budget discussions for 2021-2022 and beyond.

Scenario	**Reactive Privacy Posture**	**Responsive Privacy Posture**	**Proactive Privacy Posture**
Description	Assess, secure, and respond to only a limited number (estimated 10% coverage) of high-risk systems Minimal capacity to adapt to new federal privacy frameworks	Assess, secure, and respond to some (estimated 50% coverage) of privacy-relevant systems and community requests Reasonable capacity to adapt to new federal privacy frameworks	Assess, secure, and respond to almost all (estimated 90% coverage) privacy-relevant systems and community engagement Full capacity to lead the nation in adopting new privacy frameworks Invest in innovative citywide technology and processes to protect privacy
Estimated Additional Annual Funding	None	$500,000	$1,000,000

CONCLUSION

The City Council approved San José's Privacy Principles in 2019. Council approval of the Digital Privacy Policy would allow the City to move forward with implementation of those principles at an operational level to guide City projects, services, and security practices. The proposed next steps for implementation are designed to position the City to plan to implement

privacy with an equity lens, and to adapt to potential evolutions in the technology and legal landscape. However, current funding for privacy is not sufficient to enable full-scale implementation. Cities like Seattle and Dublin are already making significant investments in privacy, and given the potential for near-term action on privacy at the federal level, the City should prepare to make investments moving forward. Even in the absence of federal action, this policy area is dynamic, and the City must expect to adapt over the coming years based on changing standards, legislation, and community input.

EVALUATION AND FOLLOW-UP

This Digital Privacy Policy is a step towards implementation of the Privacy Principles. Evaluation throughout implementation is critical, and staff will provide a verbal update on implementation planning to the Smart Cities and Service Improvements Committee. Additionally, staff anticipates bringing forward funding options for privacy policy implementation as part of the 2021-2022 budget.

CLIMATE SMART SAN JOSE

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

PUBLIC OUTREACH

Staff will continue to engage the Privacy Advisory Task Force comprised of community leaders from the nonprofit, technology, academic, law enforcement, and government sectors. Additionally, staff is planning a community education and outreach process to be conducted during the remainder of 2020-2021, to be led by nonprofit CivicMakers, which will include outreach and engagement in English, Spanish, and Vietnamese.

COORDINATION

This memo was coordinated with the Office of the Mayor, the City Manager's Office, the City Attorney's Office, the City Manager's Budget Office, the Library Department, the Police Department, and the Housing Department.

COMMISSION RECOMMENDATION/INPUT

No commission recommendation or input is associated with this action.

BUDGET REFERENCE

The table below identifies the fund and appropriation to fund privacy work through the remainder of 2020-2021, including the community engagement effort referenced in this memo.

Fund #	Appn. #	Appn. Name	Total Appn.	Amt. for Project	2020-2021 Proposed Operating Budget Page**	Last Budget Action (Date, Ord. No.)
001	0112	City Manager Non-Personal/Equipment	$2,557,535	$99,000	VII-51	6/23/2020 Ord. No. 30437

**The 2020-2021 Adopted Operating Budget was approved on June 16, 2020 and adopted by the City Council on June 23, 2020.

CEQA

Not a Project, File No. PP17-010, City Organization & Administrative Activities resulting in no changes to the physical environment.

/s/
ROB LLOYD
Chief Information Officer

For questions, please contact Andrew Ehrich, City Data Analytics Lead, at (818) 575-0010 or Marcelo Peredo, Chief Information Security Officer, at (408) 535-4821.

Attachment:
Digital Privacy Policy