COUNCIL AGENDA: 09/13/19
FILE: 19-793
ITEM: 3.6

CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR
AND CITY COUNCIL

FROM: Dolan Beckel

SUBJECT: APPROVAL OF CITYWIDE PRIVACY PRINCIPLES

DATE: September 4, 2019

Approved

Date 9/5/19

RECOMMENDATION

Adopt a resolution approving the City-wide Privacy Principles.

OUTCOME

The Privacy Principles are the first step in building a centralized Privacy Policy that safeguards the public's trust in the City's use of technologies that could identify and/or store personally identifiable information. The Privacy Principles will be the "northstar" that guides the development of San José's first ever detailed Privacy Policy.

BACKGROUND

In May 2018, the City engaged and received pro-bono guidance from the Harvard Cyberlaw Clinic (Harvard), part of the Berkman Klein Center for Internet & Society, to shape a strong approach to privacy in the City's adoption of new and 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. The Harvard team noted that the privacy landscape is changing and that no true standard has emerged for communities to follow.

(2) Use the Privacy Principles to develop a Privacy Policy for the City. The Harvard team noted that while few Cities in the United States have developed both privacy principles and privacy policy, there is a need for such policy to guide still-emerging uses of identifying technologies and data, as well as, due to inaction by the Federal Government.

Privacy Principles Background

The City applied Harvard's recommendation and established a three-pronged approach to create and vet its Privacy Principles. The following actions were taken to advance this work:

(1) **Creation of a Privacy Working Group**. The Privacy Working Group is comprised of senior, cross-departmental staff from the City organization, and receives and integrates input from public forums and the Privacy Advisory Taskforce.
(2) **Creation of a Privacy Advisory Taskforce**. The Privacy Advisory Taskforce meets quarterly with eight (8) members as subject-matter experts 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 of San José's Privacy Working Group used a combination of expert knowledge and public input to develop the Privacy Principles which are intended to guide City policies regarding how the City provides services through the collection, management, retention, and sharing of data. The City Manager's Office requests City Council consideration and approval of the City's Privacy Principles that express the core values the City will uphold to safeguard the public's trust as the City further develops privacy policy.

The accompanying report to this memo, "San José Digital Privacy Principles Summary of Community Engagement Findings" (Attachment A), provides details into a wide-range of community members' perspectives, needs, and concerns regarding privacy-specific local government operations and services. These insights helped inform and improve the City's Privacy Principles.

<u>The City of San José's Privacy Principles</u>

Upon conclusion of the community and expert input efforts, the following Privacy Principles were presented to, and approved by, the Smart Cities and Service Improvements Committee on June 6, 2019, and then referred by the Committee to the full City Council for approval.

The Privacy Principles are the following:

- **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.

ANALYSIS

Iterations of Privacy Principles

The City completed several iterations of the Privacy Principles since they were first developed by the Privacy Working Group. Each iteration was reflective of the changes and learnings gained from each community engagement and was subsequently considered and ultimately recommended by the Privacy Working Group.

The City contracted with CivicMakers, a community engagement consulting firm, to conduct the initial stakeholder interviews in English, Spanish, and Vietnamese. As mentioned above, these interviews laid the groundwork for identifying the correct constituencies for the public forums and gave the City clear direction on how best to comprise the Privacy Advisory Taskforce as summarized in the attached report, "San José Digital Privacy Principles Summary of Community Engagement Findings" (Attachment A).

At a high level, the three public forums showed that residents:

1. Generally agreed with the overall intent of the Privacy Principles and confirmed that the City is on the right path with clear values-driven Privacy Principles that safeguard the public's trust;

2. Sought more tangible examples of how the Privacy Principles are going to be implemented and showed an interest towards reviewing the final policy language; and

3. Encouraged the City to develop a strong method to ensure City and vendor compliance with the Privacy Principles.

The Privacy Advisory Taskforce provided subject matter expertise during the creation of the Privacy Principles. Feedback that was provided during the three initial Taskforce meetings that was included in the Privacy Principles include:

1. Acknowledge privacy as an inherent human right;
2. Focus the Privacy Principles on plain language;
3. Clearly provide information on data collection, distribution, and retention;
4. Thoroughly evaluate the privacy and security risk when collecting data; and
5. Provide timely notification of data breaches.

EVALUATION AND FOLLOW-UP

Moving from Privacy Principles to Privacy Policy and Implementation

The overall story for development, implementation, and elaboration of the City's Privacy Policy can be thought of in four phases:

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

The organizational approach taken for Phase 1 was successful in establishing the foundation needed to move into Phase 2 but was not sufficient to scale citywide reviews of technologies, nor develop the formal citywide Privacy Policy. To address this capacity issue, the Office of Civic Innovation partnered with the Office of Administration, Policy, and Intergovernmental Affairs, and the Information Technology Department as a joint City Manager's Office Team (CMO Team) to co-lead and manage the Privacy Policy Development (Phase 2).

The CMO Team is committed to reinforcing the role of the Privacy Advisory Taskforce, as well as the internal Privacy Working Group as policy development moves through Phase 2 and into Phase 3. Continuous process and policy improvements will be considered upon completion of the Privacy Policy. Evaluation throughout the implementation process will be critical as this policy area is dynamic and technology and public opinion on these issues is always evolving.

The CMO Team will finalize project scoping and resourcing as well as complete research and analysis by the end of October 2019. As staff transitions to developing solutions over the winter, the team will provide an information memo update to City Council by March 2020. Finally, an annual update to City Council is scheduled for June 2020 to assess our approach, deliverables, and set the path forward for a Citywide Privacy Policy.

