From: Seattle Community Surveillance Working Group (CSWG)
To: Seattle City Council
Date: June 4, 2019
Re: Privacy and Civil Liberties Impact Assessment for Acyclica (SDOT)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Report (SIR) on Acyclica, a surveillance technology included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides our recommendations to the Council, then provides background information, key concerns, and outstanding questions on Acyclica technology.

Our assessment of Acyclica focuses on three major issues rendering protections around this technology inadequate:

1. SDOT has no explicit policies governing its use of Acyclica technology.
2. There is no contract between SDOT and Acyclica, which contributes to the following concerns:
   a. There is no policy or other agreement that ensures SDOT owns the non-aggregated data collected by Acyclica devices;
   b. Acyclica's stated data security practices are misleading and unclear;
   c. There are no limits on Acyclica's retention of non-aggregated data; and
   d. There is no limit on or designation of which third parties will access Acyclica's data, for what purpose, and under what conditions.
3. There is no evaluation of the technical abilities of the EDI DA-300 (the new sensor that we have learned will replace the RoadTrend sensor evaluated in the SIR), and it is not stated whether the EDI DA-300 will be used in conjunction with or replace all RoadTrend sensors.

Recommendations

The Council should adopt, via ordinance, clear and enforceable rules that ensure, at the minimum, the following:

1. The purpose of Acyclica technology must be clearly defined, and operation of the technology and data collected by it must be explicitly restricted to those purposes only. For example: Acyclica may only be used for traffic management purposes, explicitly defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
2. There must be a written, binding contract directly between SDOT and Acyclica (as well as Western Systems, if applicable) that includes the following minimum provisions:
   a. SDOT owns all data, not Acyclica (or FLIR, the company that acquired Acyclica).
   b. SDOT receives only aggregated data.
   c. The data retention period for any data Acyclica collects shall be 12 hours or less, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both the non-aggregated and aggregated data.
   d. Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.

3. SDOT must produce an annual report detailing its use of Acyclica, including details of what data is collected, how much data is collected, how SDOT used the data collected, for how long it was retained, and in what form.

Background: Privacy and Civil Liberties Concerns with Acyclica Technology

Acyclica technology is a transportation management tool used by SDOT that raises privacy and civil liberties concerns because of its ability to uniquely track, identify, and create a detailed map of individuals' movements. Acyclica manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that collect encrypted media access control (MAC) addresses—unique identifiers attached to devices—from any WiFi-enabled device (e.g., cell phones, computers, and vehicles) within range of the sensors in Seattle.

Because these sensors are placed on at least 301 intersections in Seattle and collect and record MAC addresses 24 hours a day, 7 days a week, and 365 days a year, Acyclica can generate extremely precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of drivers and riders in vehicles, but they can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close buildings (e.g. apartments and offices). This powerful location-tracking technology raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These privacy concerns are exacerbated by the absence of specific policies governing use of Acyclica technology and the absence of a contract between SDOT and Acyclica. Without contractual restrictions on data use, ownership, and sharing, Acyclica data can be shared with third parties (e.g., companies and law enforcement), may be combined with additional data such as facial recognition data, and repurposed for non-traffic management purposes.

Of additional concern is that the RoadTrend sensors evaluated in the current SIR were discontinued in March 2019 after Acyclica was acquired by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense. While SDOT states that it is in the process of procuring a new sensor, the EDI DA-300, the SIR does not include an evaluation of this new sensor's capabilities.

Finally, while SDOT cites cost savings and Acyclica's ability to accurately measure traffic times as the two key reasons it decided to procure Acyclica technology, the results of the study attached to the SIR[1] are inconclusive on Acyclica's accuracy. The study states: "In terms of accuracy, Acyclica did not perform as well as desired."[2] Given this assessment, it is unclear how privacy and civil liberties concerns were considered when SDOT made the decision to acquire Acyclica—while Acyclica may generate cost savings relative to some other (but potentially not all) comparable technologies, it also creates new privacy challenges without presenting clear gains on accuracy.

