

UNIVERSITY *of* WASHINGTON

CENTER FOR HUMAN RIGHTS

HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

WHO'S WATCHING WASHINGTON?

DANGERS OF AUTOMATED LICENSE
PLATE READERS TO IMMIGRANT
AND REPRODUCTIVE RIGHTS IN
WASHINGTON STATE



**Who's Watching Washington?
Dangers of Automated License Plate Readers to Immigrant and Reproductive Rights in
Washington State**

University of Washington
December 2022

The University of Washington Center for Human Rights is committed to interdisciplinary excellence in the education of undergraduate and graduate students in the field of human rights; promoting human rights as a core area of faculty and graduate research; and engaging productively with local, regional, national, and international organizations and policymakers to advance respect for human rights.

Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights | Facebook, Twitter: @uwchr

CONTENTS

<i>Introduction</i>	<i>4</i>
<i>ALPRs: What They Are and Why They Matter for Human Rights</i>	<i>6</i>
<i>Threats to Immigrant Rights.....</i>	<i>8</i>
<i>Threats to Reproductive Rights</i>	<i>11</i>
<i>Methods.....</i>	<i>13</i>
<i>Findings</i>	<i>15</i>
<i>Data Retention</i>	<i>15</i>
<i>Data Sharing.....</i>	<i>16</i>
<i>Transparency.....</i>	<i>19</i>
<i>Conclusion and Recommendations</i>	<i>21</i>

INTRODUCTION

In recent years, local and state governments in Washington have taken important legislative and executive action to protect vulnerable residents from rights abuses. Many of these actions, such as the so-called “sanctuary” laws of Keep Washington Working (2019) and Courts Open to All (2020) Acts, seek to protect the rights of migrants by limiting the degree to which local authorities can collaborate with civil immigration enforcement by ICE or CBP. More recently, the language of “sanctuary” has also been used in the context of the right to reproductive health care at both the state and local levels. On June 30, 2022, Governor Jay Inslee issued a directive prohibiting the Washington State Patrol from “providing any cooperation or assistance whatsoever” with efforts to investigate or prosecute those seeking access to reproductive health care in our state.¹ And some local jurisdictions have followed suit. On July 5, 2022, King County Executive Dow Constantine issued an order banning the King County Sheriff and other county agencies from providing any information or assistance with efforts to “obstruct, restrict, diminish or discourage” access to reproductive health care.² And on July 26, 2022, the Seattle City Council voted to bar local police from assisting in investigations or executing warrants issued by other jurisdictions that criminalize seeking or assisting in abortions.³

1 Governor Jay Inslee, *Directive of the Governor 22-12: Prohibiting cooperation or assistance with out-of-state abortion and other reproductive health care investigations, prosecutions or other legal actions*, June 30, 2022, [https://www.governor.wa.gov/sites/default/files/directive/22-12%20-%20Prohibiting%20assistance%20with%20interstate%20abortion%20investigations%20\(tmp\).pdf](https://www.governor.wa.gov/sites/default/files/directive/22-12%20-%20Prohibiting%20assistance%20with%20interstate%20abortion%20investigations%20(tmp).pdf)

2 County Executive Dow Constantine, *Use of Executive Branch Resource to Impede Reproductive Health Care Prohibited*, July 5, 2022, <https://kingcounty.gov/~media/elected/executive/constantine/news/documents/2022/Signed-EO-07-05-22.ashx?la=en>.

3 Sarah Grace Taylor, “Seattle police won’t make arrests

These strongly-worded directives are important statements of Washington state values. Yet research conducted in Washington and elsewhere shows that data gathered by state and local law enforcement remains accessible to both law enforcement from other states, and federal immigration enforcement agencies, through interoperable databases.⁴ ICE documents show that federal immigration agents have deliberately increased their use of digital tools in recent years in direct response to the limitations created by local policies designed to limit collaboration with federal immigration enforcement.⁵ Although it remains to be seen whether out-of-state attempts to prosecute people for seeking, or providing, access to abortions in Washington will pass legal muster,⁶

on abortion-related charges, after City Council establishes ‘sanctuary city,’” *Seattle Times*, July 26, 2022, <https://www.seattletimes.com/seattle-news/politics/seattle-police-wont-make-arrests-on-abortion-related-charges-after-city-council-establishes-sanctuary-city/>.

4 Nina Wang, et al., “American Dragnet: Data-Driven Deportation in the 21st Century,” *Center on Privacy & Technology at Georgetown Law*, May 10, 2022, <https://americandrag.net/>.

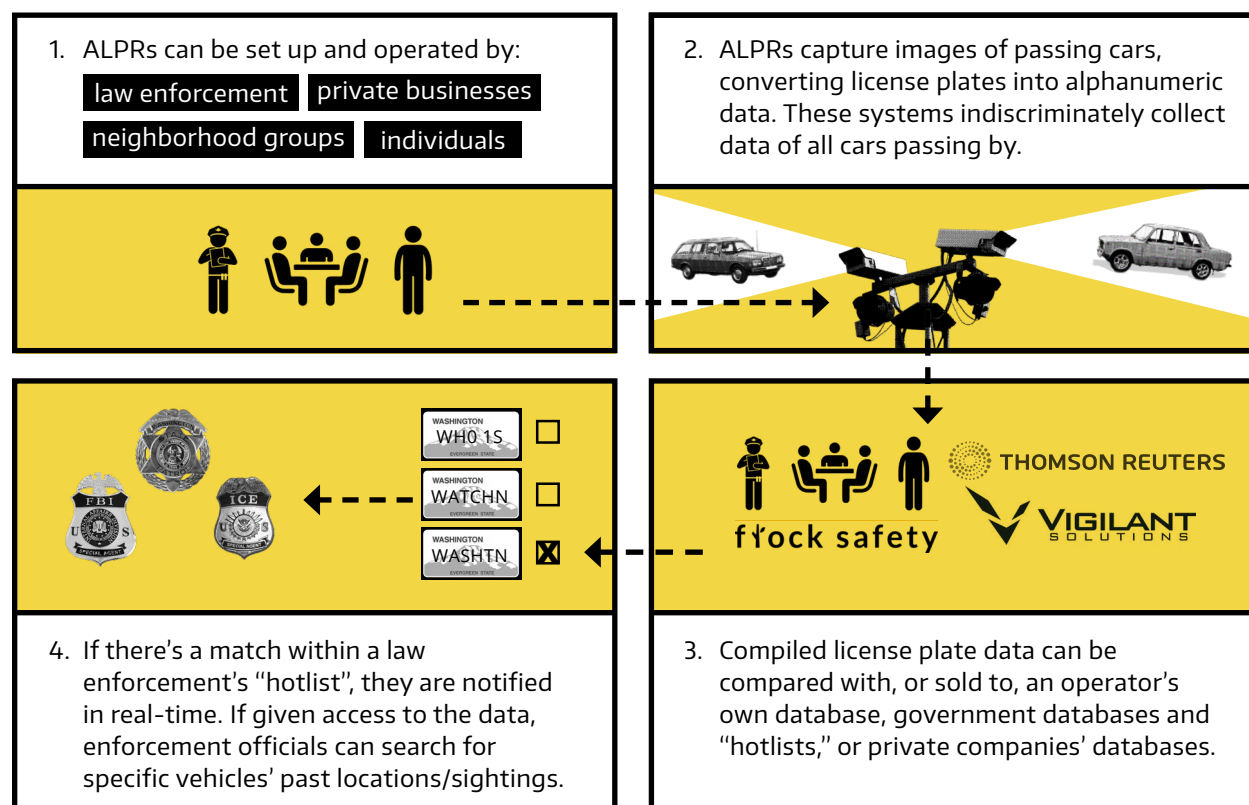
5 See, for example, Sabotaging Sanctuary. Mijente et al., “Sabotaging Sanctuary,” (Denver: Colorado Immigrant Rights Coalition, 2022), https://coloradoimmigrant.org/wp-content/uploads/2022/04/Sabotaging-Sanctuary_Final-Report_Design-4-1.pdf. The ACLU also reports that “[ICE] has been candid about contracting with LexisNexis for the purpose of side-stepping state policies.” Ana Temu Otting, “How ICE Sidesteps the Law to Find and Deport People,” *ACLU*, June 9, 2022, <https://www.aclu.org/news/immigrants-rights/how-ice-sidesteps-the-law-to-find-and-deport-people>. In a budgetary explanation as to why they wanted to contract with Appriss, the agency explained: “Due to policy or legislative changes, [ICE Enforcement and Removals Office] has experienced an increase in the number of law enforcement agencies and state or local governments that do not share information about real time incarceration of foreign-born nationals with ICE ... There would be a major operational impact on public safety without these screening tools.” Immigration and Customs Enforcement Agency, *ICE Acquisition Manual: Justification for Other Than Full and Open Competition*, June 29, 2021, <https://govtribe.com/file/government-file/p00002-ja-21-00148-competition-advocate-signed-6-dot-24-dot-21-redacted-dot-pdf>.