PUBLIC OUTREACH

Privacy Public Engagement

The City has vetted the Privacy Principles through a series of community engagement efforts and feedback provided by subject matter experts serving on the Privacy Advisory Taskforce.

The City leveraged the expertise of CivicMakers, a community engagement consulting firm, which helped the City design and implement the City's community engagement strategy. CivicMakers helped the City drive participation, facilitate outreach, and compile engagement findings that were incorporated into the development of the Privacy Principles.

A timeline of engagement is shown below.

Privacy Advisory Taskforce #1
November 27, 2018 - The Taskforce provided feedback on the Privacy Working Group's first version of the Privacy Principles.

Public Forum #1
December 4, 2018 - Participants included local leaders and representatives from community-serving nonprofits, small businesses, local industry, elected officials, and neighborhood associations. This forum was conducted in English.

Smart Cities and Service Improvement (SCSI) Committee Update
December 6, 2018 - The SCSI Committee reviewed the second revision of the City's Privacy Principles. The Committee accepted the update and provided feedback on the second revision of the Privacy Principles.

Stakeholder Interviews
February - March 2019 - Participants included community-facing staff at local community organizations focused on serving low-income, immigrant groups, including Spanish-speakers, Vietnamese-speakers, Chinese-speakers, and others.

Privacy Advisory Taskforce #2
February 14, 2019 - The Taskforce provided feedback on the Privacy Working Group's third version of the Privacy Principles.

Privacy Advisory Taskforce #3
April 10, 2019 - The Taskforce provided feedback on the Privacy Working Group's fourth version of the Privacy Principles.

Public Forum #2
April 24, 2019 - The forum was conducted in Spanish. Participants included predominantly female Spanish-speakers.

Public Forum #3
April 24, 2019 - The forum was conducted in Vietnamese. Participants from the Vietnamese-speakers was very broad and ranged from ages 30 to over 65.

Smart Cities and Service Improvement Committee Update
June 6, 2019 - The City's SCSI Committee reviewed and referred the fifth revision of the City's Privacy Principles to City Council for consideration and adoption.

COORDINATION

This memo was coordinated internally with members of the Privacy Working Group including the City Manager's Office, the City Attorney's Office, the Office of the Mayor, the Library Department, the Information Technology Department, and the Police Department.

COMMISSION RECOMMENDATION/INPUT

There is no commission recommendation or input associated with this action.

FISCAL/POLICY ALIGNMENT

This recommendation aligns with the City's Broadband and Digital Inclusion strategy approved by the City Council in November of 2017.

CEQA

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

/s/
DOLAN BECKEL
Director, Office of Civic Innovation

For questions, please contact J. Guevara, Broadband Manager, Office of Civic Innovation, at (408) 535-8123 or Sarah Zárate, Assistant to City Manager, Office of Administration, Policy, and Intergovernmental Affairs, at (408) 535-5601.

Attachments:
A. San José Digital Privacy Principles Summary of Community Engagement Findings

City of San José Digital Privacy Principles

Summary of Community Engagement Findings

June 2, 2019

Concerned about your digital privacy?
Learn More
bit.ly/SJprivacy
*****
Share Now!
CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Table of Contents

Executive Summary

Our Approach

Engagement Findings

- Community Workshop Summary (Dec 4, 2018)
- Stakeholder Interviews Summary (Feb - March 2019)
- Spanish-Language Focus Group Summary (April 24, 2019)
- Vietnamese-Language Focus Group Summary (April 24, 2019)
- Focus Groups: Combined Summary (April 2019)
- Privacy Advisory Taskforce
  - Taskforce Meeting #1 (November 27, 2018)
  - Taskforce Meeting #2 (February 14, 2019)
  - Taskforce Meeting #3 (April 10, 2019)

Appendix

- Information shared at Community Workshop
- Information shared ahead of Stakeholder Interviews
- Information shared at Focus Groups

Executive Summary

The City of San José's Digital Privacy Working Group has developed a set of digital privacy principles to guide City policies regarding digital data across all City services and city-serving vendors, including how data is collected and managed within the City, and how and with whom it is retained and shared outside of the City.

To understand public awareness of digital privacy issues and ensure that the privacy concerns of San José's diverse community are considered in the development of the digital privacy principles, the City's Privacy Working Group, in consultation with CivicMakers, gathered community input via a series of stakeholder interviews, three public forums including two in-language focus groups (one in Spanish (ES) and one in Vietnamese (VI)), and through subject matter experts which serve on a Privacy Advisory Taskforce .

The following report provides insights regarding San José community members' perspectives, needs and concerns regarding digital privacy in the context of the City government and the services it provides.

The following table summarizes key takeaways from the community engagement effort. The table is organized by topic and corresponding community input. The input is organized by engagement event because the participants at each event represented different segments of the community. The participants at each event were as follows:

- **Community Workshop -** Participants included local leaders and representatives from community-serving nonprofits, small businesses, local industry, elected officials, and neighborhood associations.
- **Stakeholder Interviews -** Participants included community-facing staff at local community organizations focused on serving low-income immigrant groups, including Spanish-speakers, Vietnamese-speakers, Chinese-speakers, and others.
- **Focus Groups -** Participants were low-income female Spanish-speakers (mostly mothers of young children) and Vietnamese-speakers ranging in age from middle age to elderly.
- **Privacy Advisory Taskforce -** The Taskforce is comprised of subject matter experts external to the City that provide input to the City regarding the development of the City's Digital Privacy Principles. The Taskforce is represented by eight subject matter experts from non-profit organizations, technology industry representatives, academia, law enforcement, and other government leaders beyond the City of San José.

