Surveillance Technology Working Group

Meeting #64

09/10/2024

Agenda

- Presentation (Corinne Worthington & Albert Fox Cahn at Surveillance Technology Oversight Project at The Urban Justice Center)
- Cybercheck Update
- Quick Updates
- Coming Up
- Questions

Reference Slides

Review

Past Decisions

- **Fotokite:** Aerial UAS allowing for different perspectives during crisis response. Not exempt, will go through the process.
  - Press Release out, done with public comment period
  - Public comments received, received comments from SPD
  - Recommendation was sent to the Mayor
- **Vacant Lot Monitoring:** Sensor that detect changes in a scene to monitor lots for dumping. Not exempt, will go through the process.
  - Press Release out, done with public comment period
  - Grandfathered in because the request was made before review process
- **Community Asset Tracker:** Camera with machine learning algorithm to identify objects within the city.
  - Assessed pilot, documentation provided
- **COPS:** Cameras strategically placed around the city to aid in policing
  - Exempted

Review

Past Decisions

- **Samsara:** Fleet management technology
  - Assessed in previous session
  - Public comment period completed
  - Recommendation was sent to the Mayor on 2/01
  - Mayor Walsh stated that he read the read the groups recommendations, and is in agreement with a **qualified approval**, and is in agreement with the importance of putting in appropriate policies and procedures.
- **Flock Safety/ALPRs:** Street cameras that capture vehicle plates.
  - Assessed in previous session
  - Public comment period completed
  - The Work Group heard from SPD Officers on 1/25/22 for more information regarding this.
  - The STWG created guidelines for ALPR Use and this was recommended to the mayor with the stipulations written on 3/11/22.

Review

Past Decisions

- **Cyclomedia:** Right of Way Imaging
  - Public comment period completed
  - Recommendation was sent to the Mayor on 5/07/22
  - Mayor Walsh stated: I have reviewed the STWG's recommendation and I am in agreement with it.
- **Dataminr**: Social Media monitoring of violent posts.
  - Dataminr staff met with STWG on 6/21/2022.
  - Dataminr then removed their offer of service on 6/21/2022.
- **Rubicon**: Vehicle route optimization software
  - STWG met on 9/27/22 and this was determined to not be a form of Surveillance
- **Opticom**: Software that in an event of an emergency the Fire Department could switch the traffic lights on their route to turn green for them.
  - STWG met on 12/06/22 and this was determined to not be a form of Surveillance

Review

Past Decisions

- **Body-Worn Camera's (Code Enforcement):**
  - Recommendation was sent to the Mayor in Sept. 2023
  - Mayor Walsh signed a letter stating that he is in agreement with the groups determination.

Review

Internal Norms

Attendance:

1. If members have unjustified absences for three meetings in a three month time period, the Surveillance Team Working Group (STWG) Coordinators will reach out to the member.
2. The working group is required to have at least 50% of all members present before we hold a recommendation vote.
    a. Of those present at least 40% should be non-city staff.

External Participants:

1. Outside participants should request permission before-hand to the API team.
    a. The API team will inform the STWG before meetings if there will be outside participants joining the group.

Documentation for Community Review:

1. The notes from the STWG Sessions will be posted to the STWG Website after the meetings.

Letter of Commitment:

1. Is effective for one year, and is to be sent out annually.

View Attendance and Guest Norms

Review

Service Level Agreements (SLAs)

2 - 6 Weeks (10 - 30 Business Days)	Every 2 Weeks (10 Business Days)	2 Weeks (10 Business Days)	2 Weeks (10 Business Days)
Initial submission to determination of surveillance	Short duration meeting to vote on technology exemptions	Public comment period: ● Issuance of press release ● Council meeting (*) For now public input will be received via a Google Form and in the future will be on the new website.	Submission of finalized form (by dept.) to time of recommendation. Group will individually research; departments will get follow-up questions; group to vote yes/no; and submit recommendation.

STWG Planning (Review)

Update STWG Website ☑ **(Complete)**

- Tech Recommendations
- Meeting Notes and Slide Decks

Connect with other **cities doing Surv. Tech Work**

Short Term (April – June 2022)

Revamp our approach to **community engagement**

Complete Citywide **departmental training**

- Determine Schedule for refresher trainings (annually or every 6 months)

Medium Term (July – September 2022)

Complete an audit of technologies currently used by the City as **Surveillance or Not** ☑ **(Complete)**

Release an **Annual Report**

- Including recommendations, data that came from recommendations, and if stipulations are being followed.

Long term (October 2022 – December 2023)

STWG Long Term Plan (Review)

Begin process of trying to transfer STWG to a **City Ordinance**

Determine Member's **Term Duration**

Requires more planning

Definition

Definition of a Surveillance Technology (According to Mayor's Executive Order on Surveillance Technology):

- Technologies that "observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice."

