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 surveillance technology inventory and the evaluation of technologies as they go through the surveillance technology process. The goal of the group will be to ensure due diligence is done on all technologies fitting the surveillance characteristics so thorough and valid recommendations can be given to the final decision maker on how any given technology will impact the City of Syracuse in a variety of areas including equity or service, efficacy of collection techniques, financial capabilities of implementation, and benefit to the taxpayer. This working group will be selected by the Mayor with recommendations from Senior Staff and the Office of Accountability Performance and Innovation (“api”).

The group is tasked with the responsibilities listed below.

A. Creation

1. Internal Stakeholder Selection
    a. Stakeholders to be selected by the Mayor
    b. One representative from api
    c. One representative from IDEA
    d. One representative from IT

2. External Stakeholder Selection
    a. Stakeholders to be appointed by the Mayor
    b. Up to five to seven stakeholders from a variety of community groups in City of Syracuse
        i. Must include at least one member from each of the following types of organizations: social justice, technology, community outreach, research institution/partnerships (NuAir, universities)

B. Responsibilities

1. Determination of whether surveillance technology falls into one of two categories: First category will have characteristics that if met automatically define a technology as surveillance. Second category will have characteristics that if a certain percentage are met the technology will be considered surveillance.
2. Initial audit defining technologies currently used or owned by the City as surveillance or not. These technologies will be grandfathered into the system and not go through the voting process, will simply be tracked for public dissemination.
3. Regular meetings to review proposed technologies, define these technologies as surveillance or not, and give recommendations about whether systems that are deemed to be surveillance technology should be implemented.
4. Upkeep and maintenance of the technology audit list. The audit list will track all technologies that go through the group, any recommendations by the group, all drafts and final documentation about those technologies, and the final approval.

C. Recommendations

1. api will work with the working group once they have been selected by the Mayor and present initial recommendations around definition of surveillance characteristics and process structure.
2. Recommendations provided by the working group will be presented in a standardized format designed by the working group
3. It is recommended that the working group develops Service Level Agreements to ensure a swift but effective process.

Process

A. Departments interested in the use of a data collection technology must submit to the working group for a determination of whether it qualifies as a “Surveillance Technology”

1. Surveillance Technology Definition:

   a. Technology whose primary purpose is to 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. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.
2. Exemptions:
   a. Technology that is used to collect data where any individual knowingly and willingly provides the data.
   b. Technology that is used to collect data where individuals were presented with a clear and conspicuous opt-out notice.
   c. Technologies used for everyday, normal course of business office use.
   d. Body-worn cameras (refer to existing BWC policy).
   e. Cameras installed in or on a police vehicle (refer to existing policy).
   f. Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations (data collected would be used exclusively for traffic enforcement purposes).
   g. Cameras installed on City property solely for security purposes.
   h. Cameras installed solely to protect the physical integrity of City infrastructure, such as cameras at water reservoirs.
   i. Technology that monitors only City employees in the performance of their City functions.
3. Technologies that will not be considered and are effectively banned from use in the City of Syracuse
   a. Any technologies using biometric, facial recognition, or whole-body gesture analysis
   b. Predictive policing algorithms

B. Preliminary form completion

Draft form can be found at this link: https://www.surveymonkey.com/r/NXTSQFQ
For a complete list of questions please reach out to the api team.

C. Determination of surveillance by working group

Working group will review the proposed technology and determine whether the technology meets the definition of surveillance technology or not. If the technology is deemed not to constitute surveillance technology, it proceeds straight to the City's standard procurement process. If the technology is determined to meet the threshold of surveillance it will continue on to the public comment period.

D. Public comment period (if deemed surveillance technology)

1. Preliminary form is posted online for at least two weeks with form for comments available
2. Preliminary form is presented in a press release from the Mayor's office the day it is also posted online.
3. Preliminary form is presented at at least one Common Council committee meeting

E. Final form completion

1. Following the public comment period, the preliminary form is finalized, including any comments that came in during the public comment period.
2. Final draft is provided to the working group for review.