Table 1. Key Takeaways

Topic	Community Input
General Attitudes & Awareness of Privacy	**Community Workshop:** ● General awareness that digital privacy is important

	● Unclear on the details of how and how much data is collected and shared ● Some confusion about definitions of “privacy” vs. “digital privacy” (especially in the public realm) ● Many take actions they believe will protect their privacy, but these actions may not actually protect them ● Want both convenience and security ● General trust of the City, especially versus Federal Government ● Many amenable to video collection; but have big concerns about protecting immigration status **Stakeholder Interviews**: *observations of the population groups with whom they work* ● Generally unaware of digital privacy ● Most wary of providing personal info in general ● Some are willing to sign up for digital services that are seen as high need; otherwise wary of or uninterested in digital services ● General hesitance to sign up for government services
Overall Privacy Concerns	**Community Workshop**: ● **Sharing.** ○ Highest concerns related to sharing personal contact info, financial info & device identification ○ Most concerned about how data would be used, specifically for: monetization, profiling, marketing ○ Major concerns for immigrant community over data collection, storage and usage ○ Seniors also very concerned about protecting personal data ● **Storage.** Many wondered how long data/footage is stored, as well as who has access to data & associated security protocols--not just departments but individuals **Stakeholder Interviews:** *observations of the population groups with whom they work* ● **Sharing**. ○ Generally concerned about having to provide proof of identification to access government (or any) services ○ Most are concerned about who their data will be shared with and how it will be used ○ Many concerned about the potential to receive spam/marketing ● **Trust.** General suspicion of unidentifiable phone calls. ○ Concern that the other person will only speak English ○ Concern that it could be a government official ○ Concern that it could be a part of a phone scam

Needs & Suggestions	**Community Workshop:** ● Most want to know how data will be used and by whom ● Asked for help interpreting the Terms of Service agreement (ToS) and what data is being collected, shared, stored, etc. ● Request for an option to use a service without a personal account (anonymously) ● Interest in going through a pre-existing, trusted account (ex: library card) ● Would like to have more control over what data they share and what data the City already has ● Providing the Principles "cold" was not helpful - caused confusion for some and colored feedback of others ● Many see these as trusted sources: personal hotspots, Xfinity, hospitals, city, local businesses **Stakeholder Interviews:** *observations of the population groups with whom they work* ● Many are more likely to trust the City government if the message or request is relayed through a trusted community organization ● Most are likely to trust face-to-face interactions with frontline City employees who are culturally sensitive and can confirm the validity of the City's policies (specifically meaningful when providing assurance that the City will not share their personal information with other entities) ● Informational tools that community members are typically comfortable with / trusting of: Facebook, email and phone/SMS from known contacts
Principle #1 WE VALUE PRIVACY The City of San José affirms that privacy is an inherent human right. We commit to fully evaluating risks to your privacy before collecting, using, or sharing your information.	**Focus Groups:** ● Concerns about "fully evaluating risks to your privacy before collecting, using, or sharing your information." What is the evaluation procedure? Who will conduct the evaluation? ○ Want to make sure the evaluation is clear and transparent ● After collecting the information, how does the City use and share this information? ● City should frequently check and audit all departments and facilities that collect the information ● Only necessary information should be collected ● The resident should have a right to refuse providing information ● How will the City guarantee that collected information will not be compromised?
Principal #2	**Focus Groups:**

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.	● The City should encourage (enforce) other external agencies and facilities to apply these principles ● If there is any violation of these principles, how will the City solve the problem and compensate the victims? ● Regarding “comply with the law” - what does that mean? Are these the rules in San José? Or the rules according to ICE? Needs clarification
Principal #3 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.	● No comments regarding this principle
Principal #4 WE GIVE YOU CONTROL OVER YOUR DATA We will provide you with the information to make an informed decision about sharing your data, wherever possible. We have clear processes that ensure data accuracy and provide you visibility into what data the City has collected from you.	**Focus Groups**: ● If the residents refuse to provide their personal information, will they still be able to access services from the City? ○ If residents cannot access services because they refuse to provide the personal information, are there any other alternatives for residents to access these services? ● City should clearly explain why they collect the information. The principles should be available at the front desk in their own language, and staff should be able to provide explanation when the residents ask questions about the principles. ● In the case of electronic forms, when residents do not want to fill in the required information (*), normally the computer will not allow them to progress. How can residents skip these required questions? City should design the option to skip in the electric form (or consider what fields are required) ● What does “whenever possible” mean? Does this guarantee my privacy? ● Regarding “give you control of your information.” Will you be giving others my information without informing me? How can I see what information you have on me?
Principal #5 WE SHARE ONLY WHAT WE NEED We anonymize your information before we share it outside the City,	**Focus Groups**: ● What are the “limited circumstances?” Please specify ● When the information is shared, the City must let the residents know and explain why they share it ○ The residents have to be informed that the information is shared and with whom

except in very limited circumstances. We require our vendors and partners to adhere to these principles.	● Principle #4 and #5 are conflicted. In principle #4, the residents have the right to control their information, but in the principle #5, the City has the right to share residents' information ○ Make sure that the City must ask the residents' permission and authorization before they share the information ● Provide examples to help people understand the principles
Principal #6 WE DESIGN AND BUILD FOR PRIVACY AND SECURITY We integrate privacy and security into every aspect of 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.	**Focus Groups**: ● What are the strict protocols that address when the information is compromised? Please specify ○ When the information is compromised, the City must inform the residents. They need to know how the City can stop it, and who is responsible ● What is the technology that is being modernized? ● Regarding "when it is under our control:" What happens when it's passed to others? Will the information still adhere to the privacy principles? Clarification needed.

