



THE SILICON HILLS HAVE EYES

*How ARIC Fusion Center Surveillance Makes
Austin Less Safe*



JUST
FUTURES
LAW

grassroots
leadership
helping people gain power



Boston University School of Law

ACKNOWLEDGEMENTS

Take Back Tech Fellow: Professor Sarah Sherman-Stokes, Clinical Associate Professor of Law at the Boston University School of Law

Writers: Daniela Hargus, Cristina Moreno, Kennedy Barber-Fraser—
Students from the Boston University School of Law

Editors: Bob Libal, Paromita Shah, Bethany Carson, Professor Sarah Sherman-Stokes

Research Support: Julie Mao

Design: Katya Guzman and Maria Reza

July 2021



Boston University School of Law

THE SILICON HILLS HAVE EYES

How ARIC Fusion Center Surveillance Makes Austin Less Safe

TABLE OF CONTENTS

Executive Summary	4
Introduction	8
Background: The Austin Regional Intelligence Center	9
ARIC Evades Community Accountability	11
ARIC Shares Personal Data With APD	12
ARIC's Spyware	13
ARIC's Toll on Austin Communities	15
<i>Targeting Activists, including Black Lives Matter</i>	16
<i>Increasing Risk of ICE Enforcement Activity in Austin</i>	17
<i>ARIC facilitates surveillance and criminalization of Students and Youth</i>	18
ARIC Continues Data Mining and Surveillance Despite Community-driven Changes	19
Conclusion & Recommendations	20

EXECUTIVE SUMMARY

"Always eyes watching you and the voice enveloping you. Asleep or awake, indoors or out of doors, in the bath or bed—no escape. Nothing was your own except the few cubic centimeters in your skull." - George Orwell, 1984

On a clear November evening in 2019, a father mails a package of toys to his children in Lebanon from a Lakeway Park Mail store. He smiles as he hands over the box to be weighed, anticipating the video his wife would later send of his children opening their gifts with delight. The smile fades to frustration as he attempts to convince the clerk that indeed, Lebanon does not use zip codes, so he cannot provide one to fill the automated boxes on his screen. The father is completely unaware of the citizen informant standing a few people behind him who begins filming the interaction, squinting with suspicion at his accent and raised voice as he attempts to explain Lebanon postal address formats for the dozenth time. Later that evening, the informant will report him to a collection of 20 law enforcement agencies as a "suspicious" "Middle Eastern" person, suspected of terrorist activity for "refusing to provide personal info for mailing a package to Lebanon." This father is now on a watch list.

Six months later, a flora enthusiast photographs local wildflowers, moved by their resilience as they grow through the cracks in the concrete jungle. Spotting some from his car window growing along a chain link fence, he pulls over to zoom in. Unaware that the wildflowers he is admiring took root outside an Austin police training facility,

he is surprised to be confronted by several officers who only allow him to leave after he shows them his photos of the flowers. What he doesn't know is that later that night, police officers would search his Facebook profile and find posts expressing support for organizing against fascism. This photographer, too, is placed on a watch list.

Though these scenarios may read like scenes from a dystopian novel, they are actual instances of surveillance by the Austin Regional Intelligence Center (ARIC), Central Texas' regional law enforcement "fusion center."

ARIC claims that its mission is about protecting the public from "criminal and terrorist activity." Documents revealed to the public through a 2020 BlueLeaks hack of ARIC's system exposing incidents like the ones narrated above proved that its net is much wider. From surveilling online cultural events and student protests to sharing information mined from residents' utility accounts, Facebook profiles, and license plate reader technology with agencies like Immigration and Customs Enforcement, ARIC collects and disseminates vast quantities of data about Austin residents with minimal limitations or oversight.





ARIC also claims in its mission that it exists to “detect and prevent” this “criminal and terrorist activity,” reminiscent of the high-tech “crime prevention” infrastructure once imagined as a warning to future societies regarding the dangers of surveillance in the pages of sci-fi works such as 1984 and Minority Report. These high tech surveillance and data sharing networks that seek to preemptively monitor and profile people’s behavior and whereabouts are no longer confined to fiction, but are increasingly a reality in many Black, brown, and poor neighborhoods.

This report lays out the technology ARIC uses to carry out its surveillance and data sharing, the kind of information it knows about us, the corporations and law enforcement agencies involved, and how this infrastructure harms some of Austin’s most vulnerable community members.

Between ARIC’s wide net, intrusive technology, and data sharing with a massive network of government agencies leading to increased surveillance and arrest, the ARIC fusion center certainly has the core elements of Orwell’s Big Brother.

Accordingly, we find that it is impossible to maintain this surveillance and data sharing infrastructure without violating Austinites’ fundamental safety and civil liberties. Its existence threatens all residents’ rights to privacy, freedom of speech and movement. It subjects especially Black and immigrant Austinites to criminalization, arrest, and deportation.

At a moment when Austin is reconsidering its budget priorities and reimagining safety, Austin City Council must move away from funding surveillance and data sharing that threaten residents’ rights and safety; instead, the city should invest in fundamental safeguards to those rights. To prevent the expansion of harmful technology and data sharing, Austin must refrain from accepting any additional funding for surveillance and data sharing, and invest instead in a mandatory Equity review prior to consideration of procurements, grants, and council agenda items, as recommended by the Reimagine Public Safety Task Force. The city must also invest in immigrant legal defense through the Travis County Public Defender’s Office to keep Austin families together and offset the harm ARIC has already enacted on immigrant community members.

KEY FINDINGS

ARIC conducts invasive surveillance on a wide array of Austin residents through a web of high-tech surveillance and data sharing contracts as well as in-person monitoring.

- ARIC contracts with corporations that collect, catalogue, and disseminate information of Austin residents with at least 20 local law enforcement agencies, in addition to state and federal agencies. These companies have included Accurint - LexisNexis, Carfax for Police, Dataminr, Justice Exchange, APPRISS, LEARN (Vigilant Solutions), Real-Comp Data & Marketing, Whooster, and TLOxp TransUnion.
- ARIC has trained 1,400 “threat liaison officers,” including more than 300 private citizens, who report “suspicious activity” that is then shared across the network. These informants have targeted activities including a protest by Bee Cave high schoolers and a “Middle Eastern” person mailing a package of toys to Lebanon.
- A BlueLeaks hack of ARIC’s system revealed that throughout the summer of 2020, ARIC frequently surveilled Black Lives Matter demonstrations, celebrations, and even a virtual Juneteenth festival.