Meeting slides

Guest Presentation

Corinne Worthington & Albert Fox Cahn at Surveillance Technology Oversight Project at The Urban Justice Center

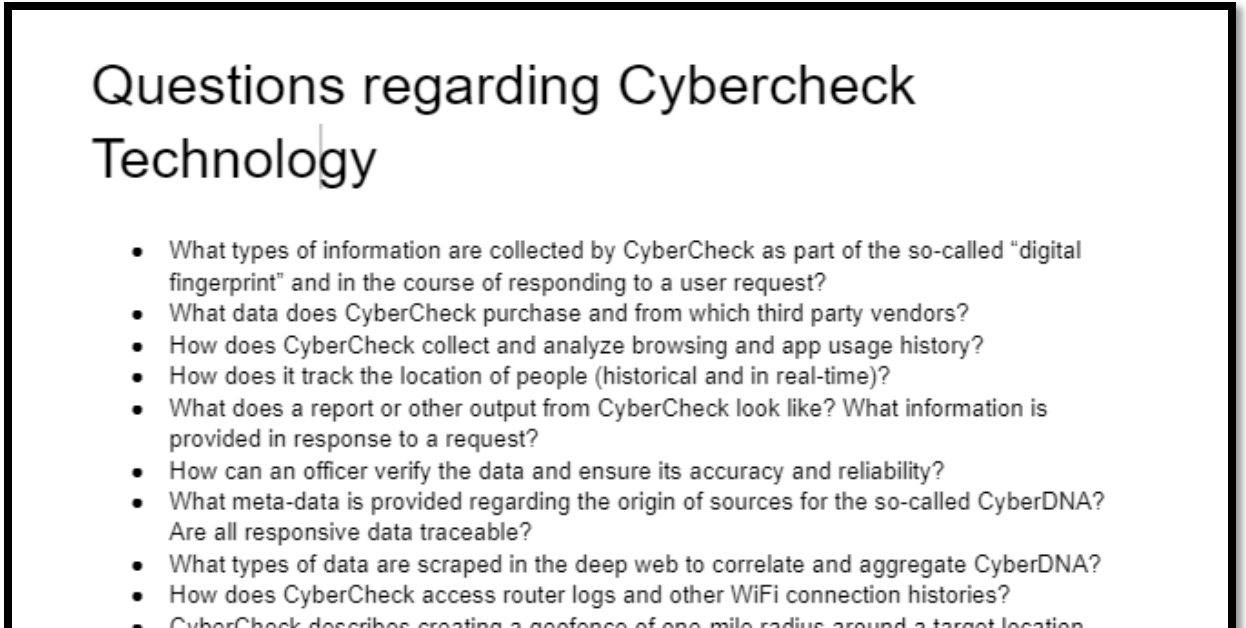
SPD – Cybercheck Digital Footprint Tracker

Which City department is requesting this technology?	Police Department
Who will be the department contact for this technology?	Deputy Chief Richard Shoff
Please give a brief description about the technology that you are looking to implement?	This is a subscription service to generate investigative leads based on someone's potential "digital footprint". This service queries publicly accessible databases in order to generate potential investigative leads for persons of interest at the scene of a criminal incident. Their product is able to query large batches of data exponentially faster than a single user could.
Do you have a vendor selected that you would like to work with?	Yes
What is the name of the vendor?	Cybercheck
Are you looking for this to be a pilot program or a new technology implementation?	New Technology
What will be the purpose of this new technology? What do you hope to accomplish with this?	We wish to generate investigative leads on suspects who were potentially in the area of a criminal incident.
Do you know where the information that is obtained will be stored?	The data queried by this company is from publicly available databases
Who is the intended audience for this system?	Law enforcement

Do you know how long you plan on using this technology?	1 year (with option to renew)
Is this a piece of physical hardware or software?	It is a subscription service, no Syracuse Police user will have access to a software or hardware piece.
What type of information would be captured from this technology?	The company captures publicly available connections which are made by a subjects device interacting with another device at a specific location of interest.
Have you started the procurement process for this yet?	Yes
Where are you currently at in the procurement process?	Contacted Cybercheck and received a quote for one year subscription
Is there anything else about this technology that you would like to let us know about?	This company has a law enforcement user make an investigative inquiry about a particular location involved in criminal activity. For example, a law enforcement user will advise the company about a crime occurring at a particular location and they will develop suspect information independently. Law enforcement users will provide Cybercheck with pieces of the suspect's "digital fingerprint" and ask Cybercheck to query if any of these digital fingerprints are in the area of the crime during that particular time. This company then generates possible investigative leads on "digital fingerprints" that were in the area of the incident at that time. These digital fingerprints could be an IP address or an email address which was trying to query devices for possible connections like a wireless router or some type of Bluetooth device. The company describes these data as devices "waving" to each other in an attempt to make a connection in the future. The easiest example to describe is when your phone searches for WiFi in an area and recognizes the available networks within range. Cybercheck is able to find those potential connections by querying publicly available data. Law enforcement users are then able to follow up with further legal process with those generated investigative leads.