Our Approach

The City partnered with CivicMakers, a civic innovation and engagement firm, to develop a strategy to gather community input to inform the City's digital privacy principles. The goal was to gain candid feedback from community members regarding their perceptions, needs and concerns around digital privacy. The community engagement strategy set forth a two-pronged approach designed to:

1. Reach a broad and representative audience via a **community workshop** and widely-distributed **survey** (note: the survey has not yet been released)
2. Reach diverse groups who are often left out of traditional engagement efforts (particularly those who are more vulnerable with regards to their digital privacy needs, such as immigrant groups and low-income residents) via targeted **stakeholder conversations** and **focus groups** with Spanish speakers and Vietnamese speakers.

Another key component of our approach was to ask a representative group of community members (via stakeholder interviews) how they (and others in their network) would prefer to be engaged on this topic. To the extent feasible within budget and time constraints, we integrated the following community recommendations into our approach:

- Provide incentives for feedback
- Pay local community organizations trained in outreach to reach diverse groups
- Provide a foundation in digital privacy before engaging people in these discussions
- Target the younger generation to get the participation of their parents and grandparents
- Assess what the community considers as the government, and which government groups they trust
    - Potential to lessen concerns about government with an official assurance endorsed by a community group
    - Suggest that more frontline employees that are culturally sensitive and can confirm the validity of the City's policy to not share information with other government entities
- Use outreach tools that users are typically comfortable with: Facebook, email, SMS
- Include an option to provide feedback on paper, and/or with one-on-one support for online surveys

Outreach & Engagements

Between December 2018 and May 2019, the City reached out to and engaged community members in the following ways:

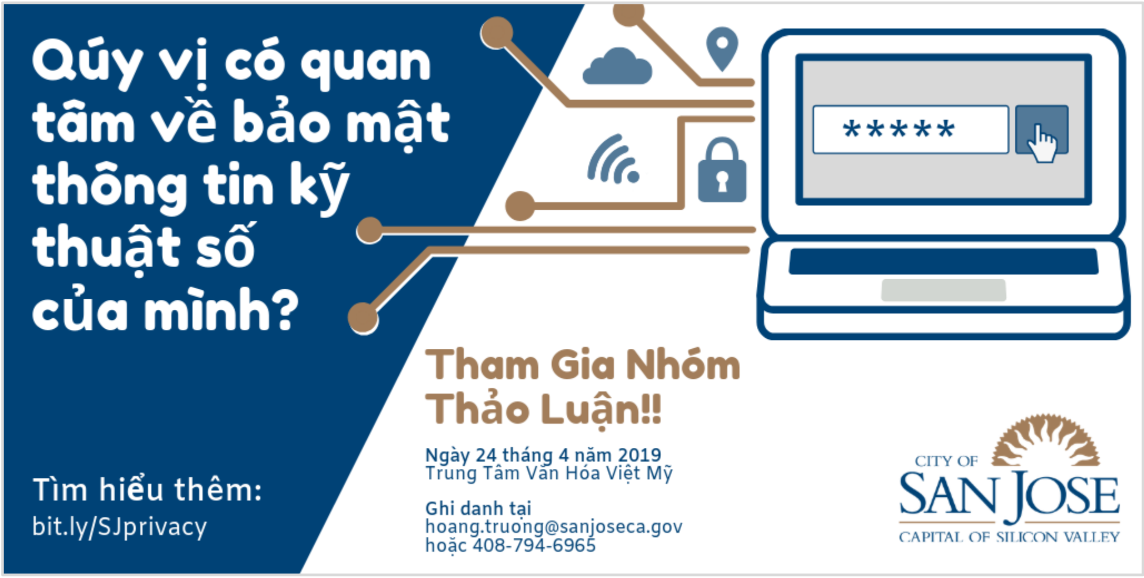
- **Informational Webpage** - The City maintains an informational webpage on the City's website with details about the Digital Privacy initiative. The webpage can be accessed at http://sanjoseca.gov/digitalprivacy
- **Community Workshop (English) -** The City hosted a Digital Privacy Engagement Workshop on December 4, 2018 to gather initial input from community members.

- Outreach. The project team conducted extensive research to compile a stakeholder list intended to represent a large swath of the San José public. Staff sent personal invitations to this list.
- Participants. 19 participants from these diverse groups:
    - San José Silicon Valley Branch of the National Association for the Advancement of Colored People (NAACP) (2)
    - Silicon Valley Council of Nonprofits
    - Services, Immigrant Rights & Education Network (SIREN)
    - Catholic Charities of Santa Clara
    - Evergreen Business Association
    - Friends of Levitt Pavilion San José
    - Cisco
    - Somos Mayfair
    - Neighborhood associations (3)
    - Offices of elected officials (2)
- Structure. Split into small groups and rotated through the discussion of 3 digital privacy scenarios:
    - Privacy and Free Wi-Fi Internet Access
    - Privacy and Online Accounts
    - Privacy and Public Spaces
- Data Collection.
    - Each person completed a worksheet with questions corresponding to each scenario
    - Groups discussed each scenario in facilitated conversation
    - Debrief conversation with full group over lunch
    - At the end of the workshop, participants filled out an evaluation form to give overall feedback on the engagement session and share additional input regarding their thoughts about privacy in general

- **Stakeholder Interviews -** In January and February 2019, the City's consultant, CivicMakers, conducted stakeholder interviews to understand privacy needs and concerns of diverse groups.
    - Outreach. Compiled a stakeholder list of community organizations, community leaders, academics, and others representative of the diversity of San José and groups who might have unique digital privacy needs.
    - Participants. Spoke with four different community members and leaders who either represent or work directly with key stakeholder groups (immigrants; Spanish-, Chinese-, and Vietnamese-speakers; low-income populations):
        - Hoang Truong, *Vietnamese American Cultural Center (VACC)*
        - Jeremy Barousse, *Services, Immigrant Rights and Education Network (SIREN)*
        - Saul Ramos, *SOMOS Mayfair*
        - Karmann Hung, *Asian Americans for Community Involvement (AACI)*

  - ○ Structure. ~ 45-minute phone conversations.
  - ○ Data Collection**.** Took detailed notes during conversations.