6 David S. Cohen, Greer Donley, and Rachel Rebouché, “The New Abortion Battleground,” *Columbia Law Review* 123 (2022), https://scholarship.law.pitt.edu/fac_articles/517.

automatic license plate recognition (ALPR) data documenting presence at abortion clinics in our state could be deployed as a powerful tool to flaunt Washington policies.

In order for Washington to live up to its promises to provide “sanctuary” for those exercising their lawful rights in Washington, our state and local governments must take steps to close the gaps in existing systems of digital surveillance. Towards this end, the UW Center for Human Rights has launched an effort to understand the practices of digital surveillance in our state and their potential to undermine access to the very rights protections our government has pledged to uphold. This report focuses on just one dimension of this multidimensional threat: the dangers posed by the misuse of automated license plate recognition technology by law enforcement agencies. Future reports will examine other digital tools.

ALPRS: WHAT THEY ARE AND WHY THEY MATTER FOR HUMAN RIGHTS



How Automated License Plate Readers work

The use of automatic license plate recognition (ALPR, also sometimes called LPR) is believed to have expanded dramatically in recent years, though due to the total lack of statewide regulation of this technology in Washington, there are no reliable estimates as to how many systems are currently in operation. ALPRs are typically more concentrated in urban settings, but are also common in rural areas;⁷ while they are used by police, municipalities also employ them for parking enforcement, and private property owners can deploy them for any desired purpose.

⁷ Thor Benson, "The Danger of License Plate Readers in Post-Roe America," *Wired*, July 7, 2022, <https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>.

In Seattle, the Police Department reported in 2018 that it operated 19 vehicles with ALPR technology;⁸ Seattle Department of Transportation reported owning 99 cameras.⁹ Each camera is capable of amassing vast numbers of license plate scans. In 2017, data from the Washington State Patrol showed that in 2017, the agency's ALPR systems recorded almost 1.5 million license plate scans.¹⁰

⁸ Seattle Police Department, "2018 Surveillance Impact Report: Automated License Plate Recognition (ALPR) (PATROL)," March 23, 2021, <http://seattle.legistar.com/View.ashx?M=F&ID=9374029&GUID=067A8F9B-6A11-44BB-9C01-6B86B7EA7980>.

⁹ Seattle Department of Transportation, "2018 Surveillance Impact Report: License Plate Readers," May 7, 2019, https://www.seattle.gov/documents/Departments/Tech/Privacy/License%20Plate%20Readers_Final%20SIR.pdf.

¹⁰ 2017 WSP Data was released to Michael Miller and

ALPR systems consist of a camera set up to capture images of passing cars, paired with software that scans the images, converting license plate numbers into alphanumeric data that is then compared against “hot lists”¹¹ of target vehicles. These “hot lists” can be compiled locally by the organization or law enforcement agency operating the ALPR reader, or obtained from others through sharing agreements. For example, in Washington state, national target data from the FBI’s National Crime Information Center (NCIC) “hot file” is made available to local law enforcement agencies through the Washington State Patrol’s ACCESS database.¹² When the ALPR reader detects a license plate whose number matches the number on a hot list – whether a locally compiled list or national database – a “hit” is generated, sending a real-time notification to law enforcement.

Because ALPRs collect data indiscriminately—all passing vehicles are scanned—the vast majority

of drivers whose information is scooped up are not associated with any public safety threat.¹³ Because the license plate numbers and the geographic locations are observable in public—in theory, anyone could notice a car driving down the street and jot down its license plate—courts have ruled that ALPR data is public information, and therefore can be collected by or handled by anyone.¹⁴

published on Muckrock. Washington State Patrol Public Records Center, *Washington Public Records Act Request: ALPR data generated by the Washington State Patrol*, August 26, 2018, <https://www.muckrock.com/foi/washington-54/alpr-data-generated-by-the-washington-state-patrol-59986/>.

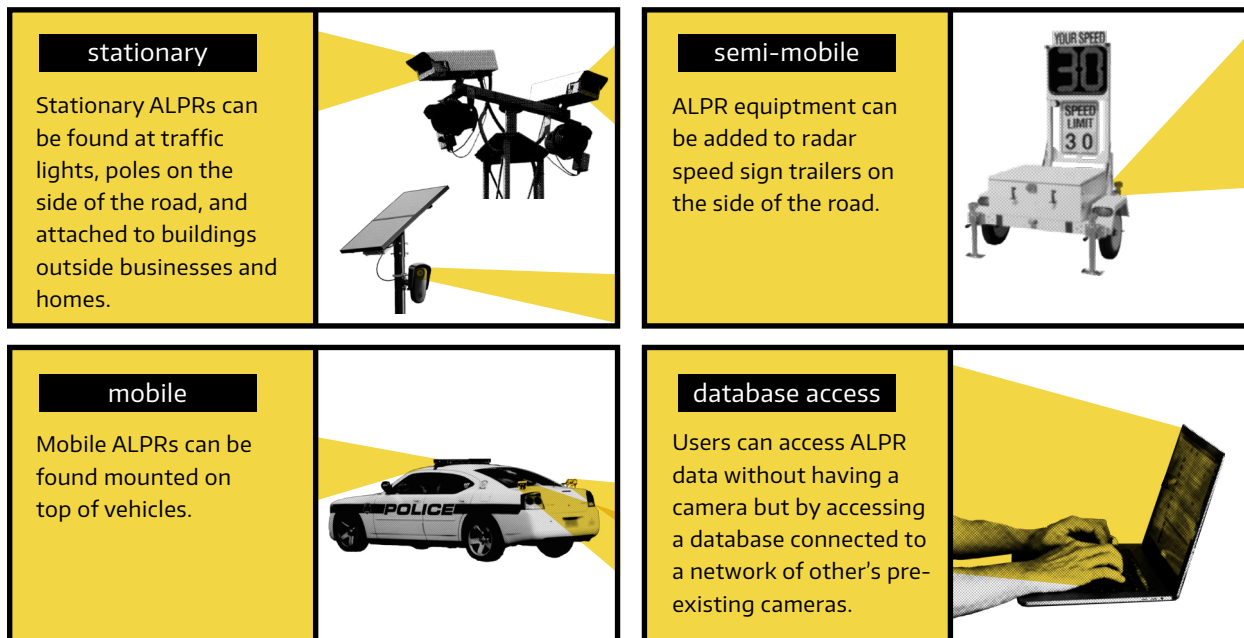
Note: data was not provided for September or October 2017, so the annual estimate was produced by averaging the monthly totals across the 10 months of data provided, producing a monthly average of 123.211 scans/month, and multiplying that figure by 12, for an estimated total of 1,479,732 scans. The same data release shows that 5 of those scans corresponded to stolen vehicles.

11 In the Washington’s Association of Sheriffs and Police Chiefs’ 2008 document laying out guidelines for ALPR use by law enforcement, it explains hot lists as follows, “An ALPR reads a plate and compares it against a database of suspect vehicles, alerting the officer to any matches. It uses a large list of target plates stored locally in a ‘hot list’ rather than relying on real-time communications with State or Federal data sources. The list is typically transferred daily and can be updated by the operator or by a central station if wireless communications are not available in the vehicle. The hot list can contain any set of plate data, including watch lists as well as stolen vehicles. When a target plate is located, the officer in the vehicle is notified with a message that is specific to the plate. This hit occurs even if the driver of the vehicle has not committed a traffic offense or been involved in a traffic accident.” Washington Association of Sheriffs and Police Chiefs, *Guidelines for Washington State Law Enforcement: Operation of Automated License Plate Readers*, September 2008, 5, <https://www.waspc.org/assets/ProfessionalServices/modelpolicies/alprpolicy.pdf>.

12 Washington Association of Sheriffs and Police Chiefs, *Guidelines*, 5.

13 Moreover, while the “hot lists” against which vehicles’ plates are compared can include information about stolen vehicles or reported abductions, they can also include those listed in databases of suspected immigration violators. Ángel Díaz and Rachel Levinson-Waldman, “Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use,” *Brennan Center for Justice*, September 10, 2020, <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>. They can also include lists of people who have unpaid court fees. Dave Maass, “‘No Cost’ License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners,” *Electronic Frontier Foundation*, January 26, 2016, <https://www.eff.org/deep-links/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and/#clarification>.