ARIC uses city resources to share personal information of vulnerable Austin residents—including students and immigrants—with federal agencies, placing them at greater risk of arrest, detention, and deportation.

- APD accesses and shares Austin’s city utility billing information (Austin Energy) through ARIC. APD shared at least 141 utility reports of Austin residents from Austin Energy or Water with ICE since 2019. Austin Energy recently revoked ARIC’s access to its utility database. However, ARIC’s new contract with LexisNexis Real Time may allow it to access the same utilities data.
- From 2016-2020, APD contracted with Vigilant Solutions, one of the nation’s largest data-sharing networks that has long supplied ICE with license plate data, enabling the agency to track the current and past locations of billions of people. Vigilant license plate and location data of Austin residents was shared through ARIC, further opening the door to ICE accessing this sensitive information. Although APD no longer contracts with Vigilant (as of December 2020), ARIC was pursuing a LexisNexis Real Time contract, which itself would contain Vigilant data.
- ARIC’s data sharing with local schools and community colleges enabled the Austin Independent School District (AISD) Police Department and ICE to profile and target noncitizen students and students of color based on arbitrary determinations of gang affiliation. APD and ICE’s Homeland Security Investigations maintain data-sharing agreements with TXGANGS, the state gang database that obtains gang “confirmation” from APD and AISD. Determinations of gang membership by AISD exceeded over 300 in the last four years.

ARIC has refused to abide by even the weak oversight mechanisms and civil liberty protections proscribed in its own policy.

- Although its policy supposedly requires a “criminal nexus” before storing or sharing information about someone, ARIC continues to assume that noncitizen status is indicative of criminal activity, placing immigrants at greater risk of ICE detention and deportation. Until recently, ARIC shared information with ICE when provided with only a person’s A-number, a registration number provided to all non-citizens. ARIC’s current practice does not require there to be any criminal record or charge whatsoever before sharing someone’s information with ICE.
- ARIC’s interlocal agreement says it will undergo external audits subject to review by the City of Austin’s Public Safety Commission. However, the Commission has received only one such audit — a two page, non-substantive review of a 2014 “exchange” between ARIC and its counterpart fusion center in El Paso. In 2018, APD told the Public Safety Commission Chair that the Commission would no longer receive audits.
- The ARIC interlocal agreement calls for a Privacy Policy Advisory Committee of five members, including a community advocate selected by the City of Austin, to “review the Privacy Policy annually to ensure safeguards, and sanctions are in place to protect personal information.” Despite this, in March 2018, APD admitted that the Privacy Committee had not met for two years and had no meetings scheduled in 2018. The Privacy Committee also did not produce annual reports in these years.

RECOMMENDATIONS

1. Move funding away from ARIC and other surveillance and data sharing infrastructures.
2. Refrain from accepting any additional grant funding for surveillance and data sharing.
3. Invest in a mandatory Equity Review prior to consideration of city procurements, grants, and council agenda items related to public safety, as recommended by the Reimagine Public Safety Task Force.
4. Invest in immigrant legal defense through the Travis County Public Defender’s Office.

INTRODUCTION

"ARIC HAS A LONG HISTORY OF SURVEILLANCE OF ACTIVISTS, IMMIGRANTS, AND OTHER AUSTIN RESIDENTS."

The Austin Regional Intelligence Center ("ARIC") was created in 2010 and is one of eight Department of Homeland Security fusion centers in Texas. Covering the 10-county area surrounding Austin and including at least 20 local law enforcement agencies, ARIC is headquartered at and overseen by a designee of the Austin Police Department ("APD").

ARIC has a long history of surveillance of activists, immigrants, and other Austin residents. The center trains "threat liaison officers" — both area law enforcement agents and more than 300 private citizens — to file suspicious activity reports that are shared across the network and have targeted activities including a protest by Bee Caves high schoolers and a "Middle Eastern" person mailing a package of toys to Lebanon.

ARIC has also come under increasing scrutiny for its use of databases and broad surveillance technology that collect a wide variety of information on Austin-area residents, including license plates, utility records, driver's license records, and school incident reports. ARIC distributes this information to other local and federal agencies, including Immigration and Customs Enforcement (ICE), raising alarms that it increases exposure of Austin area residents to deportation while also subjecting all Austinites to unprecedented levels of police surveillance in their daily lives. Unfortunately, ARIC's continuing operations are insulated from any public oversight; accountability and oversight mechanisms are, at the very least, insufficient and ineffective.



**ARIC AND OTHER
INVASIVE
SURVEILLANCE AND
INFORMATION
SHARING
PROGRAMS
THREATEN THE
SAFETY OF SOME
OF AUSTIN'S MOST
VULNERABLE
RESIDENTS.**

ARIC's interlocal agreement says it will undergo external audits subject to review by the City of Austin's Public Safety Commission.¹ However, the Commission has received only one such audit — a two-page, non-substantive review of a 2014 “exchange” between ARIC and its counterpart fusion center in El Paso. In 2018, APD told Public Safety Commission Chair Rebecca Weber that the Commission would no longer receive audits.

In August 2020, following the national reckoning over police killings of George Floyd in Minneapolis and Mike Ramos and Javier Ambler in Austin, the Austin City Council put ARIC's \$2 million budget into the Reimagine Fund,² part of a broader Reimagining Public Safety process in Austin. The Reimagine Fund was given one year to consider whether the funds could be better used for another public safety purpose.

The Austin City Council will consider its 2021-2022 budget over the coming months. In May, Governor Abbott signed into law HB 1900 which punishes large Texas cities that reduce their police budgets below 2019 levels.³ It is not yet fully clear how the implementation of HB 1900 will impact Austin's budget.

What remains clear is that ARIC and other invasive surveillance and information sharing programs threaten the safety of some of Austin's most vulnerable residents. Instead of continuing to fund ARIC's information collection and surveillance efforts, we recommend the city transfer funds away from ARIC and towards initiatives, including immigrant legal services through the Public Defender's Office and a mandatory Equity Office oversight process prior to consideration of city procurement, grants, and agenda items related to public safety, as proposed by the Reimagine Public Safety Task Force.