- **Focus Groups (Spanish & Vietnamese) -** The City hosted two focus groups (one in Spanish and one in Vietnamese) in April 2019 to understand the perspectives of these groups with regard to digital privacy and the City. Both meetings were facilitated in-language - led by City of San José staff members - and held at local community organizations[1]. Food and childcare were provided for the Spanish language session. Food was provided for the Vietnamese session. Participants were entered in a raffle to win a family pass to Happy Hollow Zoo, which was provided to the winner at the end of each meeting.
  - ○ Outreach.
    - ■ ES: Partnered with META[2] to conduct outreach to the Spanish-speaking community in East San José. META conducted outreach in person by spreading the word verbally at popular community locations and events.
    - ■ VI: Partnered with the Vietnamese-American Cultural Center (VACC) to conduct outreach to Vietnamese speakers who frequent the center. The VACC spread the word verbally by making announcements at scheduled onsite programs and via social media.


Qúy vị có quan tâm về bảo mật thông tin kỹ thuật số của mình?
*****
Tham Gia Nhóm Thảo Luận!!
Tìm hiểu thêm:
bit.ly/SJprivacy
CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Ngày 24 tháng 4 năm 2019
Trung Tâm Văn Hóa Việt Mỹ

Ghi danh tại
hoang.truong@sanjoseca.gov
hoặc 408-794-6965

[Social Media Graphic in Vietnamese]

  - ○ Participants. The focus groups included the following participants:
    - ■ ES: 14 Spanish-speaking community members (all women and mostly mothers of small children) from the Mayfair/East San José area.

[1] Somos Mayfair and Vietnamese-Amerian Cultural Center, respectively

[2] “Mujeres Empresarias Tomando Acción” (“Entrepreneurial Women Taking Action”)

        - VI: 20 Vietnamese-speaking community members ranging in age from middle age to retirement age.

    - Structure. Each focus group lasted two hours and followed this agenda:
        - Introductions and overview of meeting objective and agenda
        - Overview of the project, definition of digital privacy, and examples of how the City uses data
        - Presentation of privacy principles and discussion about each principle based on the following prompts:
            - Do these principles reflect your needs and concerns?
            - If not, what's missing?
            - Is there anything that is unclear or needs further explanation?

Engagement Findings

Community Workshop Summary (Dec 4, 2018)

[*Photo: Community Workshop at Dr. Martin Luther King, Jr. Library; Dec 4, 2018*]

General Attitudes & Awareness of Privacy

- General awareness that information is collected; uncertain what is collected; assumptions that more is collected than necessary, sometimes much more (i.e., "everything").
- Generally don't read Terms of Service agreements.
- Most make decisions based on how they think they can protect their personal info online.

- Balance between convenience and security: learning what info is collected/shared significantly decreased willingness to sign-up/create account; learning benefits of creating accounts moderately increased willingness to create one.
- Trust is critical; trust in government varies widely between community groups; greater trust for the City than other jurisdictions (Federal was the least desirable/trusted); more accepting of private entities collecting information, but when City does there is more concern.
- Generally positive take on video collection, aside from concern when immigration status may be questioned/impacted; some, but not all considered surveillance implications of video footage.

Overall Privacy Concerns

- Particular concerns related to personal contact info and contacts, financial information and device identification.
- Most expressed concerns about how data would be used, specifically for: monetization, profiling, marketing, legal implications.
- Many wondered how long footage data is stored, as well as who has access to data and associated security protocols--not just departments but individuals.
- Major concerns for immigrant community over data collection, storage and usage, including data sharing; seniors also very concerned about sharing personal info.
- Some general confusion about the distinction between "privacy" and "digital privacy" especially in public space.

Needs & Suggestions

- Want to know how data will be used and by whom.
- Asked for help interpreting ToS and what data is being collected, shared, etc.
- Provide an alternative to use the service without a personal account.
- Interest in going through a pre-existing, trusted account (ex: library card).
- Would like to have more control over what data they share and what data has already been collected.
- Providing the principles "cold" was not helpful - caused confusion for some and colored feedback of others.
- Trusted sources mentioned: personal hotspots, Xfinity, hospitals, city, local businesses.

What did you learn that surprised you?

- "My own comfort with allowing access vs. ease, convenience, benefit."
- "The great work the City is doing with community engagement and strengthening data privacy."
- "It surprised me that you were even doing this study. I think it is important and I want to thank you."
- "Immigrant community concerns - hadn't considered that previously."
- "Different interests in the matter among vulnerable communities (seniors v. immigrants)."

What do you want to learn more about?

- "What data does the city 'need to know?'"
- "How to open accounts without sharing private info."
- "What are limitations for public agencies and private companies to invade people's privacy?"
- "City approach to privacy."

- “City’s data control process.”
  “What is the city doing to go deeper in community engagement and strengthen digital privacy?”

Stakeholder Interviews Summary (Feb - March 2019)

Observations of the population groups with whom they work. ES denotes Spanish; VI denotes Vietnamese.

General Attitudes & Awareness of Privacy

- Generally unaware of digital privacy and its consequences.
- Willingness to sign up for services that are seen as high need/urgency, but otherwise wary of or uninterested in digital services.
  - Youth are generally more concerned, and act as a bridge for their older relations to engage.
  - Signing up for services doesn’t necessarily equate to trust around sharing personal information.
  - (VI) In particular, when asked to share personal information, likely to submit incomplete forms or provide false information.
- (ES) Generally consider sharing information on the screen as something new and suspicious.