14 A 2013 Crosscut article states “Vehicle registration data (the name and address of the person who owns a vehicle) is deemed private by Washington state law [RCW. § 46.12.640 {2021}], but the license plate numbers themselves and their geographic locations are public information, which means that anyone could request the data from the police department through a public disclosure request.” Mike A. Fiske, “Never Mind the Drones: The SPD already knows where you’ve been,” *Crosscut*, January 23, 2013, <https://crosscut.com/2013/01/never-mind-drones-spd-already-knows-where-youve-be>. The Seattle Police department, similarly, notes in its 2018 Surveillance Impact Report that ALPR data is subject to the Public Records Act. Seattle Police Department, “2018 Surveillance Impact Report: Automated License Plate Recognition (ALPR) (PATROL),” January 31, 2019, <https://www.seattle.gov/documents/Departments/Tech/Privacy/SPD%20ALPR%20%28Patrol%29%20-%20Final%20SIR.pdf>. Detailed data derived from law enforcement ALPRs in the City of Seattle has, in fact, been released pursuant to public records requests. Bryce Clayton Newell, “Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Info[r]mation Privacy, and Access to Government Information,” *Maine Law Review* 66, no. 2 (2014): 400. <https://digitalcommons.maine.edu/mlr/vol66/iss2/4>. In a puzzlingly divergent interpretation of the same laws, however, WSP’s policy manual states that “Except as otherwise provided by law, all electronic images or data gathered by ALPR is for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public.” Washington State Patrol, “Chapter 18.00.160 Automated License Plate Readers (ALPR),” *Washington State Patrol Policy Manual*, 482, 2018, https://jsis.washington.edu/human-rights/wp-content/uploads/sites/22/2022/11/2018_WSP_Regulation_Manual_Policy_18_00_160_ALPR.pdf.



Types of ALPRs¹⁵

ALPR devices can be operated by branches of federal, state, and local government, as well as private parties;¹⁶ the cost of the technology has plummeted in recent years, encouraging its wide adoption by not only major corporations but small businesses and even private individuals.¹⁷ The data gathered is frequently shared or sold through networks established by their commercial software provider; in this way,

ALPR data gathered in Washington can and does wind up in the hands of law enforcement agencies and corporations located elsewhere. Of course, information about people's movements can be useful if handled responsibly. ALPR data can help in locating stolen vehicles, responding to Amber alerts, and even solving murders.¹⁸ But even promoters of this technology admit that only a small percentage of scans—typically less than a fraction of one percent—turn out to be relevant to public safety concerns. When indiscriminately-gathered data is broadly shared, and particularly when it is integrated with algorithms and data from other forms of surveillance, it becomes possible to use ALPR data to identify individual drivers and track their movements in real time.¹⁹ This could permit the use of ALPR data to undermine Washington's commitment to immigrant and reproductive rights.

15 Dave Maas, "The Four Flavors of Automated License Plate Reader Technology," *Electronic Frontier Foundation*, April 6, 2017, <https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology>

16 Consider, for example, the activities of Digital Recognition Network, described by *Vice* as "a private surveillance system crowdsourced by hundreds of repo men who have installed cameras that passively scan, capture, and upload the license plates of every car they drive by to DRN's database. DRN stretches coast to coast and is available to private individuals and companies focused on tracking and locating people or vehicles. The tool is made by a company that is also called Digital Recognition Network... DRN has more than 600 of these 'affiliates' collecting data, according to the contract. These affiliates are paid a monthly bonus for gathering the data..." Joseph Cox, "This Company Built a Private Surveillance Network. We Tracked Someone With It," *Vice*, September 17, 2019, <https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn>.

17 Josh Kaplan, "License Plate Readers Are Creeping Into Neighborhoods Across the Country," *Slate*, July 10, 2019, <https://slate.com/technology/2019/07/automatic-license-plate-readers-hoa-police-op-nalpr.html>.

18 Seattle Police Department, "2018 Surveillance Impact Report," 2019.

19 See, for example, "Street-Level Surveillance: Automated License Plate Readers (ALPRs)," *Electronic Frontier Foundation*, August 28, 2017, <https://www.eff.org/pages/automated-license-plate-readers-alpr>.

THREATS TO IMMIGRANT RIGHTS

ALPRs are only one in a series of technologies used by ICE and CBP to subject ever larger swaths of the U.S. public to digital surveillance in recent years; other tools include facial recognition software, app-based location data,²⁰ and even utility data to which ICE has purchased access through the CLEAR database produced by data brokers Thomson Reuters²¹ or LexisNexis' Risk Solutions.²² The availability of these private databases poses severe civil liberties concerns.²³ While law enforcement would need to present a warrant or subpoena to gather such information themselves in the context of a criminal investigation, purchasing the data from private data brokers like Thomson Reuters or LexisNexis allows the sidestepping of long

standing due process protections.²⁴ For this reason, both of these companies are currently facing litigation over their practices: Thomson Reuters was sued in California in 2020,²⁵ and LexisNexis in Illinois in August 2022.²⁶

Across the country, many localities have adopted "sanctuary" laws to limit local officials' collaboration with federal immigration enforcement. But research has shown that by tapping into vast reservoirs of personal data offered up by private data brokers, ICE is able to effectively bypass such limitations. For example, researchers discovered that in Union City, California, despite being a sanctuary jurisdiction, officials were (perhaps unwittingly) "feeding their residents' personal information to ICE"²⁷ through ALPR contracts with Vigilant Solutions, a company whose data is included in Thomson Reuters' CLEAR database, to which ICE has had access for years.²⁸

As the Electronic Frontier Foundation warns, "By matching your car to a particular time, date, and location, and then building a database of

20 Joseph Cox, "Customs and Border Protection Paid \$476,000 to a Location Data Firm in New Deal," *Vice*, August 25, 2020, <https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs>.

21 Over time, ICE has accessed Vigilant's ALPR data through multiple approaches: a direct sole-source contract with the company (Homeland Security Today, "ICE Acquires License Plate Tracking Data Through Sole Source Contract," *Homeland Security Today*, January 29, 2018, <https://www.hstoday.us/uncategorized/ice-acquires-license-plate-tracking-data-through-sole-source-contract/>.) and through its inclusion in the CLEAR database provided by Thomson Reuters. Alex Cook, "Thomson Reuters brings Vigilant license plate recognition data to CLEAR investigation platform," *Thomson Reuters*, June 18, 2017, <https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-brings-vigilant-license-plate-recognition-data-to-clear-investigation-platform.html>; Edward Ongweso Jr., "Shareholders Push Thomson Reuters to End Intimate Ties With ICE," *Vice*, May 26, 2020, <https://www.vice.com/en/article/n7wbbd/shareholders-push-thomson-reuters-to-end-intimate-ties-with-ice>.

22 Lexis-Nexis Risk Solutions also offers LPR data as part of its package of "cross-jurisdictional data" for law enforcement. "Law Enforcement and Public Safety," *LexisNexis*. <https://risk.lexisnexis.com/law-enforcement-and-public-safety/information-data-sharing>.

23 Jennifer Lynch, "Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases," *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper 2104* (2021), https://www.hoover.org/sites/default/files/research/docs/lynch_webready.pdf.

24 Drew Harwell, "ICE investigators used a private utility database covering millions to pursue immigration violations," *The Washington Post*, February 26, 2021, <https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/>.

25 Brooks & Shabazz v. Thomson Reuters Corp., 2020, Cal. Sup. Ct., <https://www.classlawgroup.com/wp-content/uploads/Thomson-Reuters-CLEAR-class-action-lawsuit.pdf>.

26 Kathleen Foody, "Immigration advocates sue LexisNexis over personal data," *AP News*, August 16, 2022, <https://apnews.com/article/chicago-lawsuits-georgia-immigration-635396b572cadf172c74b4a0000f52e8>.

27 Vasudha Talla, "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations," *ACLU*, March 13, 2019, <https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data>.