BACKGROUND

The Austin Regional Intelligence Center was created in December 2010 and is one of eight Department of Homeland Security Fusion Centers in Texas. It serves as an “all-crimes information analysis center” that collaborates with regional partners to “maximize” its ability to disrupt and respond to “criminal threats” in the Austin area.⁴ Primary responsibility for the operation of ARIC is in the hands of the Austin Police Department, with APD's chief serving as (or assigning) ARIC's director. ARIC's executive board consists of the five major law enforcement agencies in the Austin-Round Rock Metropolitan area.⁵ Austin further serves as the fiscal agent for ARIC and “agrees to provide office space, equipment, and supplies to carry out the administrative operation of ARIC.”⁶

1 Interlocal Cooperation Agreement for the Austin Regional Intelligence Center (ARIC), S. Nev. Counterterrorism Ctr. (last visited May 20, 2020), https://www.ci.austin.tx.us/police/downloads/aric_general_interlocal_with_council_changes_060910.pdf.

2. Rebeca Flores, Austin's new budget starts Oct. 1. What does that mean for APD?, KVUE (Oct. 1, 2020),

<https://www.kvue.com/article/news/local/austin-police-budget-cuts-city-council/269-380a6db1-b07e-4396-8db5-aaa5d8ea2dbb>.

3. Audrey McGlinchey, Abbott Signs Into Law Bill Penalizing Texas Cities That Cut Police Funding, KUT (May 28, 2021), <https://www.kut.org/crime-justice/2021-05-28/bill-penalizing-texas-cities-that-cut-funding-for-police-heads-to-governors-desk>

4. John Anderson, *ARIC and Privacy: 'Unconstitutional on its Face,'* Austin Chron. (Aug. 29, 2014), <https://www.austinchronicle.com/news/2014-08-29/aric-and-privacy/>.

5. Interlocal Cooperation Agreement for the Austin Regional Intelligence Center (ARIC), S. Nev. Counterterrorism Ctr. (last visited May 20, 2020), https://www.ci.austin.tx.us/police/downloads/aric_general_interlocal_with_council_changes_060910.pdf.

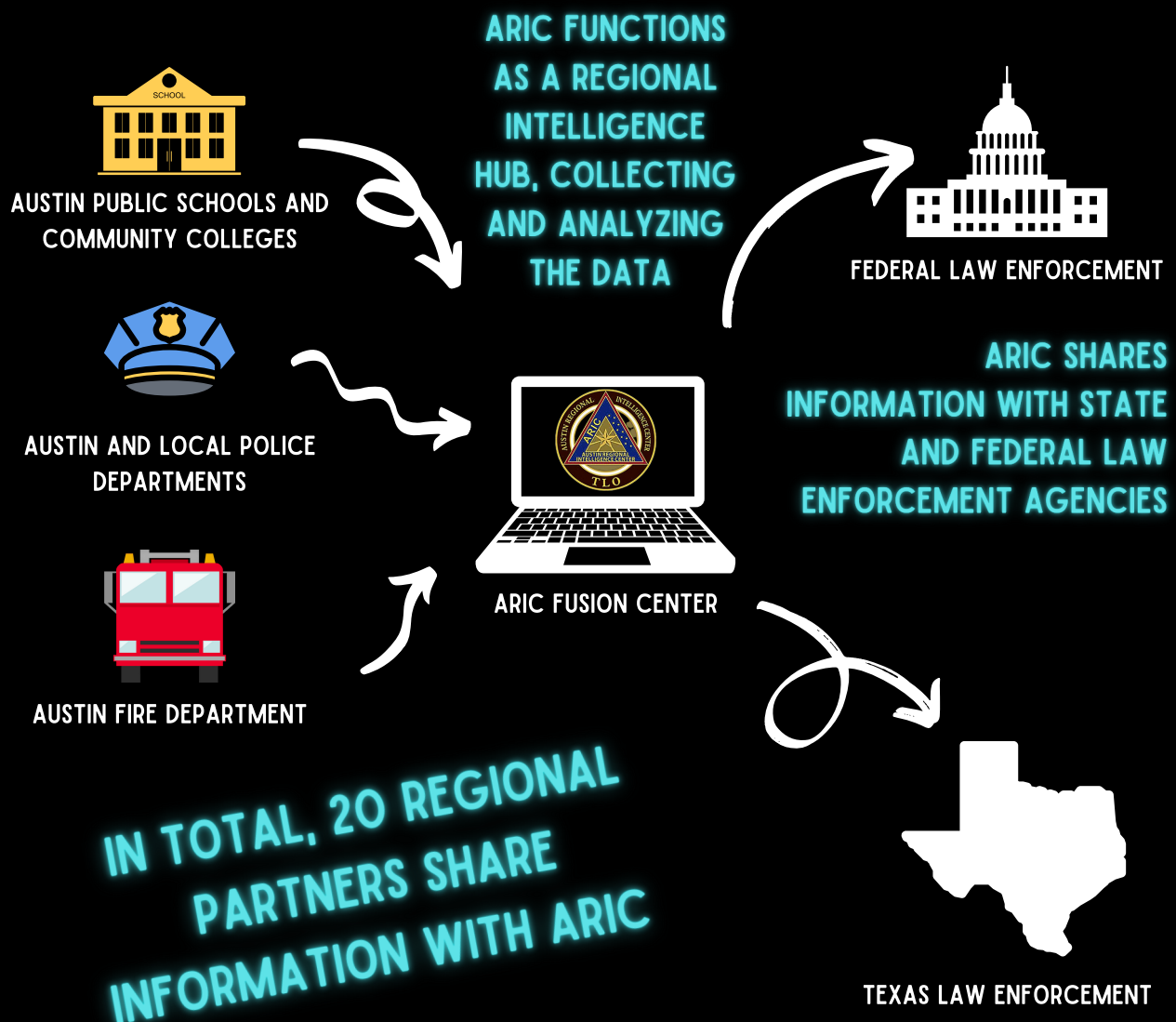
6. *Id.*

ARIC's membership now includes 20 law enforcement agencies in the 10 counties surrounding Austin, including Bastrop, Blanco, Burnet, Caldwell, Fayette, Hays, Lee, Llano, Travis, and Williamson counties. ARIC "partner agencies" include city police departments and county Sheriff's offices, the Austin Fire Department, and five school district, university, and community college police departments.⁷

ARIC functions as a regional intelligence hub, collecting and analyzing data, research, and expertise from regional partners in the Austin area. ARIC partner agencies' primary goal is to collect and share information across databases. These agencies, along with government databases, provide information including, but not limited to the following: booking photos, incarceration reports, police reports, utility reports, vehicle registration information, financial records, driver's license reports, and school incident reports.

