ST Meeting #27 - 6.07.22

Participants:
Jason Scharf
Mujtaba Tirmizey
Martha Grabowski
Chief Tim Gleeson
Johannes Himmelreich
Daniel Schwarz
Ken Stewart
Kelsey May
Michelle Sczpanski
Deputy Mayor Sharon Owens
1st Deputy Chief Shoff
Ocesa Keaton
Jessica Brandt

Absent
Nico Diaz (Excused)
Mark King (Excused)
Jennifer Tifft (Excused)

Agenda:

- Discussion of new Technology Request for Review - Dataminr
- Coming Up
- Questions

Meeting Notes:

- We've met our one-year mark for meeting and doing this great work! There will be a social event to celebrate, as we get more information about that social gathering we will be sharing.
- Letters of commitment - we are still missing this signed document from 3 members. Please go ahead and do that!
- Data Miner technology
    - Not everyone was able to review the documentation shared.
    - What it does is scan already available on social media looking for keywords that would direct them to threats or events that they could mitigate risk. The software then notifies specific SPD personnel of the findings.
    - There were some questions/concerns about data storage and sharing risks.
    - Is this a data-gathering tool or does it integrate information from multiple platforms?
        - Unsure at this time regarding the answer to this.
    - Johannes asked if the vendor might be able to provide a demonstration of the tech.
    - Chief Gleeson has some experience with this.
        - It was used as a surveillance and monitoring tool. It is an advanced tool that can be used for very specific needs. The company does targeting scanning as well as broad scanning. It did integrate and scan the other media sites when it caught a trip.
        - Chief said that they were able to use it to make educated decisions relative to a specific event happening in real-time and helped them to deploy resources in real-time as the event was unfolding.
    - Is this a surveillance tech?
    - Martha asked if this tech was used offline as well as Chief Gleeson's experience was in real-time use.
        - Yes
    - We need more information about if there will be training for this.
- Is this a surveillance tech - vote?
    - Yes: unanimous
    - No: None
- Does this technology meet any of the exemptions?
    - Opening a vote if anyone feels that the technology does meet an exemption.
        - Chief Shoff raised a question on one exception. Not sure what the vote was otherwise
        - Chief Shoff made a point that the data is public and he questioned if the tech does meet that exemption.
            - The technology is where it would meet the opt out, not where the data is coming from. There was support that A could be considered as an exemption (gray area).
            - This is special access to data that not everyone has, the expectations of the users should be considered. Users of social media do not expect the data to be used by police and governing bodies. Social media data shouldn't be thought of as public.
                - Daniel supports this reasoning. Dataminr uses AI to geotag posts which is not something folks generally do when posting on social media.
                - A Legal definition is needed for what is considered public information
                    - Muj said he will look this up
            - Can it be used to identify other types of events? It could lead to events or probes by public safety and cold cases, but knowing how and why the tech is used is critical.
- Does this tech meet any of the exemptions - no one feels that this tech meets the exemptions.
- We will request Lt. Malinowski to join the next meeting.

    - Johannes asks that whoever knows the most about the tech would be the best to join in order to avoid many SPD personnel joining.
        - Whoever is vetting other use cases.
    - We will also invite someone from the vendor company to join and answer questions.
        - A document that outlines the capabilities of the platform would be incredibly helpful provided by the vendor.
            - Info they want =
                - Perhaps we could specify that we'd like a document beyond what is posted on their website -- system architecture, data storage policies, data retention policies, case studies of successes and failures
                - what data sources? What targeting possibilities? What inferences can they make (eg location, demographic info)? What steps have been taken to detect and mitigate bias?
                - How does the risk classification work? Are there audits for their machine learning tools (NLP, image recognition, audio recognition, ...)? How are they ensuring no First Amendment protected posts are captured?
- Anyone that wants to volunteer to do some research on this tech = Chief Shoff
- Daniel will send some links over to Jason
- We will be reaching out to the vendor for some answers and working on the press release simultaneously and decide to push the press release with or without the additional information when we get there.
- What is SPD’s goal for deploying this technology? This information has been requested.

Action Items:

- □ Muj stated that he will look up a legal definition for what is considered a legal definition of public information related to social media posts.
- □ Daniel to send over some information that the Brenner Center and NYCLU have already gathered regarding Dataminr technology.
- □ Jason will reach out to Communications team to start the Press Release
- □ Jason will reach out to Lt. Malinowski to invite him and Dataminr staff to the next STWG meeting.
    - □ Chief Shoff and Jason will also to share the questions that have been posed regarding the technology.
- □ Jen Tifft and Jason will be working on planning the STWG social get together.