**City of Seattle**
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

**Privacy & Cybersecurity Committee volunteers**
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

**Community Technology Advisory Board**
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

# SFD: Computer-Aided Dispatch (CAD)

## Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

## Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov."
https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov."
https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018,
https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

# SDOT: Acyclica

## Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

## Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/

[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/

[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

# SCL: Binoculars, Check Meter, SensorLink

## Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

## Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

# SPD: 911 Logging Recorder

## Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

## Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

# SPD: Computer-Aided Dispatch (CAD)

## Comments

As mentioned in the section “SFD: Computer-Aided Dispatch (CAD)” and the section “SPD: 911 Logging Recorder”, these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD’s CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

## Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by “other civilian staff whose business needs require access to this data”. All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD’s CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

# SPD: CopLogic

## Comments

### Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

### Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

## Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page