28 "Oversight Subcommittee Launches Investigation into Sale of Utility Customer Info to ICE for Deporting Immigrants," *U.S. House of Representatives Committee on Oversight and Reform*, February 26, 2021, <https://oversight.house.gov/news/press-releases/oversight-subcommittee-launches-investigation-into-sale-of-utility-customer-info>.


that information over time, law enforcement can learn where you work and live, what doctor you go to, which religious services you attend, and who your friends are.” By applying algorithms to this data, “systems can reveal regular travel patterns and predict where a driver may be in the future. The data also reveal all visitors to a particular location. [While] the data generally does not include the driver’s name, law enforcement officers can use other databases to connect individual names with their license plate numbers.”²⁹

While that may sound hypothetical, it’s not—documents released in ACLU’s California lawsuit showed that during seven months in 2018, ICE queried one nationwide license plate location database thousands of times each month. The documents include explanations for each search query, including “investigations attempting to locate travel patterns most likely locations of interest where to locate subject” and other similar annotations.³⁰

Records received by UWCHR add additional evidence, revealing that ICE agents in Washington received alerts from ICE’s National Criminal Analysis and Targeting Center (NCATC) which led them to carry out arrests of people at their homes or in the community.^{31,32,33} The NCATC is a unit within ICE which uses commercial

data from Lexis-Nexis³⁴ to obtain targets for raids and other operations. According to the National Immigration Project, ICE provides names and dates of birth to its commercial partner in an electronic format on a weekly basis, and receives back additional identifying data like biographical information and vehicle information.³⁵ In the cases reviewed by UWCHR, the consultation of these private databases was key to identifying a target for ICE arrests.

By contracting out to unregulated private companies to perform key elements of its investigative work, ICE sidesteps the need for search warrants or other forms of collaboration by local governments in the jurisdictions in which it operates. This not only streamlines their process, but essentially removes their activities from the oversight of courts in our communities.



AS THE ELECTRONIC FRONTIER FOUNDATION WARNS, “BY MATCHING YOUR CAR TO A PARTICULAR TIME, DATE, AND LOCATION, AND THEN BUILDING A DATABASE OF THAT INFORMATION OVER TIME, LAW ENFORCEMENT CAN LEARN WHERE YOU WORK AND LIVE, WHAT DOCTOR YOU GO TO, WHICH RELIGIOUS SERVICES YOU ATTEND, AND WHO YOUR FRIENDS ARE.”

29 “Street-Level Surveillance,” *EFF*.

30 Vasudha Talla and Matt Cagle, “Records Reveal ICE Agents Run Thousands of License Plate Queries a Month in Massive Location Database,” *ACLU NorCal*, June 5, 2019, <https://www.aclunc.org/blog/records-reveal-ice-agents-run-thousands-license-plate-queries-month-massive-location-database>.

31 “Form I-213: Record of Deportable/Inadmissible Alien, 2019-1CLI-00003-021864,” *Department of Homeland Security*, 2019.

32 “Form I-213: Record of Deportable/Inadmissible Alien, 2019-1CLI-00003-023059,” *Department of Homeland Security*, 2019.

33 “Form I-213: Record of Deportable/Inadmissible Alien, 2019-1CLI-00003-8598,” *Department of Homeland Security*, 2019.

34 DHS’ budget documents for Fiscal Year 2022 state that Lexis/Nexis software is used by the NCATC. Department of Homeland Security, *U.S. Immigration and Customs Enforcement Budget Overview: Fiscal Year 2022, Congressional Justification*, 130 (or p. 156 of the pdf), https://www.dhs.gov/sites/default/files/publications/u.s._immigration_and_customs_enforcement.pdf.

35 National Immigration Project, *NIPNLG Surveillance & Technology Newsletter*, no. 1, <https://secure.nationalimmigrationproject.org/np/clients/nationalimmigration/viewOnlineEmail.jsp?emailId=7b825ecef8ed783fafb7cf-3b5af935e57m9055627b8>.

THREATS TO REPRODUCTIVE RIGHTS

Even in states where abortion remains legal, those seeking reproductive health services face what the Electronic Freedom Foundation warns is “unprecedented digital surveillance”; ALPR systems are only one dimension of this problem.³⁶ If, as some predict,³⁷ abortion-banning states begin directing their criminal justice apparatus to investigate and prosecute abortion across state lines, there is little reason to expect they would not tap into the many public and private databases that include location

THIS “VIRTUAL STAKEOUT” FUNCTION COULD BE APPLIED TO CAPTURE DATA ON ALL VEHICLES IN THE PROXIMITY OF AN ABORTION CLINIC, FOR EXAMPLE; OVERLAID WITH INFORMATION FROM OTHER DATABASES, THE DATA COULD THEN REVEAL THE IDENTITIES OF INDIVIDUALS ASSOCIATED WITH THE VEHICLES AND THEIR FRIENDS, FAMILY, OR SOCIAL NETWORKS.

data gathered by ALPRs in Washington state to monitor potential targets. Indeed, they’re doing this already: as the MIT Technology Review warns, activists from Operation Rescue and other groups have been recording the license plates of vehicles arriving at clinics for years.³⁸

In 2022, the legal and political landscape has just created incentives for abortion opponents to take it up a notch.

Motorola’s Vigilant Solutions, for example, not only shares ALPR data with ICE, but also with a host of law enforcement agencies around the country through Thomson Reuters’ nationwide CLEAR database. As Thomson Reuters boasted in 2017, “CLEAR LPR subscribers will now reap the benefit from Vigilant’s vehicle location data, analytics and commercial LPR detections gathered from all over the U.S....As part of an investigation of suspected criminal activity, law enforcement can leverage CLEAR to research people and organizations connected to the vehicle. Additionally, CLEAR LPR subscribers will have access to LEARN, Vigilant’s investigative data platform, which provides users with insights, including: vehicle location, year, make and model search; the best location to find a vehicle; vehicle detection sharing; and the ability to virtually stakeout a vehicle location.”³⁹ This “virtual stakeout” function could be applied to capture data on all vehicles in the proximity of an abortion clinic, for example; overlaid with information from other databases, the data could then reveal the identities of individuals associated with the vehicles and their friends, family, or social networks.

One of Motorola’s main competitors, Flock Safety, began as a startup in 2017 but has grown precipitously by offering low-cost, solar-powered cameras that connect wirelessly to a nationwide network⁴⁰ made up of some

36 Adam Schwartz, “Congress Probes How Location Data Brokers Threaten Reproductive Privacy,” *Electronic Frontier Foundation*, July 12, 2022, <https://www.eff.org/deeplinks/2022/07/congress-probes-how-location-data-brokers-threaten-reproductive-privacy>.

37 Cohen *et al.*, “New Abortion Battleground.”

38 Abby Ohlheiser, “Anti-abortion activists are collecting the data they’ll need for prosecutions post-Roe,” *MIT Technology Review*, May 31, 2022, <https://www.technologyreview.com/2022/05/31/1052901/anti-abortion-activists-are-collect->

[ing-the-data-theyll-need-for-prosecutions-post-roel/](https://www.technologyreview.com/2022/05/31/1052901/anti-abortion-activists-are-collect-ing-the-data-theyll-need-for-prosecutions-post-roel/).

39 Cook, “Thomson Reuters brings Vigilant.”

40 Jay Stanley, “Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System,” *ACLU*, March 3, 2022, <https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system>.

20,000 cameras and 1,800 law enforcement agencies, according to an email from a company representative.⁴¹ The company's materials boast the ability not just to search by license plate number, but also color and make of car, even details like the presence or absence of specific vehicular features like a roof rack; its analytics also permit "convoy analysis," or the identification of cars apparently traveling together.⁴² Flock takes no position on law enforcement's possible use of its system for limiting access to reproductive rights: "Flock's mission as a business is to eliminate crime," Josh Thomas, the vice-president of external affairs at Flock, told the Guardian recently. "Our position at Flock remains consistent in response to the Dobbs decision. Our perspective is that we do not enact laws, and our mission is not specific to any particular laws... We expect cities in California may operate differently than cities in Texas or Illinois or Rhode Island. So it would be inaccurate to characterize Flock as being for or against any particular issue."⁴³

The practice of virtually staking out a location is similar to "geofencing," the practice whereby law enforcement seeks location data, typically cell phone data,⁴⁴ to enable it to identify all people within a given geographic boundary during a specific time. Yet while geofencing using cell phone data requires a criminal warrant to compel companies like Google to provide the data,⁴⁵ location data from ALPRs is often

shared indiscriminately, rendering the need for warrants moot. What's more, private parties *already* engage in geofencing to send targeted ads to people in the vicinity of abortion clinics; only one state, Massachusetts, has banned this practice.⁴⁶ ALPR data, if it remains unregulated, can be used by private parties, including those committed to discouraging abortion through shaming and harassment that, in the "old days," relied on physical presence at clinics. It can also be used by public authorities in anti-abortion jurisdictions to build cases against seekers or providers of abortion services.