7. Austin Regional Intelligence Center, austintexas.gov (last visited May 20, 2020), <https://www.austintexas.gov/department/austin-regional-intelligence-center>.

ARIC'S SURVEILLANCE NETWORK



ARIC EVADES COMMUNITY ACCOUNTABILITY

ARIC's charter says the fusion center "shall establish both internal and external audit functions prior to ARIC becoming operational" and that the "external audit function process will be subject to review by the City of Austin Public Safety Commission."⁸ The Public Safety Commission has a written record of one peer-to-peer exchange with the El Paso Fusion Center known as MATRIX from 2014. However, the report provides little in the way of substantive information beyond noting that the exchange between the agencies was "very productive" and that the agencies both operate under Texas law and used similar software at the time. The two-page report concludes by saying "the comparison in fusion center focus and activities between the two centers and how they each address privacy, civil rights, and civil liberties fostered great discussion of each fusion center's operations and the application of its privacy policies."⁹

When Public Safety Commission Chair Rebecca Webber inquired about whether the Commission would receive future audits, Assistant Police Chief Chris McIlvain told her that City of Austin attorney Cary Grace had determined there was "no ongoing obligation by the Public Safety Commission."¹⁰ While a June 2015 ARIC presentation to the Public Safety Commission mentioned a peer-to-peer review with the Boston Fusion Center, the Public Safety Commission received no written materials on this review, leaving ARIC without formal public oversight mechanisms.

Similarly, the interlocal agreement calls for a Privacy Policy Advisory Committee of five members, including a community advocate selected by the City of Austin, to "review the Privacy Policy annually to ensure safeguards and sanctions are in place to protect personal information."¹¹ In June 2017, community advocate Greg Foster resigned his position because his family was moving out of the city.¹² In APD emails sent to Public Safety Commission Chair Rebecca Webber in March 2018, APD admits that the Privacy Committee had not met for two years and had no meetings scheduled in 2018. The Privacy Committee also did not produce annual reports in these years.¹³

Peter Steffensen, a lawyer with the Texas Civil Rights Project, was appointed to the privacy committee in 2018.¹⁴ Steffensen proposed changes that were ultimately adopted to allow the privacy committee to provide comments before new technology contracts were signed. Steffensen raised concerns about ARIC's 2019 contract renewal with Vigilant Solutions that, in addition to providing access to its license plate reader database, would also explicitly give APD access to Vigilant's facial recognition software.¹⁵

8. Austin Regional Intelligence Center, austintexas.gov (last visited May 20, 2020), <https://www.austintexas.gov/department/austin-regional-intelligence-center>.

9. DHS/DOJ Fusion Process Technical Assistance Program and Services, Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise—Peer-to-Peer Exchange at the Austin Regional Intelligence Center, January 22, 2014.

10. Email from Chris McIlvain to Rebecca Webber, April 19, 2018. Acquired from Rebecca Webber, July 2, 2021.

11. Interlocal Cooperation Agreement for the Austin Regional Intelligence Center (ARIC), S. Nev. Counterterrorism Ctr. (last visited May 20, 2020), https://www.ci.austin.tx.us/police/downloads/aric_general_interlocal_with_council_changes_060910.pdf.

12. Comments of Gregory Foster, City of Austin Community Advocate Appointee, to the Public Safety Commission Meeting, June 5, 2017.

13. Email from APD Assistant Chief Troy Gay to Rebecca Webber, March 12, 2018.

14. Austin Police Department, Staff Response to Resolution No. 20180920-063, December 17, 2018.



<http://www.austintexas.gov/edims/pio/document.cfm?id=312674> accessed July 5, 2021.

15. Peter Steffensen email to Rebecca Webber, June 11, 2019.





ARIC SHARES PERSONAL DATA WITH APD

ARIC has a history of sharing personal, sensitive information with the Austin Police Department, often through contracts with commercial databases or with city agencies. After Grassroots Leadership requested information about the extent of APD's relationship with ARIC, they discovered that APD previously accessed Austin's city utility billing information (Austin Energy) through ARIC.¹⁶

 CITY OF AUSTIN Utility Customer Care & Billing System ACCESS REQUEST AND AGREEMENT <i>- City of Austin Employee -</i> 	
Email completed form with signatures to: AE.CCTraining@austinenergy.com	
Full Legal Name: Ryan W [REDACTED]	City E-Mail Address: ryan.w [REDACTED]@austintexas.gov
Job Title: Detective	Telephone: (512) 974-[REDACTED]
City Dept: Austin Police Department	Network Username/ID: ausps/ap3590
Describe business need and role: Used in intelligence gathering in support of the ARIC mission	
I hereby acknowledge and agree that information accessed through the City of Austin's Utility Customer Care & Billing system may be confidential, proprietary, or trade secrets of the City.	

Austin Energy recently revoked ARIC's access to its utility database for gas and electric usage—information that law enforcement had passed along to ICE in the past.¹⁷ Unfortunately, this revocation is almost meaningless if ARIC's new contract with LexisNexis Real Time would allow it to access this same utilities data.

 CITY OF AUSTIN Utility Customer Care & Billing System ACCESS REQUEST AND AGREEMENT <i>- City of Austin Employee -</i> 	
Email completed form with signatures to: AE.CCTraining@austinenergy.com	
Full Legal Name: Justin W [REDACTED]	City E-Mail Address: justin.[REDACTED]@austintexas.gov
Job Title: Strategic Intelligence Officer	Telephone: (512) 974-[REDACTED]
City Dept: Austin Police Department	Network Username/ID: 7050
Describe business need and role: Newly assigned officer to the regional law enforcement intelligence center (ARIC)	

16. Documents on file with Grassroots Leadership. Acquired through public record act requests to the Austin Police Department in 2020.
 17. Resolution 20180614-074 - Immigration Enforcement Quarterly Report #6: April 1st -June 30th, 2020 Report. Date: July 31st 2020.
http://www.austintexas.gov/sites/default/files/files/Resolution%2074%20Q2_Apr-Jun%202020_070820.pdf Accessed online June 22, 2021.