Cybercheck

- Have list of questions for SPD here
- Officers will review and get back to group at an upcoming meeting
- Are waiting to do public comment, until the group gets feedback from SPD



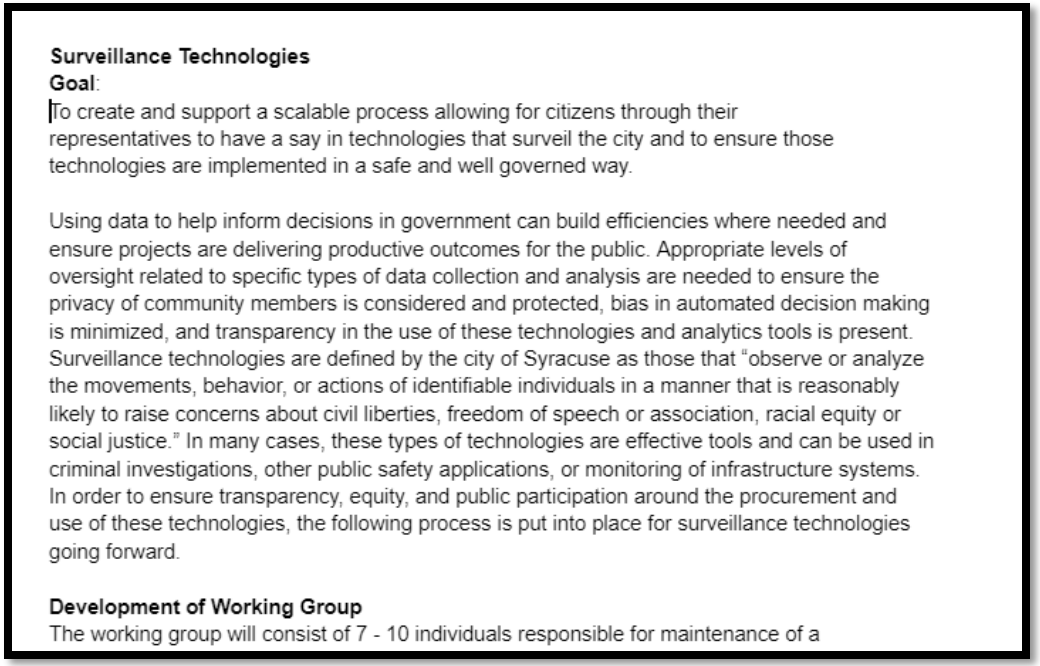
Questions regarding Cybercheck Technology

- What types of information are collected by CyberCheck as part of the so-called "digital fingerprint" and in the course of responding to a user request?
- What data does CyberCheck purchase and from which third party vendors?
- How does CyberCheck collect and analyze browsing and app usage history?
- How does it track the location of people (historical and in real-time)?
- What does a report or other output from CyberCheck look like? What information is provided in response to a request?
- How can an officer verify the data and ensure its accuracy and reliability?
- What meta-data is provided regarding the origin of sources for the so-called CyberDNA? Are all responsive data traceable?
- What types of data are scraped in the deep web to correlate and aggregate CyberDNA?
- How does CyberCheck access router logs and other WiFi connection histories?
- CyberCheck describes creating a geofence of one-mile radius around a target location

Quick Updates

Proposed Revisions to Executive Order #2

Proposed revisions have been made in a Google Document HERE



Surveillance Technologies
Goal:
To create and support a scalable process allowing for citizens through their representatives to have a say in technologies that surveil the city and to ensure those technologies are implemented in a safe and well governed way.

Using data to help inform decisions in government can build efficiencies where needed and ensure projects are delivering productive outcomes for the public. Appropriate levels of oversight related to specific types of data collection and analysis are needed to ensure the privacy of community members is considered and protected, bias in automated decision making is minimized, and transparency in the use of these technologies and analytics tools is present. Surveillance technologies are defined by the city of Syracuse as those that "observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice." In many cases, these types of technologies are effective tools and can be used in criminal investigations, other public safety applications, or monitoring of infrastructure systems. In order to ensure transparency, equity, and public participation around the procurement and use of these technologies, the following process is put into place for surveillance technologies going forward.

Development of Working Group
The working group will consist of 7 - 10 individuals responsible for maintenance of a

Coming Up

Presentation Schedule

Month	Presenter	Organization	Topic
Sep-24	Corinne Worthington & Alan Newcomb	Surveillance Technology Oversight Project @ The Urban Justice Center	AI bias and responsible evaluation and Selection of Technologies that might be employed at a Local Level
Dec-24	Ivey Clark	Brennan Center for Social Justice	Overview of the Brennan Centers Work
TBD	Daniel Schwarz	NYCLU	TBD

If you have ideas for upcoming presenters, please email Jason Scharf at jscharf@syr.gov

Questions