In Washington state, except for Seattle's Surveillance Ordinance passed in 2017,⁴⁷ there are no legal standards governing the use of ALPR systems⁴⁸ or the management of the data they generate. It is therefore extremely important to know not only who is gathering the data that permits the tracking of Washingtonians' movements, but how that data is being stored and shared, to ensure that it is not used in ways that invalidate the important rights protections our institutions have pledged to defend.

Warrant, 2020, <https://www.documentcloud.org/documents/21197805-seattle-fbi-geofence-warrant-oct-2020>

46 Office of Attorney General Maura Healey, "AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities," April 4, 2017, <https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities>.

47 "An ordinance relating to The City of Seattle's acquisition and use of surveillance technologies," 2017, <http://seattle.legistar.com/LegislationDetail.aspx?ID=2981172&GUID=0B2FEFC0-822F-4907-9409-E318537E5330&Options=Advanced&Search=>.

48 "Automated License Plate Readers: State Statutes," *National Conference of State Legislatures*, February 3, 2022, <https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx>. See also Seattle Department of Transportation, "2018 Surveillance Impact Report," 14.

41 Mack Larkin, email message to Jonathan Schwarder of Richland Police Department, July 18, 2022.

42 Joseph Cox, "Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras," *Vice*, March 3, 2021, <https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader>.

43 Johana Bhuiyan, "How expanding web of license plate readers could be 'weaponized' against abortion," *The Guardian*, October 6, 2022, <https://www.theguardian.com/world/2022/oct/06/how-expanding-web-of-license-plate-readers-could-be-weaponized-against-abortion>.

44 Lynch, "Modern-Day General Warrants."

45 See, for example, this search warrant filed by the FBI to obtain data from Google regarding all parties in proximity to a specific incident in Seattle in 2020. Application for a Search

METHODS

Beginning in November of 2021, UWCHR filed public records requests across Washington state in an effort to understand the scope, regulation and use of ALPR systems by sheriffs and police departments.⁴⁹ Because blanketing every law enforcement agency in the state would require an exorbitant amount of labor, we instead targeted our public records requests in three ways, based on initial research into local practices.⁵⁰

First, UWCHR researchers sought to determine which Washington law enforcement agencies had contracts with Vigilant Solutions, and with whom those agencies share their ALPR data, since for the reasons discussed above Vigilant is a known vector for “data-driven deportation”⁵¹ and it could serve a similar purpose for prosecuting abortion. To gauge Vigilant’s footprint in Washington state, UWCHR replicated the method developed by EFF,⁵² and requested the user agreement governing all Vigilant contracts; the names of agencies and organizations with which ALPR data is shared; the names and agencies with which “hot lists” of targets are shared; the net number of scanned plate images obtained and the percentage of these that generated “hits” against local law enforcement’s designated targets.⁵³

Second, prior research by UWCHR led us to suspect that in some jurisdictions, law enforcement agencies have allowed ICE or CBP to tap into their ALPR systems directly.⁵⁴ Of these jurisdictions, UWCHR requested training material, contracts and policies regarding ALPR use and associated software, and information on any technology received through Operation Stonegarden.^{55, 56}

receives ALPR data; (3) The names of agencies and organizations with which the Agency shares “hot list” information; (4) The names of agencies and organizations from which the Agency receives “hot list” information; (5) The aggregate number of “detections” (i.e. license plate scans and associated data) collected from October 1, 2020 to September 30, 2021. (6) The aggregate number of detections collected from October 1, 2020 to September 30, 2021. (7) The aggregate number of “hits” (i.e. times that a plate on a hotlist was detected) from October 1, 2020 to September 30, 2021. (8) The aggregate number of “hits” from October 1, 2020 to September 30, 2021.”

54 Operation Stonegarden (OPSG) is a FEMA program that promotes cooperation among CBP/Border Patrol and local and state law enforcement agencies; grant funds are provided on the condition that CBP will be given access to the information generated by local law enforcement agency purchases. FEMA describes Operation Stonegarden as “support[ing] enhanced cooperation and coordination among Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies to improve overall border security.” FEMA Grant Programs Directorate, “Preparedness Grants Manual,” *FEMA*, February 2021, 7, https://www.fema.gov/sites/default/files/documents/FEMA_2021-Preparedness-Grants-Manual_02-19-2021.pdf.

55 In Okanogan County, WA, funds from a Stonegarden grant were used to purchase and install license plate readers, and CBP was granted access to the information generated by these devices. As Okanogan Chief Deputy Laura Wright explained in a December 2019 email, “We actually signed up the [Border Patrol] on our system and they look at everything themselves. It was quite easy when we set up all the accounts. We made sure that Aaron forwarded us the people that need to review and add to the system.” In June 2022, after Okanogan transitioned to Vigilant, Deputy Wright again set up user accounts for CBP officials to access the system directly. Laura Wright, email message to Ricky Covarrubias and Cody Lunn, June 1, 2022.

56 “The Center for Human Rights (“Center”) at the University of Washington respectfully submits the following request under Washington State’s Public Records Act. The Center requests copies of all memoranda, policies, instructional and training materials, manuals, agreements and contracts regarding any technology or devices in the possession of What-

49 UWCHR researchers used language modeled after a similar request made by EFF and the ACLU in 2018. *Lagleva v. Marin County Sheriff*, 2021, Cal. Sup. Ct., <https://www.eff.org/document/lagleva-v-marin-county-sheriff>

50 This report was authored by Angelina Snodgrass Godoy with research support from Priya Hendry, Nancyrose Houston, Lukas Illa, and Tara Saleh.

51 Nina Wang *et al.*, “American Dragnet.”

52 “Data Driven: What We Learned,” *Electronic Frontier Foundation*, <https://www.eff.org/pages/what-we-learned>.

53 “The Center for Human Rights at the University of Washington respectfully submits the following request under Washington State’s Public Records Act: (1) The names of agencies and organizations with which the Agency shares Automated License Plate Recognition (ALPR) data; (2) The names of agencies and organizations from which the Agency

Lastly, since 2007, the Washington Auto Theft Prevention Authority (WATPA) has issued grants totaling \$1.3M to dozens of Washington law enforcement agencies for the purpose of purchasing ALPRs. WATPA has drafted model guidelines for ALPR use in light of privacy concerns, which include regular audits to ensure compliance with local laws;⁵⁷ therefore, UWCHR obtained a list of all local law enforcement agencies that had received grants from WATPA to purchase ALPRs, and requested the original grant proposal and governing policies for ALPR system audits from each of the 29 agencies.⁵⁸

Obtaining this information was challenging. Some agencies, such as Walla Walla Police Department,⁵⁹ Whatcom County Sheriff, and Battle Ground Police Department, failed to respond altogether; others responded that they had no relevant records. In many other cases, such as the Police Departments of Federal Way and Edmonds, responses were incomplete. Despite explicit instructions provided in our requests, many local law enforcement agencies claimed they did not know how to access the information in their digital systems that would

show with whom their ALPR data was being shared.

It is also vitally important to understand that in addition to public agencies, ALPR data is also gathered by *private* owners of ALPR technology; at present, those private parties may share the data they obtain with whomever they want. Indeed, several ALPR companies actively promote the use of their technology by private parties. The parent company of Vigilant Solutions, Motorola, also owns another subsidiary, Digital Recognition Network, which employs private contractors to collect license plate data, encouraging them to scan shopping malls, sporting events, and workplace parking lots by day and apartment complexes by night.⁶⁰ More recently, Flock Safety has transformed the market by offering lower-priced ALPR technology, encouraging homeowners' associations, neighborhood groups and other private citizens to install their own ALPR readers and share data with law enforcement.⁶¹ Not only are researchers unable to submit public records requests to private parties who may be gathering ALPR data, but in most cases we don't even know who they are, let alone what they are doing with the data.

As a result, the findings shared in this report should be understood as only a *partial* picture of ALPR use in Washington and the human rights concerns it raises, rather than a comprehensive account of the full extent to which the technology is currently in use. It is likely, in fact, that the use of this technology is far more widespread than documented here.

com County Sheriff's Office which enable electronic reading of license plates or electronic collection of license plate data. This includes technology purchased through grants from Operation Stonegarden and other sources, and refers not only to the devices themselves but the software required to manage the data they generate."

