Draft Minutes
COIT Privacy and Surveillance Advisory Board Meeting
City and County of San Francisco

Thursday, March 23, 2023
1:30 PM – 03:30 PM
City Hall Room 305 and Webex Online Event

Members
Mike Makstman – Chair, Chief Information Security Officer, Department of Technology
Guy Clarke – IT Governance Director, San Francisco International Airport
Mikela Clemmons – Technical Director, Digital Services
Mark de la Rosa – Director of Audits, City Service Auditor, Controller's Office
Jillian Johnson – Chair, Director, Committee on Information Technology
Michelle Littlefield – Chief Data Officer, Data SF and Digital Services
Molly Peterson – Contract Reform Manager, Office of the City Administrator

1. Call to Order by Chair

Mike Makstman called the meeting to order at 1:31 PM, provided instruction on how to give public comment, and conducted the roll call.

2. Roll call

Mike Makstman – Chair, Chief Information Security Officer, Department of Technology
Guy Clarke – IT Governance Director, San Francisco International Airport
Mikela Clemmons – Technical Director, Digital Services
Mark de la Rosa – Director of Audits, City Service Auditor, Controller's Office
Jillian Johnson – Chair, Director, Committee on Information Technology
Michelle Littlefield – Chief Data Officer, Data SF and Digital Services

COIT Staff
Julia Chrusciel
Danny Thomas Vang
Neil Dandavati

3. General Public Comment

There was no public comment.

4. Approval of Meeting Minutes from February 24, 2023 (Action Item)

There was no public comment.

Jillian Johnson made a motion to approve, Mark de la Rosa seconded.
The minutes were approved by Mike Makstman, Guy Clarke, Mikela Clemmons, Mark de la Rosa, Jillian Johnson, and Michelle Littlefield.

5. Surveillance Technology Policy Review: Audio Recording Technology (Action Item)

Alexander Leontiev, Robert Eickwort, Stephanie Rossi, David Turk, and Phillip Mau presented their policy for the ongoing use of:
- Human Services Agency: Call Recording Technology

Mikela Clemmons, Guy Clarke, Jillian Johnson, and Mike Makstman Asked:
- What is the average time that a recording remains on the system?
- Is there multi-factor authentication?
- Do people know that the recordings can be used in other cases, such as for legal purposes?
- Is there any additional notification when you ask for consent with the signature?
- Is it difficult/possible to retain the tele-signature without everything else?

The following was recommended by members:
- Under the authorized use section, be more explicit on how the department uses the data and when it will be used. Include use cases such as those affiliated with legal or law enforcement.
- Include specific language stating that information can be pulled via a subpoena.
- Include the Welfare Institution Code in the policy, to clarify what information can be shared with law enforcement.
- Under the external data sharing section, include state or federal agencies if applicable.
- Specify that a case can last from a few months to several decades.

There was no public comment.

Guy Clarke made a motion to move this item forward with the amended language, Jillian Johnson seconded.
The motion was approved by Mike Makstman, Guy Clarke, Mikela Clemmons, Mark de la Rosa, Jillian Johnson, and Michelle Littlefield.

6. Surveillance Technology Policy Review: Social Media Monitoring Technology (Action Item)

Connor Loeven, Karlie O'Toole, and Valeri Shilov presented their policy for the ongoing use of:
- Department of Elections: Social Media Monitoring Technology

Michelle Littlefield, Mikela Clemmons, Guy Clarke, and Mike Makstman asked questions about
- For the five-year data retention period, is this for the reports generated through the platform, or for the overall platform itself?
- Does this include private communications with this tool, or does it just include open and public social media?
- Is there an audit trail for posts that are deleted due to inappropriate or profane comments?
- If there is PII/PHI, how is that data being protected? What is the data protection controls of the platform?
- How many account administrators are there for the platform?
- Outside of multi-factor authentication, are there any safeguards for preventing the distribution/influence of the personal opinions of staff?
- Is the department monitoring replies and posts affiliated with its own post, or is the department monitoring election discussions from other people?

The following was recommended by members:
- Specify that the department is not using the platform to scrape or save social media data.
- Increase specificity on the intended use cases. Be explicit that the platform will not be used to listen to discussions and will not collect data on elections, nor be used for political speech.
- Remove the language surrounding facial recognition if not applicable.
- Remove the name of the platform from the document, and refer to it as social media monitoring technology.

There was no public comment.

Michelle Littlefield made a motion to move this item forward with the amended language, Mikela Clemmons seconded.
The motion was approved by Mike Makstman, Guy Clarke, Mikela Clemmons, Mark de la Rosa, Jillian Johnson, and Michelle Littlefield.

7. Department Updates & Announcements

Jillian Johnson gave an update on the migration from One Trust to LogicGate, a risk and compliance platform.

Mike Makstman asked if the subcommittee will be recruiting a public member in the near future, and suggested that members start to think about potential candidates.

Public commenter introduced themselves to the subcommittee.

8. Discussion: Surveillance Technology Inventory

Jillian Johnson discussed the Surveillance Technology Inventory with the Privacy and Surveillance Advisory Board members, including what is currently scheduled and the future schedule for 2023.

Mikela Clemmons noted that surveillance cameras might be able to fall under a central policy. There was no public comment.

9. Adjournment

The meeting adjourned at 2:55 PM.