ARIC'S SPYWARE:

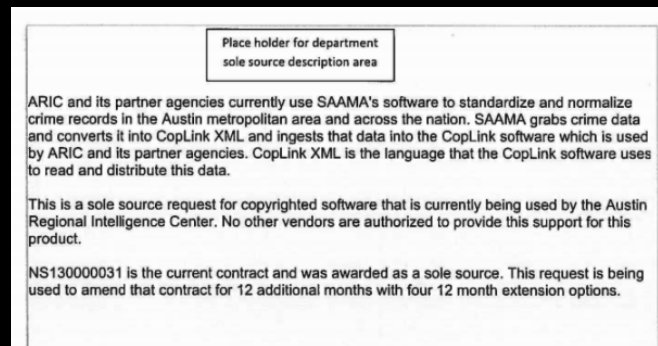
ARIC CONTRACTS WITH CORPORATIONS THAT COLLECT, CATALOGUE, AND DISSEMINATE INFORMATION OF AUSTIN RESIDENTS.

These companies have included Accurant - LexisNexis, Carfax for Police, Dataminr, Justice Exchange, APPRISS, LEARN (Vigilant Solutions¹⁸), Real-Comp Data & Marketing, Whooster, and TLOxp TransUnion. These contracts enable ARIC to surveil people who find themselves in any of the counties policed by ARIC partner agencies, including community organizers and activists convening virtual events. In short, data acquired by these companies that APD inputs into these tech platforms can be accessed by any other law enforcement agencies with access to those platforms. It is unclear where the data travels, how it is being used and its role in criminalizing or deporting Austin's communities of color.

Through ARIC, aggregated data from these databases and on-the-ground surveillance by law enforcement as well as civilian informants is distributed in real time to Texas law enforcement agencies and Immigration and Customs Enforcement ("ICE").¹⁹

The following are some of the Austin Police Department (APD) and the Austin Regional Intelligence Center (ARIC) surveillance contracts. Together, they facilitate local law enforcement's real-time information on residents' social media accounts, provide law enforcement access to non-criminal databases like phone records, and

allow for the sharing of information with federal agencies including Immigration and Customs Enforcement (ICE).²⁰



COPLINK

APD has a contract with California company Forensic Logic for its Coplink software. The software is used for information sharing between ARIC member agencies. APD has a contract with options that began in 2018 and runs through 2023 for a total of \$655,583. Forensic Logic's Coplink data sharing platform is hosted by Microsoft Azure and the Nlets national law enforcement facility in Phoenix. Coplink and Nlets allow for data sharing en masse between local and federal law enforcement, invading people's privacy and granting federal agents from the FBI and ICE access to personal information from local sources.²¹

18. Mary Tuma, ICE Strikes Deal with Surveillance Firm, Austin Chronicle (Mar. 2, 2018), <https://www.austinchronicle.com/news/2018-03-02/ice-strikes-deal-with-surveillance-firm/>.

19. Id. Brant Bingamon, ARIC Trainings Teach Cops and Informants Junk Science, Austin Chron. (Aug. 28, 2020), <https://www.austinchronicle.com/news/2020-08-28/aric-trainings-teach-cops-and-informants-junk-science/>.

20. Austin's Big Secret: How Big Tech and Surveillance Are Increasing Policing, August 2020.

https://grassrootsleadership.org/sites/default/files/reports/austins_big_secret_how_big_tech_and_surveillance_are_increasing_policing.pdf

21. Contract on file with Grassroots Leadership.

APD has the ability to cancel this contract by providing 30 days notice. In addition, Austin contracted with SAAMA Technologies to create software products to collect, analyze and modify crime data acquired on Austin residents for COPLINK's software. SAAMA products were estimated to cost approximately \$96,000/yr starting in 2018, for a total amount of \$491,000.²²

LEXIS NEXIS/ACCURINT

ARIC and APD also have access to LexisNexis' Accurint, a comprehensive database with information such as personal phone records, addresses, and "public records that would ordinarily take days to collect." The City of Austin has a \$456,000 contract for Accurint, and APD makes frequent contractual payments to LexisNexis. APD gets this personal data from commercial sources that individuals do not normally grant their consent to share with law enforcement—meaning law enforcement agencies with access to ARIC data, including ICE, collect detailed personal records on individuals not related to criminal records.²³



APPRISS SAFETY

Service Agreement Renewal Quote

Date: October 5, 2018

Customer Name: City of Austin
Attn:

Address: 715 E. 8th Street
Austin, TX 78701-3397

Service(s): JusticeXchange (referred to as 'JX' or Justice Intelligence)

Original Service Agreement Date: December 8, 2016

Last Service Agreement Date: December 1, 2017

Service Agreement Renewal Date: October 1, 2018

Service Agreement Renewal Term: 60 months

Next Service Agreement Renewal Date: October 1, 2023

Description: JusticeXchange (also known as Justice Intelligence) is a secure web portal that provides access to an instant up-to-date database of current and historical booking information including biographical information, charges, and photographs of offenders.

Pricing for this renewal includes thirty (30) JusticeXchange (JX) Licenses for 5 years.

Service Pricing:

Year	Number of Active JX Licenses	Annual Total
Year 1 (10/1/18-9/30/19)	30 Licenses	\$30,600.00
Year 2 (10/1/19-9/30/20)	30 Licenses	\$30,600.00
Year 3 (10/1/20-9/30/21)	30 Licenses	\$31,824.00
Year 4 (10/1/21-9/30/22)	30 Licenses	\$33,096.96
Year 5 (10/1/22-9/30/23)	30 Licenses	\$34,420.84

JX/APPRISS

Justice XChange is an investigative database and network that offers ARIC and its partner agencies "real-time" access to Austin's booking information, which includes photos and biographical information of anyone arrested by APD. This booking information is pooled into a booking data bank collected from other cities in the United States, estimated at 135 million booking photos from 2,900 jails and prisons. The five-year contract, which began in October 2018, will cost Austin \$160,541.80. Moreover, all the information acquired in Appriss' databases are "owned" by Appriss, not the City of Austin.²⁴