Key Concerns

(1) **There are no specific policies defining purpose of use.** In the updated SIR, SDOT states, "We have no specific policies guiding our use of Acyclica, but SDOT's intent is to use this data service to deliver travel time, delay, analytics and other traffic data."[3] This stated intent and other uses cited in the SIR are vague and impose no meaningful restrictions on the purposes for which Acyclica devices may be used. For example:

[1] *Acyclica Travel Time Accuracy & Reliability Analysis*
[2] The study states, "Acyclica did not pass the t-test because the results showed that the means were not the same." This means that Acyclica was unable to produce similar values to License Plate Reader Cameras, which were assumed to represent the ground truth. Though it is possible that the LPR data itself could have been inaccurate, the study's results are inconclusive on Acyclica's accuracy in measuring traffic times.
[3] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 120.

- Section 1.1 of the abstract states that Acyclica is used by over 50 agencies "to help to monitor and improve traffic congestion."
- Section 2.1 provides some examples of types of information Acyclica uses (e.g., calculated average speeds) to produce certain outcomes (e.g., correcting traffic signal timing), but it is unclear if the examples cited constitute a complete list.

The above statements do not describe the purpose of use, all the types of information Acyclica collects, and all the types of work that Acyclica technology facilitates.

(2) **There is no contract between SDOT and Acyclica.** In the updated SIR, SDOT states, "SDOT does not have a contract with Acyclica."[4] Without a contract or statutory protections, data ownership and restrictions on the scope of data sharing and repurposing cannot be enforced. For example, without contractual restrictions or statutory protections, Acyclica would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate readers or facial recognition data. Because SDOT does not have a contract with Acyclica, even if SDOT did have specific policies defining and restricting purpose of use, SDOT cannot enforce those policies restricting the use of Acyclica technology to the intended purpose.

(3) **There is a lack of clarity on data ownership.** In the updated SIR, SDOT states, "SDOT owns the raw and aggregated data. See the attached letter *SDOT Acyclica Data Ownership* which clarifies that."[5] However the attached letter[6] does not actually provide any documentation showing that SDOT owns the raw (i.e., non-aggregated) data. This letter simply states that FLIR will not grant unauthorized users access to Acyclica software.[7]

(4) **There are no limits on Acyclica data retention.** In the updated SIR, SDOT states, "Acyclica/FLIR does not have a limit on data retention. The reason for this policy is that as they develop new methods of analyzing traffic, the analyses are effective as of the date the sensors were first deployed rather than when the feature was first available in the software."[8] If SDOT owns all of the data, including the non-aggregated data, it is unclear why Acyclica/FLIR would be setting their own limits on data retention. The upshot appears to be no enforceable limits on data retention.

(5) **There is a lack of clarity on the capabilities and usage of the new Acyclica/FLIR sensor (EDI DA-300).**[9] Acyclica has recently been acquired by FLIR Systems, and the RoadTrend sensors evaluated in the SIR have been discontinued. SDOT states: "Since the RoadTrend product line was discontinued, we've begun procuring the EDI DA-300 (please see attached data sheet) in its place. The EDI DA-300 will be the model we consistently deploy in the foreseeable future, and there are no plans to consider an alternative at this point. This unit has additional features differentiating it from the RoadTrend such as generating alarms when a traffic cabinet door is opened, and the ability to provide remote access to traffic signals using cellular communication." It is unclear whether the EDI DA-300 will be used in

[4] Ibid.
[5] Ibid.
[6] See Appendix A – Letter on SDOT Acyclica Data Ownership
[7] Moreover, in a 2018 conversation between the American Civil Liberties of Washington (ACLU-WA) and Daniel Benhammou (President of Acyclica), Benhammou stated that Acyclica owns all of the non-aggregated data. These contradictory statements make it unclear who actually owns the non-aggregated data.
[8] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 121.
[9] The initial SIR failed to mention that Acyclica had been acquired by FLIR and that the RoadTrend sensor had been discontinued. Only in response to the ACLU-WA's pointed questions did SDOT include in the updated SIR that it was aware of the FLIR acquisition and has been making clear plans to procure a new sensor.