Overall Privacy Concerns

- Major concerns about having to provide proof of identification.
- General suspicion around phone calls.
  - Concern for whether the other person will only speak English.
  - (ES) Concern that it could be a government official.
  - (ES) Concern that it could be a part of phone scams that have been targeting members of the community.
- Many consider the potential to receive spam/marketing.
- (ES) Concern seems to be less about providing their information, and more about who it could be shared with. Hesitance to sign up for government services.

Suggestions for Community Engagement

- Provide incentives for feedback.
- Suggest requesting feedback on paper forms, and/or with one-on-one support.
- Provide a foundation in digital privacy before engaging people in these discussions.
- (VI) Suggest targeting the younger generation to get the participation of their parents and grandparents.
- (ES) Assess what the community considers to be “the government”, and which government groups they trust.
  - Potential to lessen concerns about government with an official assurance by a trusted community organization.
  - Frontline employees who are culturally sensitive will be more trusted in confirming the validity of the City’s policy to not share personal information with other government entities.

- (ES) Outreach tools that community members are typically comfortable with: Facebook, email, phone.

Spanish-Language Focus Group Summary (April 24, 2019)

[*Photo: Spanish-language Focus Group at Somos Mayfair; April 24, 2019*]

General Response

- Participants did not necessarily understand the differences in programs/services provided by the City versus County, State, and/or Federal government. They repeatedly asked for examples.
- Participants keyed in on the situational or caveat language written into the principles. They wanted additional clarification and/or examples in several principles. (These instances are reflected in Table 2, below).
- There is a very pervading fear of the Federal government and how different agencies can access the participants' information. Clarification of City services will help with this as well as addressing in writing their concerns about sharing information with USCIS/ICE.
- Some participants were aware of ways online services allow them to review what information the company has on them and were looking for a similar way to see all the information they've shared (with the City) and opt out.

Sharing Personal Information

- When are you asked for your personal information?
    - Medi-Cal
    - Insurance
    - Getting a cell phone
    - Loans
    - Women, Infants and Children (WIC)
    - Taxes

- What information are you comfortable sharing?
  - Name
  - Telephone number
  - Address

- What information are you NOT comfortable sharing?
  - NOT social security number
  - DO NOT share any information about people who are looking for housing vouchers or low income housing

Additional Discussion

- Are there protections in place now, or not?
- What are the consequences if someone doesn't follow these principles?
- Before you do this next time, it's important that you give the participants a document that lists the departments and/or services of the City
- If we don't share our information it can also impact us because then the City is only capturing the information of citizens
- The information the police department asks for just to let me in the building puts me at risk
  - They should stop asking for a driver's license or ID
  - They don't need to know that many details
- Who are the City's vendors? This needs a better definition

Vietnamese-Language Focus Group Summary (April 24, 2019)

[*Photo: Vietnamese-language Focus Group at Vietnamese-American Cultural Center, April 24, 2019*]

General Response

- The principles should be provided in both languages.
- There are some professional terminologies in the principles translation. Overall, the participants understand and agree with these principles.

- One participant responds that the principles are well crafted and obvious.
- The participant concerns that these principles are for Digital Privacy, so how about non-Digital Privacy? Does the City have other principles or the same principles for that issue?

Sharing Personal Information

- When are you asked for personal information?
  - Asked for SSN at Social Service Agency
  - Asked for Medical/Medicare information when applying for free phone
  - Asked for personal information when applying to school or volunteering
- What information are you comfortable sharing?
  - Name
  - Telephone number
  - Address
  - Email address
- What information are you NOT comfortable sharing?
  - NOT willing to provide SSN and credit card information
- They need to know exactly whether the staff who collects the information are from the City of San José. Even for the staff that are wearing badges, some participants are afraid they could be fake badges.

Additional Discussion

- Participants want to be provided staff's information (name, title, department, contact information) and the receipt when they collect the information.
- Participants feel comfortable when they are recorded by the security camera at City facilities and non-City facilities.
- Participants discussed more about when they are recorded by a personal camera. If a person records a group of people in a public area, it should be fine, but if that person records only the individuals, s/he should get their permission.
- Participants agree that after getting the permission from residents, the City has the right to analyze, store, or delete that information.
- Participants recommend that after collecting the information from the resident, the City should verify the information to ensure it is true and correct.

Table 2. Combined Feedback on DRAFT Privacy Principles

Principles	Focus Group Feedback (ES + VI)

Principle #1 WE VALUE PRIVACY The City of San José affirms that privacy is an inherent human right. We commit to fully evaluating risks to your privacy before collecting, using, or sharing your information.	● Participant concerns about 'fully evaluating risks to your privacy before collecting, using, or sharing your information.' What is the evaluation procedure? Who will conduct the evaluation? ○ Want to make sure the evaluation is clear and transparent ● After collecting the information, how does the City use and share this information? ● City needs to frequently check and audit all departments and facilities that collect the information. ● Only necessary information should be collected. ● The resident should have a right to refuse providing information. ● How to guarantee information will not be compromised?
Principal #2 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.	● City should encourage (enforce) other external agencies and facilities to apply these principles. ● If there is any violation of these principles, how will the City solve the problem and compensate the victims? ● Regarding "comply with the law" - what does that mean? Are these the rules in San José? Or the rules according to ICE? Needs clarification.
Principal #3 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.	● No comments regarding this principle
Principal #4 WE GIVE YOU CONTROL OVER YOUR DATA We will provide you with the information to make an informed decision about sharing your data, wherever possible. We have clear processes that ensure data accuracy and provide you visibility into what data the City has collected from you.	● If the residents refuse to provide their personal information will they still be able to access services from the City? ○ If residents cannot access services because they refuse to provide the personal information, are there any other alternatives for residents to access these services? ● City should clearly explain why they collect the information. The participant means the principles should be available at the front desk in their own language, and staff are able to provide explanation when the residents ask questions about the principles. ● In the case of electronic forms, when residents do not want to fill in the required information (*), normally the computer will not allow them to progress. How can residents skip these required questions? City should design the option to skip in the electric form (or consider what is required).