F. Working group review and recommendation

1. A working group (see above for details) made up of a diverse range of community members will convene to review surveillance technology documents and make recommendations, specifically considering harm a technology may cause underrepresented groups.
2. Working group reviews the document, offers comments, and returns the document to the City department.

G. Approval and Oversight

1. The Mayor's Office will decide whether to allow the use of the proposed surveillance technology.
2. If the surveillance technology is approved by the Mayor, the implementation of the technology proceeds through the City's standard procurement and contracting process, including any necessary Common Council approvals.
3. Finalized documents are made available to the public.

Surveillance Technology Mandated Standards

Building predictive models and automated decision making tools can create efficiencies in government and can enable more proactive work to happen. The model, though, is only as good as the data that feeds it. Predictive models are based on historical data, so if the data has been biased in the past, it will create a model that is biased for the future. For instance, in the case that the City was trying to predict which streets have potholes, relying on where potholes have been complained about would be problematic because community members in some neighborhoods report more potholes than in other neighborhoods. The model would predict based on that history of complaints that were filled, not actually where the potholes exist. In the

case where predictions are being made about people, issues like bias about race, ethnicity, and economic status can come into play, too, and have adverse effects.

Prior to any data project that includes automated decisions or predictive analytics, the following questions should be considered, answered, and submitted to the Chief Data Officer for approval as part of the project charter.

A. Data Collection

1. Informed consent: Any human subjects have been given informed consent, where subjects affirmatively opt-in and have a clear understanding of the usage of data to which they consent.
2. Collection bias: Consider and document sources of bias that could be introduced during data collection and survey design and any steps taken to mitigate those.
3. Limit PII exposure: Consider and document ways to minimize exposure of personally identifiable information (PII) for example through anonymization or not collecting information that isn't relevant for analysis.

B. Data Storage

1. Data security: Develop a plan to protect and secure data (e.g., encryption at rest and in transit, access controls on internal users and third parties, access logs, and up-to-date software).
2. Right to be forgotten: Create an easily accessible and publicly navigable mechanism through which an individual can request their personal information be removed.
3. Data retention plan: Develop a schedule or plan to delete the data after it is no longer needed including a timetable and rationale for data deletion.
4. Use UUIDs to ensure dissemination and analysis of data is not identifiable through PII.

C. Analysis

1. Missing perspectives: Consider and document ways to address blindspots in the analysis through engagement with relevant stakeholders (e.g., checking assumptions and discussing implications with affected communities and subject matter experts).

2. Dataset bias: Examine the data for possible sources of bias and take steps to mitigate or address these biases (e.g., stereotype perpetuation, confirmation bias, imbalanced classes, or omitted confounding variables).
3. Honest representation: Ensure visualizations, summary statistics, and reports are designed to honestly represent the underlying data.
4. Privacy in analysis: Ensure that data with PII are not used or displayed unless necessary for the analysis.
5. Auditability: Ensure the process of generating the analysis is well documented and reproducible if issues are discovered in the future. This requires a full methodology so that even when data has been removed by request or process statute solutions can be developed to remedy those issues.

D. Modeling

1. Proxy discrimination: Ensure that the model does not rely on variables or proxies for variables that are unfairly discriminatory.
2. Fairness across groups: Test model results for fairness with respect to different affected groups (e.g., tested for disparate error rates) and determine whether that fairness (or unfairness) is due to the data, the model, the scenario, or something else. Document the outcome.
3. Metric selection: Consider the effects of optimizing for our defined metrics and consider additional metrics.
4. Explainability: Explain and document in understandable terms a decision the model made in cases where a justification is needed.
5. Communicate bias: Communicate the shortcomings, limitations, and biases of the model to relevant stakeholders in ways that can be generally understood.

E. Deployment

1. Redress: Discuss with the organization a plan for response if users are harmed by the results (e.g., how does the data science team evaluate these cases and update analysis and models to prevent future harm). Ensure there is a documented process in place to address this harm.
2. Roll back: Ensure there is a way to turn off or roll back the model in production if necessary.
3. Concept drift: Complete testing and monitor for concept drift to ensure the model remains fair over time.
4. Unintended use: Document and act upon steps to identify and prevent unintended uses and abuse of the model and have a plan to monitor these once the model is deployed.