conjunction with or to replace all RoadTrend Sensors. Because a full description of the capabilities of the EDI DA-300 has not been included in the SIR, neither the public nor the CSWG was been able to conduct a full evaluation of the technology. The involvement of Western Systems[10], a third-party vendor which is the only entity with whom SDOT currently appears to have a written agreement, further complicates matters—it is unclear if terms in the MoU with Western Systems are still applicable. The relationship between SDOT, Western Systems, and Acyclica/FLIR must be explicitly clarified, and explicit contractual terms ensuring purpose, operation, data use, data dissemination, and data deletion should be put in place if they do not already exist.

(6) **There are inaccurate and contradictory descriptions of data security practices.[11]** The SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor.[12] However, according to a letter from Daniel Benhammou (President of Acyclica) provided by SDOT representatives at the first public comment meeting on the Group 2 technologies,[13] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. The response from SDOT in the updated SIR does not clarify whether the data is or is not hashed on the sensor. It simply states: "Prior to being transmitted from the sensor in the field to the cloud, the data is encrypted end-to-end using TLS and a 2048-bit encryption certificate." These contradictory descriptions make it difficult to understand Acyclica's data security practices.

(7) **It is unclear which third parties have access to the non-aggregated data, for what purpose, and under what conditions.** In the updated SIR, SDOT states: "Acyclica has given the ability for cities to manage their own users and additionally taken steps to eliminate data sharing unless the owning city has given explicit authorization. Existing users of SDOT's aggregated travel time data include: (1) SDOT staff conducting engineering studies, (2) WSDOT and KC Metro staff conducting engineering studies in partnership with SDOT, (3) Consulting partners who build traffic products on SDOT's behalf."[14] It is unclear if these users listed are *all* the users that have access to SDOT's aggregated travel time data. Of greater importance, it remains unclear who has access to the non-aggregated data, if any, for what purposes, and under what conditions.

Outstanding Questions

The following information should be included in an update to the Acyclica SIR:

(1) Who owns the non-aggregated data collected by Acyclica devices, and what policies or other documentation state this?
(2) What are Acyclica's data security practices, and what policies or other documentation state this?
(3) Which third parties that will access Acyclica's data (both aggregated and non-aggregated), for what purpose, and under what conditions?
(4) What is the relationship between SDOT, Acyclica/FLIR, and Western Systems? Are the Western Systems terms still applicable given the FLIR acquisition?
(5) What are the capabilities of the new EDI DA-300 sensors?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

[10] Western Systems is the vendor that owns, operates, and is responsible for the maintenance and replacement of the hardware used to gather the data.
[11] Section 7.2 of the SIR states: "Contractually, Acyclica guarantees that the data is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key or access to the data can identify individuals.
[12] 2019 Surveillance Impact Report Acyclica SDOT, Section 4.2, page 11.
[13] See Appendix B – Benhammou Letter
[14] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 121.

Appendix A – Letter on SDOT Acyclica Data Ownership

March 14, 2019

Jason Cambridge
Seattle Department of
Transportation 700 5th Avenue
Seattle, WA

Dear Mr. Cambridge,

Thank you for taking the time to meet with me on the 14th of March to discuss data privacy and ownership. When we started working with Seattle DOT in 2014, we committed that the only parties who would have access to the data generated by Seattle DOT would employees and those individuals which authorized users had granted access to the Acyclica software. FLIR's contractual obligations for data and support have been governed by the terms of use and the contract which our intermediary, Western Systems, executed with Seattle DOT. Some of these users, as designated by Seattle DOT have also been granted APIs for programmatically accessing aggregated data.

Moving forward, we renew our commitment to data privacy and security. FLIR will not grant access to Seattle DOT data to anyone without the express, written consent to do so. As the needs of Seattle DOT evolve, we are open to implementing additional measures to protect privacy of individuals while providing the best insights through the Acyclica platform.

Best Regards,

Daniel Benhammou

Senior Director, Software and
Solutions FLIR Systems, Inc.

Appendix B - Benhammou Letter

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.