	● What does “whenever possible” mean? Just saying so doesn’t guarantee my privacy. ● Regarding “give you control of your information:” Will you be giving others my information without informing me? How can I see what information you have on me?
Principal #5 WE SHARE ONLY WHAT WE NEED We anonymize your information before we share it outside the City, except in very limited circumstances. We require our vendors and partners to adhere to these principles.	● What are the ‘limited circumstances?’ Please specify. ● When the information is shared, the City must let the residents know and explain why they share it. ○ The residents have to be informed that the information is shared and with whom. ● Principle #4 and #5 are conflicted. In principle #4, the residents have the right to control their information, but in the principle #5, the City has the right to share residents’ information. ○ The participant wants to make sure that the City must ask the residents’ permission and authorization before they share the information ● Provide examples to help people understand the principles
Principal #6 WE DESIGN AND BUILD FOR PRIVACY AND SECURITY We integrate privacy and security into every aspect of 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.	● What are the strict protocols that address when the information is compromised? Please specify. ○ When the information is compromised, the City must inform the residents. They need to know how the City can stop it, and who is responsible. ● What is the technology that is being modernized? ● Regarding “when it is under our control:” What happens when it’s passed to others? Will the information still adhere to the privacy principles? Clarification needed.

Privacy Advisory Taskforce

San José Privacy Advisory Taskforce Meeting #1

Tuesday, November 27, 11:30 to 1:00pm
San José City Hall, City Manager’s Conference Room, 17th Floor

Meeting Participants:

1. Victor Sin, Chair of the Santa Clara Valley Chapter, ACLU of Northern California Roxana Marachi, San José Silicon Valley NAACP
2. Michelle Finneran Dennedy, Chief Privacy Officer, Cisco & Adjunct Faculty, Carnegie Mellon University
3. Don Heider, Executive Director, Internet Ethics, Markkula Center for Applied Ethics, Santa Clara University
4. Bob Lim, Vice President Information Technology & Chief Information Officer, San José State University
5. Mike Shapiro, Chief Privacy Officer, Santa Clara County

6. James Randol, Retired San José Police Department Captain
7. Dolan Beckel, Director, Office of Innovation, Office of the City Manager, City of San José
8. Rob Lloyd, Chief Information Officer, City of San José
9. Marcelo Peredo- Chief Information Security Officer, City of San José
10. Liam Crawford, Broadband and Privacy Policy Analyst, Office of the City Manager, City of San José.
11. Lawrence Grodeska, Chief Executive Officer and Co-Founder of CivicMakers
12. Judi Brown, Chief Impact Office and Co-Founder of CivicMakers

Summary:

1. Dolan Beckel, Director of Innovation and Digital Strategy, CMO, provided opening remarks. All meeting attendees provided introductions and reason for their interest in serving as Taskforce member.

2. Taskforce Introductions –Judi Brown with CivicMakers opened with an icebreaker asking "when was the last time you personally read a Terms of Service (ToS) agreement. Seven of the current eight serving Taskforce member representatives were present.

3. Overview of Process – Lawrence Grodeska, Civic Makers, provided an overview of their engagement as the City's privacy engagement consultant. Liam Crawford, Broadband and Privacy Policy Analyst, CMO, provided an overview of the presentation provided to City Council's Smart Cities and Service Improvement Committee on December 6, 2018.

4. Review of Privacy Principles –
   a. The Taskforce was asked how the City's current iteration of draft privacy principles balance the 3 dimensions of cybersecurity as defined by the public's right to privacy, and the City's ability to use data to improve City service. The feedback was received through an activity of plotting each draft principle to identify how they relate to one another.
   b. Taskforce members reviewed draft privacy principles requesting that further time be provided at the next meeting to both review and discuss the principles at length.
   c. The Taskforce agreed that they will provide consensus recommendations to the City's Privacy Working Group at the next Taskforce meeting in January. The recommendations will strengthen and amend the principles.
   d. The high-level initial requests were the inclusion of language on accountability, enforcement of the principles,

5. Privacy and the Public – CivicMakers, Lawrence Grodeska & Judi Brown
   a. The Taskforce provided additional suggestions of organizations to participate in the initial Privacy Workshop on December 4, 2018.

6. Close & Next Steps
   a. Liam Crawford, CMO closed the meeting noting the upcoming Committee presentation to Council's Smart Cities and Service Improvement Committee, the upcoming Community Engagement Workshop, and that the Taskforce meeting date in January will be set before the end of the year.

