City of Seattle

2021 Surveillance Impact Report Executive Overview

Maltego

Seattle Police Department

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD's Maltego. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

Paterva's Maltego is a cyber-security software application that is used to assist Seattle Police Department (SPD) to research publicly available data and diagram associations between individuals, devices, and networks, as part of a cybercrime investigation. Maltego allows up to two authorized users in SPD's Technical and Electronic Support Unit (TESU) to trace the origin of a specific IP address, and potentially identify a suspect, that has attacked, or attempted to infiltrate, the City's network or the network of a third party. In essence, SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

2.0 Purpose

Maltego queries public data on the internet, such as domains, and displays it in a diagram showing links. This is a useful tool for SPD to use in cyber-crime investigations, as these incidents often involve interactions between individuals, devices, and networks that are otherwise unknown. This is a popular tool that is used across the information-security community for both defensive cyber-security programs and for investigating breaches and instances of cyber-crime. SPD utilizes Maltego in these capacities.

A typical use would be Maltego's use in diagramming threat actors following a cyber-attack on the City's network. An investigator would need to research the IP address of domain of the attack source and work to find the individual(s) or organization(s) orchestrating the attack. Often, the source of the attack is a system belonging to a third party that has itself been compromised (i.e., bot networks) and a side benefit of an SPD investigation is mitigating the compromise of these third-party systems.

3.0 Data Collection and Use

Operational Policy: All use of the Maltego software must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes. Use of Maltego is governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

Maltego queries publicly available data on the internet and collects information based on the parameters of the search request, much like Google returns results based on specific search terms. Maltego is not used to collect private data, nor is it used to process or collect internal data. It is specifically a tool used to query and diagram public information related to cyber-crime investigations. In this sense, it is collecting any publicly available information on the internet related to the specific parameters of the user request.

Maltego is only used by two trained TESU Detectives whose primary duties involve the investigation of cyber- and other internet-related crimes. All data collected is related to a criminal investigation and included in the investigation file. Maltego is used when a specific incident occurs in which the network security of the City or of a private entity has been compromised, and an investigation has been instigated.

4.0 Data Minimization & Retention

Operational Policy: The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

If no data is collected that assists in the pursuit of the criminal investigation, this information is not retained, and no data is provided to the investigating Officer/Detective.

Data, when pertinent, is exported as a spreadsheet and/or visual diagram, at which point it is handled per department policy regarding digital evidence as part of a criminal investigation. A local copy of the data is only saved if the Detective operating Maltego manually initiates a local saved copy and that is also maintained and handled per department policy.

5.0 Access & Security

Operational Policy: All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including:

- **SPD Policy 12.040 - Department-Owned Computers, Devices & Software,**
- **SPD Policy 12.050 - Criminal Justice Information Systems,**
- **SPD Policy 12.080 – Department Records Access, Inspection & Dissemination,**
- **SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and**
- **SPD Policy 12.111 – Use of Cloud Storage Services.**

Access

Access to Maltego is restricted to use for the related security incident and/or pertinent criminal investigations and subject to Department Policy regarding ongoing criminal investigations.

Only authorized SPD users can access Maltego or the data while it resides in the specific workstation where it is installed. Access to Maltego is via a password-protected software interface and the software is stored locally rather than on the network or remote server.

Security

Data collected by Maltego is stored on an encrypted workstation within TESU.

Per the CJIS Security Policy:

"Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

6.0 Data Sharing and Accuracy

Operational Policy: No person, outside of SPD, has direct access to Maltego or the data while it resides in the system or technology.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared without outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by Maltego may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by Maltego.

7.0 Equity Concerns

Operational Policy: To mitigate against any potential algorithmic bias or ethnic bias to emerge in the use of link analysis software such as Maltego, SPD employees are responsible for gathering, creating, and disseminating and are bound by SPD Policy 5.140 which forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Maltego is used during the investigation of cyber-crimes by the SPD TESU and information gathered is related to these criminal investigations. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.