DATAMINR

ARIC has access to Dataminr, which provides real-time alerts from social media and public data sources. Dataminr helped law enforcement monitor Black Lives Matter protests across the country in 2020, relaying Tweets and other social media information to police. Dataminr has received funding from both Twitter and the CIA's venture capital arm, In-Q-Tel.²⁵

22. Austin's Big Secret: How Big Tech and Surveillance Are Increasing Policing. August 2020.

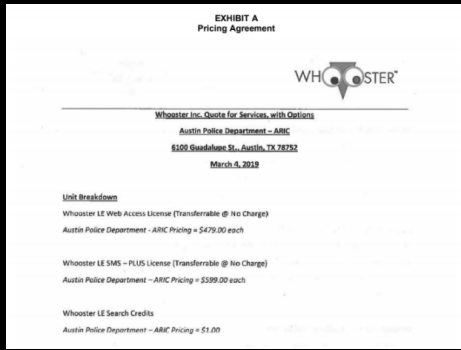
https://grassrootsleadership.org/sites/default/files/reports/austins_big_secret_how_big_tech_and_surveillance_are_increasing_policing.pdf

23. *Id.*

24. *Id.*

25. *Id.*

ARIC'S SPYWARE CONT.



WHOOSTER

In 2019, the City of Austin signed a contract worth up to \$133,990 for four years with Whooster, Inc. for APD and ARIC's use of its Investigative Database System.²⁶ Whooster is a Buda, Texas based company that provides "real-time" public and private data through a web-accessed portal to law enforcement agencies.²⁷ Whooster also contracts with the DHS's Customs and Border Protection for "targeting, vetting and analytic requirements and not available within or through other offerings" including "social media analytics" and "real time actionable intelligence related to persons of interest."²⁸

26. City of Austin Contract with Whooster, Inc dated March 20, 2019. Received in an open records request, and available online at <http://www.austintexas.gov/edims/document.cfm?id=318743>

27. Whooster.com, accessed June 21, 2022.

28. U.S. Customs and Border Protection Justification for a Brand Name Exception to Fair Opportunity (JEFO) - FAR 16.505(a)(4) Exceeding the SAT. Contract on file with authors.

29. See *Austin Regional Intelligence Center - Privacy Policy*, austintexas.gov § C.1-3 (Sept. 2015) [hereinafter ARIC Privacy Policy], http://austintexas.gov/sites/default/files/files/Police/ARIC_PRIVACY_POLICY_Sept_2015_2_.pdf (allowing ARIC to seek information that is "useful in crime analysis or in the administration of justice and public safety (including topical searches of open source information)"); John Anderson, *Is ARIC Still Watching?*, *Austin Chronicle* (Dec. 11, 2020), <https://www.austinchronicle.com/news/2020-12-11/is-aric-still-watching/>.

30. See *Austin Regional Intelligence Center - Privacy Policy*, austintexas.gov (Sept. 2015), http://austintexas.gov/sites/default/files/files/Police/ARIC_PRIVACY_POLICY_Sept_2015_2_.pdf.



ARIC'S TOLL ON AUSTIN COMMUNITIES

ARIC's reach is exceptionally broad—targeting everyday social justice organizers, students, immigrants, and people of color. Its privacy policy employs sweeping language that supports broad operational guidelines, allowing the collection of any information that may be "useful" to administer justice and public safety.²⁹ The term "useful" is not defined anywhere within the privacy policy and thus grants ARIC considerable discretion in aggregating information.³⁰ The fusion center's surveillance then enables the federal government and local law enforcement to weaponize everyday information—including utility data, vehicle registration information, cell phone location data, and other personal information that target vulnerable communities for enforcement. These practices lead to increased arrests by ICE and the Austin police.

These arrests have harmful financial and mental health impacts and can often lead to family separation, incarceration, immigration detention, and deportation.³¹

ARIC has also trained 1,400 threat liaison officers (TLOs), including both law enforcement officers and more than 300 private citizens who report “suspicious activity” that is then shared across the network.³² In many cases, these activities have been entirely lawful, including a demonstration organized by Bee Caves high school students³³ or the mailing of a package of toys to Lebanon by a person described as “Middle Eastern.” Suspicious activity reports by TLOs were filed against “Middle Eastern” people 39 times since 2016.³⁴

ARIC has further been criticized for training officers in “junk science” interrogation techniques including a “walking polygraph” test known as Scientific Content Analysis (SCAN) that includes handwriting analysis.³⁵ Scientists have found “no empirical support” that SCAN is effective at identifying whether suspects are telling the truth.³⁶

A BLUELEAKS HACK OF ARIC’S SYSTEM REVEALED THAT THROUGHOUT THE SUMMER OF 2020, ARIC FREQUENTLY SURVEILLED BLACK LIVES MATTER DEMONSTRATIONS, CELEBRATIONS, AND EVEN A VIRTUAL JUNETEENTH FESTIVAL.

TARGETING ACTIVISTS, INCLUDING BLACK LIVES MATTER

Throughout its history, ARIC has monitored activists in many areas of social justice work, including Black Lives Matter organizers, immigrants’ rights activists,³⁷ and high school and college students monitored through ARIC’s relationships with school police departments. Although ARIC claims that it “safeguards” First Amendment rights by only reporting on activities where “incitement rhetoric” could instigate acts of violence, it has repeatedly monitored events in the absence of such rhetoric.³⁸

31. Survey of impacted community members by Austin Reimagine Public Safety Task Force Patrol and Surveillance Working Group. <https://austintexas.gov/sites/default/files/files/RPS-TF%20Patrol%20%26%20Surveillance%20Recommendations.pdf>

32. Brandon Mulder, *Hackers Leaked Nearly 2,000 Incidents of Austin Surveillance. Here’s What They Found*, Austin Amer. Statesmen (Feb. 7 2021, 9:48 AM), <https://www.statesman.com/story/news/2021/02/07/austin-police-surveillance-operation-leaked-documents-raise-questions/4221649001/>.

33. *Id.*

34. John Anderson, *Austin Regional Intelligence Center’s Secret Informants Show How Profiling Works*, Austin Chron. (Aug. 7, 2020),

<https://www.austinchronicle.com/news/2020-08-07/austin-regional-intelligence-centers-secret-informants-show-how-profiling-works/>.