57 Washington Association of Sheriffs and Police Chiefs, *Guidelines for Washington State Law Enforcement: Operation of Automated License Plate Readers*, July 2017, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/LPR-Model-Policy-July-2017.pdf>.

58 Kim Goodman, "Public Records Release: WATPA Funded ALPR's," October 26, 2021, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/2021-10-26-Godoy.pdf>.

59 Nonetheless, the Walla Walla City Council minutes of March 11, 2020 meeting of the Walla Walla City Council show that it passed Resolution 2020-33, which reads in part: "The contract to supply a mobile automated license plate recognition (ALPR) system and related equipment is hereby awarded to Vigilant Solutions, LLC, and the City Manager of the City of Walla Walla, and designees of the City Manager, are hereby authorized, empowered and directed to purchase such equipment." Walla Walla City Council, "Regular Meeting Minutes," March 11, 2020, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Walla-Walla-approves-funds-to-buy-ALPR-from-Vigilant.pdf>.

60 Joseph Cox, "This Company Built a Private Surveillance Network. We Tracked Someone With It," *Vice*, September 17, 2019, <https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn>.

61 Drew Harwell, "License plate scanners were supposed to bring peace of mind. Instead they tore the neighborhood apart," *The Washington Post*, October 22, 2021, <https://www.washingtonpost.com/technology/2021/10/22/crime-suburbs-license-plate-readers/>.

FINDINGS

Based on the documents reviewed, UWCHR researchers assessed the written policies of various law enforcement agencies regarding the storing and sharing of ALPR data. We found they varied widely across jurisdictions. Below, we describe agency practices we identified in our research, and explain why each set of considerations is relevant in assessing the dangers to immigrant and reproductive rights.

DATA RETENTION

Because ALPR data is so voluminous, and in the vast majority of cases involves the movements of individuals whose activities are unrelated to public safety concerns, the prompt deletion of data not identified as linked to public safety is a best practice.⁶² Fortunately, a number of Washington agencies have policies that suggest they comply with these best practices.

For example, the city of Tacoma claims to retain no records of ALPR scans. Its parking authorities reported that their system automatically deletes any LPR data after no more than 24 hours unless it led to a citation action. Seattle Police Department's most recent (2019) update to ALPR policies states that all ALPR data "except for Hits and Data Used for a Parking Enforcement Action," is deleted within 90 days.^{63, 64}

Auburn Police Department, Fife Police Department, Sunnyside Police Department, Moses Lake Police Department, Bellingham Police Department, follow a Lexipol⁶⁵ policy which states that ALPR data downloaded to the server must be disposed of according to the Washington State Law Enforcement Records Retention Schedule. These guidelines require that state records must be retained until verification that a significant image has not been captured or the appeals process is completed.^{66, 67} In these LEAs, the responsibility to ensure proper data collection and retention falls to the Administrative Division Commander.

62 Brian M. Rosenthal, "Police cameras busy snapping license plates," *Seattle Times*, August 3, 2013, <https://www.seattletimes.com/seattle-news/police-cameras-busy-snapping-license-plates/>.

63 Seattle Police Department, "Title 16.170 POL- 5 ALPR Data Storage and Retention," *Seattle Police Department Manual*, <https://www.seattle.gov/police-manual/title-16---patrol-operations/16170---automatic-license-plate-readers>.

64 However, hits are defined as "alert[s] from the ALPR system that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason." Seattle Police Department, "Title 16.170-POL- 1 Definitions," *Seattle Police Department Manual*, <https://www.seattle.gov/police-manual/title-16---patrol-operations/16170---automatic-license-plate-readers>. The NCIC includes information on "immigration violators" and will presumably generate hits based on this information. It is unclear what action SPD officers are instructed to take when such a hit occurs—are they expected to confirm the plate, as with other hits? Is the resultant data preserved? Although SPD notes that "All

requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018," hits generated by the NCIC are not, technically speaking, requests for data from ICE, so this is unclear. Seattle Police Department, "2018 Surveillance Impact Report," 2019, 25. Michael Wishnie and Annie Lai, "Blurring the Lines: A Profile of State and Local Police Enforcement of Immigration Law Using NCIC Database," *Migrant Policy Institute*, September 2005, <https://www.migrationpolicy.org/research/blurring-lines-profile-state-and-local-police-enforcement-immigration-law-using-ncic>.

65 For some of UWCHR's past research on Lexipol, see: "Don't Ask, Do Tell: Local Law Enforcement Collaboration with ICE/CBP," *UWCHR*, September 25, 2017, <https://jsis.washington.edu/humanrights/2017/09/25/dont-ask-do-tell/>.

66 Auburn Police Department, "Policy 427.4: ALPR Data Collection and Retention," *WA Policy Manual*, November 15, 2021, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Automated_License_Plate_Readers.pdf.

67 Washington State Archives of the Office of Secretary State, "Section 6.4 Violations and Traffic Enforcement," *Law Enforcement Records Retention Schedule*(7)2, January 2017, <https://www.sos.wa.gov/assets/archives/records-management/law-enforcement-records-retention-schedule-v.7.2-january-2017.pdf>. Note: See p 31, Section 6.4 Violations and Traffic Enforcement, for ALPR (case specific and non-case specific)

DATA SHARING

Across Washington, however, many jurisdictions permit the unrestricted sharing of ALPR data with a range of federal and out-of-state law enforcement agencies, and even with private networks. These secondary agencies are not bound by Washington state's "sanctuary" laws regarding migration or reproductive health.

“UNDER THE KEEP WASHINGTON WORKING ACT, IF ICE/CBP WERE TO CONTACT LOCAL LAW ENFORCEMENT AND REQUEST HELP TRACKING A VEHICLE FOR CIVIL IMMIGRATION ENFORCEMENT, LOCAL LAW ENFORCEMENT WOULD BE BARRED FROM RENDERING THAT ASSISTANCE – BUT THANKS TO THE WIDESPREAD SHARING OF ALPR DATA, ICE AND CBP DON’T HAVE TO ACTIVELY REQUEST THE DATA, MUCH LESS EXPLAIN THEIR INTENDED USE OF IT.”

For example, through its contract with Vigilant Solutions, the Vancouver Police Department shares ALPR detection data with a list of 664 agencies,⁶⁸ including ICE Enforcement and Removal Operations in Washington DC,⁶⁹ CBP's National Targeting Center, and a range of District Attorney's offices, police departments, and sheriffs. This grants ICE and CBP the ability to tap

into local government resources to power their immigration enforcement activities. Under the Keep Washington Working Act, if ICE/CBP were to contact local law enforcement and request help tracking a vehicle for civil immigration enforcement, local law enforcement would be barred from rendering that assistance – but thanks to the widespread sharing of ALPR data, ICE and CBP don't have to actively request the data, much less explain their intended use of it.

As regards reproductive rights, many of the jurisdictions with which Vancouver shares ALPR data are in states that criminalize abortion, including in some cases out-of-state abortion. For example, at least 52 police departments and sheriff's offices are identified as being in the state of Texas alone, where the notorious "bounty law" rewards private citizens who sue others for aiding or abetting abortion.⁷⁰ This means that personnel from those departments and organizations would be able to access information in real time about vehicles as they move through Vancouver, Washington. In addition, Vancouver receives "hot lists" from 40 sheriffs and police departments across Texas; while the agency did not provide UWCHR a copy of its policies regarding response to a notification of a hit on these hot lists, this could result in incidents where Vancouver deputies pull over vehicles on the basis of suspicion of criminal activity from other states, including those states that define traveling to Washington to receive reproductive health care as a crime.⁷¹ This raises grave concerns about the possible misuse of ALPR data to erode rights Washington state has sought to uphold through recent policies and directives.

68 "Vigilant PlateSearch Agency Data Sharing Report: Vancouver Police Department," *Vigilant PlateSearch*, November 10, 2021, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/P006309_Responsive_Records.pdf.

69 Also note that per ICE policy as articulated in an ICE document titled "License Plate Reader Data from Outside of ICE," released to to the ACLU of Northern California under FOIA, "Once an agency shares data with ICE, all ICE LPR users will have access to that data." (Emphasis added) See p. 102 in: "ICE FOIA Case No. 2018-ICLI-00035 - ACLU v. U.S. Immigrations and Customs Enforcement (ICE), 18-cv-04105," *Department of Homeland Security*, 2018, https://www.aclunc.org/docs/DOCS_031319.pdf.

70 Emma Bowman, "As states ban abortion, the Texas bounty law offers a way to survive legal challenges," *NPR.org*, July 11, 2022, <https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law>.