Privacy Advisory Taskforce Meeting #2

Thursday, February 14, 2019, 2:00-3:30pm
San José City Hall, Floor 16 Room T-1654

Meeting Participants

1. Victor Sin, Chair of the Santa Clara Valley Chapter, ACLU of Northern California
2. Roxana Marachi, San José Silicon Valley NAACP
3. Heather Patterson, Senior Research Scientist, Intel Labs & Privacy Scholar at NYU
4. Michelle Finneran Dennedy, Chief Privacy Officer, Cisco & Adjunct Faculty, Carnegie Mellon University
5. Irina Raicu, Director, Internet Ethics, Markkula Center for Applied Ethics, Santa Clara University
6. Mike Shapiro, Chief Privacy Officer, Santa Clara County
7. Rob Lloyd, Chief Information Officer, City of San José
8. Liam Crawford, Privacy and Broadband Analyst, Office of the City Manager, City of San José

Overview and Summary:

1. The Taskforce received an update on the City's privacy community Engagement feedback thus far and strategy through May 2019. Liam Crawford with the City provided an update upcoming City-wide privacy survey facilitated by the City's Privacy consultant CivicMakers. The City and CivicMakers plans to translate the survey into both Vietnamese and Spanish and hold subsequent privacy focus groups guided by the feedback received from the survey.

    a. Mike Shapiro, Chief Privacy Officer, provided best practices and considerations for establishing privacy resources and staffing from lessons learned in establishing the County's Chief Privacy Officer position and broader privacy infrastructure.
    b. Rob Lloyd, San José CIO, mentioned that the City wants to take a deliberate and strategic approach to establishing governance and accountability. Some examples include the City updating its internal procurement "checklist". The City also had made considerable efforts thus far through partnerships to consider privacy concerns, but is particularly interested in formalizing a governance structure that could potential enable new technologies and services without encroaching on privacy concerns.
    c. Taskforce members noted that the City should be more proactive in telling its story around privacy and the consideration that it has taken thus far and how it has partnered with third party vendors and companies address privacy concerns.
    d. Taskforce members raised the potential of the City to consider "differential privacy" as a potential alternative to anonymity and possibly a more realistic approach for structuring data to individual's privacy impact on individual information within a given database.
    e. Members of the Taskforce recommended that any potential new staff with privacy governance responsibility be full time city-funded positions.

2. Taskforce members provided additional verbal redlines edits and committed to provided more specific redline edits following the meeting. The Taskforce members provide initial input on distribution and drafting of survey questions. The City is going to send share a draft version of the survey to get feedback from the Taskforce before finalizing and requests advice for survey circulation and potential best practices.
    a. Taskforce members were asked to provide feedback to the privacy principles v1.2 following the meeting with redline requests with justification for changes.
    b. The City must consider the capability and implementation of "real choice", revising data architecture, algorithmic transparency, and alignment with industry standards, such as IEEE P7000.

3. Taskforce members provided feedback on governance structure and areas of potential partnership with other jurisdictions also focusing on enterprise privacy policy.

a. Members of the taskforce were invited to participate in UC Berkeley and Oakland's
b. surveillance technology information questionnaire and tracking tool.
c. The City continues to work with Mike Shapiro and opportunities to further collaborate with the County of Santa Clara, particularly around best practices and lessons learned on leading their Privacy Resolution and Information Protection Principles.
a. The City of Seattle has recently published the second set of draft of Surveillance
d. Impact Reports (SIRs) for eight of the 29 currently existing surveillance technologies, and is seeking public comment.
a. Heather Patterson, Intel, to connect San José with the folks in the City of Portland

4. Discussion of next steps.
   a. Taskforce members to provide detailed redline edits on draft privacy principles v1.2
   b. Privacy Survey review and feedback once the City has a final draft of survey questions. Next Privacy Advisory Taskforce Meeting Wednesday, April 10, 2019
   c. Privacy update to the Smart Cities and Service Improvement Committee on May 2nd, 2019

Privacy Advisory Taskforce Meeting #3

Thursday, April 10, 2019, 2:00-4:00pm
San José City Hall, 17th Floor Room 1753

Meeting Participants

1. Victor Sin, Chair of the Santa Clara Valley Chapter, ACLU of Northern California
2. Roxana Marachi, San José Silicon Valley NAACP
3. Heather Patterson, Senior Research Scientist, Intel Labs & Privacy Scholar at NYU
4. Bob Lim, Vice President Information Technology & Chief Information Officer, San José State University
5. Irina Raicu, Director, Internet Ethics, Markkula Center for Applied Ethics, Santa Clara University
6. Kip Harkness, Deputy City Manager, Office of the City Manager
7. Liam Crawford, Broadband and Privacy Analyst, Office of the City Manager
8. Albert Gehami, Information Technology Department

Summary and Overview

1. Update on Digital Privacy Strategy and Timeline
   a. Background and Overview of Digital Privacy Strategy and Timeline: Liam Crawford, Office of the City Manager provided an update to the Taskforce on the overall strategy.
   b. Public Engagement: The Taskforce provided feed on the City's public engagement related to the Privacy Principles. The City will be holding a second and third focus group, which will be held in Spanish and Vietnamese respectfully. The City also plans to share the Privacy Principles in English, Spanish, and Vietnamese through a privacy feedback form.
   c. Privacy Use Case Development: The City's Privacy Working Group continues to draft privacy use cases.
   d. Members of the Privacy Working Group will provide a privacy update to the Smart Cities and Service Improvement Committee on July 6, 2019

2. Feedback on Upcoming Community Engagement
   a. The Taskforce recommended that the City establish a clear methodology for the two upcoming focus groups and the public feedback form.

b. Bob Lim, San José State CIO, offered SJSU expertise to help further flesh out the methodology for the public feedback form.
c. Included in the methodology should be a clear

3. City Privacy Resources and Governance Structure Recommendations
   a. Request for Taskforce recommendations on privacy resources and governance

4. Review and Discuss v1.4 of the Privacy Principles
   a. Taskforce members spent the latter half of the meeting reviewing v1.4 of the Privacy Principles.
   b. The City provided context for the changes that were adopted per the Taskforce requests and explained why edits were incorporated.
   c. The Taskforce came to agreement on making several additional changes to the Privacy Principles.