35. Brant Bingamon, *ARIC Trainings Teach Cops and Informants Junk Science*, Austin Chron. (Aug. 28, 2020), <https://www.austinchronicle.com/news/2020-08-28/alic-trainings-teach-cops-and-informants-junk-science/>.

36. *Id.*

37. *Id.*

38. *Id.* It should be noted that ARIC is usually lacking “probable cause to suspect actual criminal activity” which also raises Fourth Amendment concerns. Anderson, *supra* note 2.

A BlueLeaks hack of ARIC's system revealed that throughout the summer of 2020, ARIC frequently surveilled Black Lives Matter demonstrations, celebrations, and even a virtual Juneteenth festival.³⁹ Of the 24 events ARIC monitored during this time period, 23 were consistently advertised as peaceful.⁴⁰ Other events ARIC has surveilled include Occupy Wall Street demonstrations, animal rights events, Women's Marches, pro-impeachment rallies, pro-choice protests, among many others.⁴¹

INCREASING RISK OF ICE ENFORCEMENT ACTIVITY IN AUSTIN

Included in ARIC's privacy policy is permission to gather information that has a potential "criminal nexus."⁴² However, the policy includes no specific definition of criminal nexus, which further widens ARIC's discretion to surveil people who present no known threat to public safety.⁴³ Abuse of this discretion is particularly common in ARIC's surveillance of non-citizens whom it reports to ICE. According to statements made by an APD officer at a meeting with advocates in early 2021, APD was, until recently, sharing information with ICE after the agency provided only an "A-number" or "alien number." An "A-number" is an individualized registration number assigned to every noncitizen in the United States, and is not sufficient "evidence" of criminal nexus.⁴⁴ ICE is a civil agency and is unable to produce an internal criminal case number. The officer also stated that they now ask ICE to provide both the identification number and the number of the criminal code they are investigating. However, criminal nexus should be triggered upon the filing of criminal charges. It is also worth noting that even if ICE did provide ARIC with a criminal case number from another federal agency, the federal criminal offenses that APD mentioned ICE was investigating were 8 U.S.C. §1325 and 8U.S.C. §1326, unauthorized entry and re-entry, which are offenses solely based on a person's immigration status and presence in the U.S. Status offenses like 8 U.S.C. §1325 and 1326 are federal, not local, offenses and amenable to ICE's expertise, not APD. It is troubling that APD continues to assist ICE with investigation of status offenses. Moreover, it is clear that ARIC continues to assume that noncitizen status is indicative of criminal activity. This assumption exposes all noncitizens to surveillance, risking their potential detention and deportation.

ARIC has also turned over a disturbing amount of information about Austin residents to ICE. APD shared at least 141 utility reports of Austin residents from Austin Energy or Water with ICE since 2019, and at least four APD ARIC intelligence officers have full user access to the city's utility database. APD has queried utility reports to share that information (which could include home addresses and financial information) with ICE, thus making it easier for ICE to arrest Austin residents in their homes. ARIC has shared at least one school incident report from the Austin Independent School District with ICE and complied with at least 927 requests for Austin resident information from ICE since 2017.⁴⁵

39. Anderson, *supra* note 12.

40. *Id.*

41. *Id.*

42. ARIC Privacy Policy, *supra* note 8, at § C.2.

43. *See id.*

44. APD statement at January 4, 2021 Freedom Cities meeting. Recording on file with Grassroots Leadership.

45. Austin's Big Secret: How Big Tech and Surveillance are Increased Policing, https://notechforice.com/wp-content/uploads/2020/08/Austins-Big-Secret_-How-Big-Tech-and-Surveillance-Are-Increasing-Policing_v2.pdf (last visited May 20, 2021).



ARIC FACILITATES SURVEILLANCE AND CRIMINALIZATION OF STUDENTS AND YOUTH

ARIC's data sharing with local schools and community colleges also enabled the Austin Independent School District ("AISD") police department and ICE to profile and target noncitizen students and students of color based on arbitrary determinations of gang affiliation. In the past, AISD—a regional partner of ARIC—employed over 80 school police officers, some who worked on the juvenile gang task force. Determinations of gang membership by AISD exceeded over 300 in the last four years.⁴⁶ APD and ICE's Homeland Security Investigations maintain data sharing agreements with TXGANGS, the state gang database that obtains gang "confirmation" from APD and AISD.⁴⁷ Because TXGANGS includes information from Travis County, Austin residents have been captured within the database and labeled as "gang members."⁴⁸

Advocates have long criticized gang databases for casting too wide a net and promoting racial profiling amongst law enforcement.⁴⁹ Not only have systematic and consistent inaccuracies been found in gang databases across the country, but they are known to violate the privacy rights and First Amendment rights of targeted individuals.⁵⁰ Evidence of gang affiliation may simply come from a student wearing a gang's designated colors, knowing—or being related to—someone known to be in a gang, being seen in an area gangs are known to frequent, or making "gang signs" with their hands, which are often gestures widely used in mainstream culture.⁵¹ Moreover, individuals are rarely notified of being added to the database and face substantial obstacles contesting a designation.⁵² The consequences of gang database inclusion for immigrants are particularly dire. Membership in a gang database heightens an individual's risk of being targeted by an ICE raid, detained, denied immigration relief, or deported.⁵³

46. Public Record Act Responses received on AISD gang "confirmations" using CrimeStar. On file with Grassroots Leadership (dated 9-22-2020). Now, AISD claims "no other agency" has access to the CrimeStar database which houses their gang information.

47. Public Record Act Responses received on TxGangs database entries for Travis County. On file with Grassroots Leadership (dated 10-27-2020).

48. *Id.*

49. Christie Thompson, *How ICE Uses Secret Police Databases to Arrest Immigrants*, Marshall Project (Aug. 28, 2018), <https://www.themarshallproject.org/2017/08/28/how-ice-uses-secret-police-databases-to-arrest-immigrants>.

50. See *Medrano v. Salazar*, No. 5:2019cv00549 - Document 23 (W.D. Tex. 2020) where plaintiff did not meet "gang" criteria, nor did his military "gang" constitute a gang, but was still included in a gang database. Jennifer Medina, *Gang Database Criticized for Denying Due Process May Be Used for Deportations*, N.Y. Times (Jan. 10, 2017), <https://www.nytimes.com/2017/01/10/us/gang-database-criticized-for-denying-due-process-may-be-used-for-deportations.html>; *The CalGang Criminal Intelligence System*, California State Auditor (2016), <https://www.auditor.ca.gov/pdfs/reports/2015-130.pdf>.