71 For an example of a related incident: Charlie Warzel, "When License-Plate Surveillance Goes Horribly Wrong," *New York Times*, April 23, 2019, <https://www.nytimes.com/2019/04/23/opinion/when-license-plate-surveillance-goes-horribly-wrong.html>.

By contrast, Mercer Island Police Department also contracts with Vigilant, but does not share ALPR data with any external parties, as its system sharing report indicates.⁷²

In July 2022, Benton County's Board of Commissioners voted to purchase 10 ALPR readers from Flock.⁷³ This appears to be part of a multi-jurisdictional effort at coordinating ALPR use: according to records received by UWCHR from Richland Police Department, earlier in 2022, Kennewick Police Department reportedly took the lead in applying for a WATPA grant to purchase Flock ALPRs for the Police Departments of Richland, West Richland, Kennewick, and the Benton County Sheriff.⁷⁴ Despite this, in response to a September 2022 request from UWCHR researchers, however, Benton County Sheriff's office said they "do not have a Automated License Plate Recognition device," making the current status of this collaboration unclear.⁷⁵

Many law enforcement agencies in Washington appear to be transitioning to Flock. In a July 22 email to Richland Police Department, Flock salesperson Mack Larkin said that in Washington, Liberty Lake Police Department and Yakima Police Department had live Flock systems up and running, while Airway Heights Police Department, Moses Lake Police Department, Othello Police Department, Pasco Police Department, the Spokane County Sheriff's Office, Tukwila Police Department, Union Gap Police Department, and Wapato Police Department, had already signed contracts. He further claimed that

Anacortes Police Department, Arlington Police Department, Des Moines Police Department, Kent Police Department, Lake Forest Park Police Department, and Sunnyside Police Department were, at that time, reviewing possible Flock contracts, and "another 20+ agencies here in WA" were "working towards getting Flock". He cited the connection of Washington's Flock customers to some 1,800 law enforcement agencies nationwide as a selling point.⁷⁶

In some cases, CBP and ICE agents have direct access to ALPR databases, allowing them to tap into the systems directly to monitor people's movements without being shared through Vigilant, Flock, or other service providers. For example, in response to a public records request by UWCHR researchers, Okanogan County Sheriff's Office provided a list of individuals with direct access to ALPR systems;⁷⁷ the list includes 6 CBP agents, whose systems permissions allow them to access Modified Hotlists, Dispatcher, Data Mining and Dashboard services. This means CBP agents could create their own "hotlist" of targets on Okanogan's system in order to trigger a notification when such vehicles are detected. While Okanogan County's ALPR services were originally provided by Leonardo,⁷⁸ a March 2022 email exchange between law enforcement agents in Post Falls, Idaho, Okanogan County, Washington, and CBP agent Aaron McNair show that the county now contracts with Vigilant—a switch McNair celebrated because "the Vigilant system is something we use on a regular basis!"⁷⁹

72 "Vigilant PlateSearch Agency Data Sharing Report: Mercer Island Police Department (WA)," November 23, 2021, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Sharing-Report.pdf>.

73 "Board of Benton County Commissioners Minutes," July 19, 2022, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Benton-County-CommissionersMinutes07-19-22125829072822PM135.pdf>.

74 Brigit Clary, email message to Jon Amundson and Heather Kintzley, June 23, 2022.

75 Toni Mata, email message to UWCHR, September 8, 2022.

76 Mack Larkin, email message to Richland Police Department, July 18, 2022.

77 Office of the Okanogan County Sheriff, "Customer user list of ALPR systems," November 2021, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/080121OCSUsersLPRS.pdf>.

78 "ELSAG® Enterprise Operations Center™," Leonardo, <https://www.leonardocompany-us.com/lpr/elsag-eoc>.

79 This doesn't necessarily mean the county is able to use the technology. Despite repeated emails in March to May 2022 between Okanogan County and CBP about the latter's interest in using data collected by the county's ALPR trailer, in September 2022 the County informed UWCHR that Chief Deputy Laura Wright remained unable to connect to Vigilant's system. Aaron McNair, email message to Laura Wright,

In May 2022, CBP Agent McNair contacted Okanogan's Chief Criminal Deputy, Laura Wright, asking for access to the new ALPR system because "I would like to have it email me license plates as it detects them."⁸⁰ In June, Deputy Wright set multiple CBP officers up with user accounts to directly access the County's new Vigilant system.⁸¹ In September 2022, Okanogan County Sheriff's Office told UWCHR they had been unable to connect their ALPR trailer to the Vigilant system, rendering it inoperable, but that some of their patrol vehicles were equipped with ALPR cameras which send and receive data from Leonardo.⁸²

In the past, Okanogan County and other Washington state jurisdictions, including Richland Police Department and Spokane County Sheriff, have had cross-border data-sharing agreements with the Police Department of Post Falls, Idaho.^{83,84} Under the terms of the Northern Idaho License Plate Recognition Project referenced in these agreements, ALPR data collected by devices in Washington was stored on the Post Falls Police Department server, and shared with all parties who entered into agreements with Post Falls Police Department.⁸⁵ The present

status of this agreement is unclear: Post Falls Police Department told UWCHR that its system had gone down in February 2022, and that since then they were no longer using ALPR system,⁸⁶ and the agreement was no longer in effect.⁸⁷ Okanogan County Sheriff's Office also told UWCHR that it had discontinued dealings with Post Falls, creating its own Vigilant account instead.⁸⁸

It is unclear whether data-sharing might persist between other Washington jurisdictions and Post Falls. A March email from Post Falls Police Department indicates that, "After careful consideration of all ALPR vendors, and mitigating factors, we have selected Vigilant Solutions from Motorola to be our ALPR Vendor. As we transition to Vigilant, we will keep the BOSS server operational so as to allow all participating agencies the ability to either choose their own vendor or go with Vigilant."⁸⁹

When UWCHR asked Post Falls in July 2022 to clarify which company provided their ALPR services, Post Falls Police Department claimed, implausibly, that they did not know which company was involved, and did not have a written contract.⁹⁰ In November of 2022, Laura Claffey, public records officer of Post Falls Police Department, confirmed that the department has subscribed to Vigilant services but that the system is not functional at this time.⁹¹

Lastly, when asked to clarify the existence and nature of their data sharing with Post Falls, Spokane Police declined to respond despite

Tony Hawley, and Aaron Culp, March 2, 2022.

80 Aaron McNair, email message to Laura Wright, May 19, 2022.

81 Laura Wright, email message to Ricky Covarrubias and Cody Lunn, June 1, 2022.

82 Beth Barker, email message to UWCHR, September 13, 2022.

83 "Northern Idaho License Plate Recognition Project," signed April 30, 2014, contract no. 191-14, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Contract_No._191-14_Northern_Idaho_License_Plate_Reader_Project.pdf.

84 Board of County Commissioners of Spokane County, "Resolution in the matter of executing the Northern Idaho License Plate Recognition Project Agreement Between the Post Falls Police Department, Spokane County and the Spokane County Sheriff's Office," Res. No. 19-0994, April 30, 2019, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/R6617_Released_Records_No_Re-dactions.pdf.

85 Spokane County Sheriff's Office, "Agenda Sheet: in the matter of executing the Northern Idaho License Plate Recognition Project Agreement Between the Post Falls Police Department, Spokane County and the Spokane County Sheriff's Office," April 2019, <https://www.spokanecounty.org/>

[DocumentCenter/View/25816/Item-No-4e](https://documentcenter.view/25816/Item-No-4e).

86 Laura Claffey, email message to Angelina Godoy, July 15, 2022.

87 Telephone conversation July 18, 2022 between Laura Claffey of Post Falls Police Department and Angelina Godoy, UWCHR Director.

88 Laura Claffey, email message to UWCHR, July 21, 2022.

89 Aaron McNair, email message to Laura Wright, Tony Hawley, and Aaron Culp, March 2, 2022.

90 Laura Claffey, email message to Angelina Godoy, July 22, 2022.

91 Laura Claffey, email message to UWCHR, November 9, 2022.

multiple public records requests, emails, and phone calls by UWCHR's Director throughout the month of August 2022. At the time of this writing, these requests remain pending.

