March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

---

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.

[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.

[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

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 reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered 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 and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?

- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?

- Who owns the raw, non-aggregated data collected by Acyclica devices?

- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?

- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.

- What third parties will access Acyclica's data, for what purpose, and under what conditions?

- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?

- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?

- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.

- The contract between SDOT and Acyclica must include the following minimum provisions:

    - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.

    - SDOT receives only aggregated data.

    - SDOT owns all data, not Acyclica.

    - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.

- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, 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.

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

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS*. At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43

[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS*. While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD.* It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies.* At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?

- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.

- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: 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.