51. Thompson, *supra* note 22.

52. *Id.*

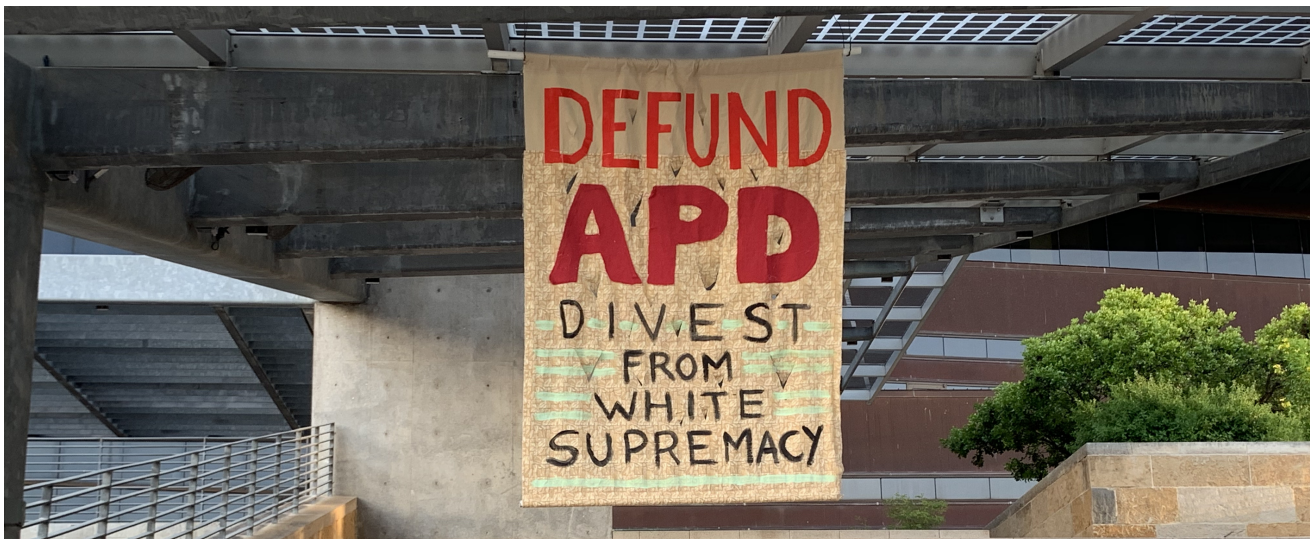
53. *Id.*

ARIC CONTINUES DATA MINING AND SURVEILLANCE DESPITE COMMUNITY-DRIVEN CHANGES

Over the past year, ARIC has phased out several contracts while expanding others. Following widespread criticism and advocacy from community organizations, APD recently phased out its contract with Vigilant Solutions, one of the U.S.'s largest data-sharing networks which had long supplied ICE with license plate data that enables the agency to track the current and past locations of billions of license plates.⁵⁴ Not only does this information present a myriad of privacy concerns for all drivers, such as revealing where an individual seeks medical care, but ICE weaponizes license plate data to locate and detain immigrants across the country.⁵⁵ APD had contracted with Vigilant since 2016 to monitor Austin residents and is known to share its data with ARIC, further opening the door to ICE accessing this sensitive information.⁵⁶

As of December 2020, ARIC was pursuing a LexisNexis Real Time contract, which itself would contain Vigilant data.⁵⁷ As such, the same information jeopardizing the privacy of all Austin residents may continue to be at ARIC and APD's fingertips.

Recent developments in ARIC's surveillance of utility reports have followed a similar pattern. Austin Energy recently revoked ARIC's access to its utility database for gas and electric usage,⁵⁸ information that law enforcement had passed along to ICE in the past. Unfortunately, this revocation is almost meaningless if ARIC's contract with LexisNexis Real Time would allow it to access this same utilities data.



54. Tuma, *supra* note 6.

55. *Id.*

56. *Id.*

57. Email exchange with Peter Steffensen, community advocate to the ARIC Privacy Policy Advisory Committee, Dec 14, 2020.

58. Resolution 20180614-074 – Immigration Enforcement Quarterly Report #6: April 1 st -June 30 th, 2020 Report Date:July 31st 2020. http://www.austintexas.gov/sites/default/files/files/Resolution%2074%20Q2_Apr-Jun%202020_070820.pdf Accessed online June 22, 2021.

CONCLUSIONS AND RECOMMENDATIONS

The Austin Regional Intelligence Center, through its use of surveillance technologies and databases, has collected a wide variety of information on Austin-area residents, including license plates, utility records, driver's license records, and school incident reports. ARIC distributes this information to other local and federal agencies, including Immigration and Customs Enforcement—increasing exposure of Austin area residents to deportation while also subjecting all Austinites to unprecedented levels of police surveillance in their daily lives.



ARIC's surveillance disproportionately harms people of color, activists, and immigrant communities with its far-reaching operational guidelines, deployment of surveillance technology, and partner agencies from which it collects and shares people's private information.⁵⁹ ARIC's expansive real-time data sharing with big tech databases and other law enforcement agencies eliminates local control and accountability over how Austin residents' private information is used; this allows the information to be weaponized in ways that make residents less safe.

Instead of continuing to fund ARIC's information collection and surveillance efforts, we recommend the City of Austin transfer funds away from ARIC. As the Austin City Council considers its 2021-2022 budget over the coming months, it is not yet fully clear how the passage of HB 1900 by the Texas legislature, its implementation, and potential litigation will impact the city's budget process. Still, we recommend that ARIC funds be redistributed towards community-benefiting initiatives, including immigrant legal services through the Public Defender's Office and a mandatory Equity Office oversight process prior to consideration of city procurements, grants, and Council agenda items pertinent to public safety, as proposed by the Reimagine Public Safety Task Force. These initiatives would begin to remedy some of the harm that ARIC has caused to vulnerable community members, as well as prevent the same threats from resurfacing through other surveillance and information sharing proposals.

59. This includes but is not limited to booking photos, incarceration reports, police reports, utility reports, vehicle registration, financial records, driver's license reports, and school incident reports.