If data sharing across state lines continues, Idaho law enforcement may be making determinations about the sharing of ALPR data gathered in Washington. Idaho currently bans abortion in most circumstances, and has passed an anti-abortion law modeled on Texas' "bounty hunter" law allowing family members to sue abortion providers for up to \$20,000.⁹² Sen. Patty Murray has spoken out about Eastern Washington clinics straining to attend to the needs of out-of-state patients;⁹³ at Planned Parenthood Spokane reportedly as many as 78% of the clinic's patients in July 2022 came from Idaho.⁹⁴ Workers at Planned Parenthood Spokane have also reported being harassed and intimidated and even followed home by protestors.⁹⁵ Yet if data revealing their regular daily movements, and that of their patients, is stored across state lines, those responsible for administering that data have no legal responsibility to uphold Washington's commitment to reproductive rights.

TRANSPARENCY

Alarming little is known about the extent of ALPR use by private and public entities in the state of Washington; this makes it difficult to carefully assess the risk they pose to human rights. One key part of the problem is the secrecy that surrounds this technology. While in part this secrecy is due to a lack of regulations requiring reporting of the technology's use, in part it also appears to be caused by many law enforcement agencies' reluctance to share information about their practices—as the aforementioned responses from Spokane and Post Falls Police Departments suggest.

In part, this secrecy is encouraged by the companies with whom law enforcement contracts. Vigilant, for example, reportedly includes non-disclosure agreements in its contracts with law enforcement,^{96,97} requiring agencies to obtain permission from the company before making public any reference to Vigilant's LEARN system⁹⁸—despite the fact that Vigilant's services are paid by tax dollars. Vigilant's training materials also recommend that police not include reference to the use of ALPR data in any written reports.⁹⁹ The company reportedly also bars contracting public agencies from "provid[ing] ANY information, including interviews, related to LEARN products or its services to any member of the media without

92 Kate Zernike, "Idaho Is First State to Pass Abortion Ban Based on Texas' Law," *New York Times*, March 14, 2022, <https://www.nytimes.com/2022/03/14/us/idaho-abortion-bill-texas.html>.

93 Senator Patty Murray, Twitter Post, July 13, 2022, 10:52AM, <https://twitter.com/PattyMurray/status/1547277716357013516?s=20&t=CvdAjkVcxF4Mjddrs0H-MA>.

94 Nina Shapiro, "Washington Attorney General Enters Fray in Idaho Abortion Lawsuit," *Seattle Times*, August 16, 2022, <https://www.seattletimes.com/seattle-news/wa-attorney-general-enters-fray-in-idaho-abortion-lawsuit/>.

95 Jamie Yuccas, "States with abortion rights expect to see surge in out-of-state patients — and protestors," *CBS Evening News*, June 24, 2022, <https://www.cbsnews.com/news/states-with-abortion-rights-surge-of-out-of-state-patients-and-protesters/>.

96 Dave Maass, "Here's Why You Can't Trust What Cops and Companies Claim About Automated License Plate Readers," *Electronic Frontier Foundation*, March 19, 2019, <https://www.eff.org/deeplinks/2019/03/heres-why-you-cant-trust-what-cops-and-companies-claim-about-automated-license>.

97 Tim Cushing, "Vigilant And Its Customers Are Lying About ICE's Access To Plate Records," *TechDirt*, March 27, 2019, <https://www.techdirt.com/2019/03/27/vigilant-customers-are-lying-about-ices-access-to-plate-records/>.

98 Vigilant Solutions, "Item 4: Restrictions on Access to LEARN Software Service, (d)Non-Publication and (e) Non-Disparagement," *Vigilant Solutions State and Local Law Enforcement Agency Agreement*, 9, June 1, 2016, <https://www.documentcloud.org/documents/4618380-ITEM-4-Contract-No-DP81191041-FY-16-17.html#document/p9/a443654>.

99 Dave Maass, "Comment: Instructs police to keep LPR use out of police reports," *License Plate Reader (LPR) Participant Guide* [Annotated], 110, March 2015, <https://www.documentcloud.org/documents/5081028-PRA-LPR-Redacted.html#document/p110/a465942>.

the express written consent of LEARN-NVLS.”¹⁰⁰ This could explain Post Falls’ claim that they did not know the name of the company with whom they were doing business, although previously-released emails had shown it to be Vigilant.

Other Washington law enforcement agencies were also less than forthcoming in their responses to requests for information. Yakima Police Department, for example, released 2018 data to EFF researchers showing that the City had a contract with Vigilant enabling the sharing of ALPR data with a whopping 489 agencies nationwide, one of which was itself a network with 521 member agencies, the names of which Vigilant has declined to disclose.¹⁰¹ Yakima officials publicly insisted that they don’t share data with ICE directly¹⁰²—which is entirely possible, but immaterial since they appear to do so indirectly through Vigilant. The Yakima Police Department told UWCHR in November 2021 that, “We no longer utilize the Automated License Plate Recognition (ALPR) system. We did not renew our contract with them, so we haven’t used it or had access to any part of the system for the past couple of years.” Yet just months earlier on local talk radio, Yakima police officers had claimed new cameras were purchased with Vigilant in 2021 and that the technology has been in use for years.¹⁰³ And in April 2022, local media reported that Yakima was the first law enforcement agency in Washington to use Flock readers, and that it was encouraging

businesses and private citizens in the city to invest in their own ALPRs and connect them to law enforcement’s Flock system.¹⁰⁴

This lack of transparency may also manifest itself in most agencies’ apparent failure to comply with requirements to conduct regular audits of their ALPR systems. Language requiring the performance of regular system audits to ensure appropriate usage is included in most of the policies reviewed by UWCHR, yet most agencies were unable to find records of such an audit ever having been performed. For example, Fife Police Department reported that “...no formal audits have been performed since the system was acquired;”^{105,106} Edmonds Police Department responded that “no audits were located,” and many others simply declined to provide records of audits, despite WATPA’s policy recommending that all participating agencies perform audits at least once per year to ensure compliance with examining LPR data security.¹⁰⁷ WATPA itself has also performed no audits, despite retaining the capacity to do so under its interagency agreement with the law enforcement agencies receiving grants.¹⁰⁸

100 Kade Crockford, “Company Asks Cops to Keep Use of License Plate Trackers Secret,” *ACLU*, March 3, 2015, <https://www.aclu.org/blog/national-security/privacy-and-surveillance/company-asks-cops-keep-use-license-plate-trackers>.

101 “Vigilant Solutions Agency Data Sharing Report: Yakima Police Department,” February 20, 2018, <https://www.documentcloud.org/documents/4432253-Data-Sharing-Report-Yakima-Police-Department.html>.

102 Colton Redtfeldt, “Yakima police license plate scans spark privacy concerns,” *Yakima Herald-Republic*, October 6, 2018, https://www.yakimaherald.com/news/local/yakima-police-license-plate-scans-spark-privacy-concerns/article_a2a8cedc-c9ee-11e8-b37e-83666d84646c.html.

103 Lance Tormey, “Police Say License Plate Readers Cams Have Been in Use for Years,” *NewsTalkKIT*, August 2, 2021, <https://newstalkkit.com/police-say-license-plate-reader-cams-have-been-in-use-for-years/>.

104 Emily Goodell, “‘Game-changing’ tech helped Yakima police catch accused child molester,” *YakTriNews*, April 20, 2022, <https://www.yaktrinews.com/game-changing-tech-helped-yakima-police-catch-accused-child-molester/>.

105 “Agreement Between Fife Police Department and the Washington Auto Theft Prevention Authority,” April 24, 2019, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/PRR-Saleh-110821-1376-RECORDS-Install02.pdf>.

106 Fife City Council, “A Resolution of the City Council of the City of Fife, Pierce County, Washington Authorizing acceptance of a Washington Auto Theft Prevention Award,” Res. No. 1859, February 12, 2019, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/PRR-Saleh-110821-1376-RECORDS-Install01.pdf>.

107 Washington Association of Sheriffs and Police Chiefs, *Guidelines*, 2017.

108 “Washington Auto Theft Prevention Authority Inter-agency Agreement — Auto Theft Prevention Grant Awards, General Terms and Conditions,” 7, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/WATPA-Interagency-Agreement.pdf>.

CONCLUSIONS AND RECOMMENDATIONS

While companies marketing ALPR technology tout them as invaluable tools for law enforcement, many law enforcement agencies in Washington told us otherwise. When asked what ratio of scans actually generated a “hit” indicating a vehicle of interest, many law enforcement agencies reported vanishing rates of return. Bellingham Police Department, for example, reported 0.000027% of scans identified wanted vehicles;¹⁰⁹ Monroe Police

TODAY, THE GATHERING OF ALPR DATA IN WASHINGTON STATE IS ENTIRELY UNREGULATED, MEANING THAT ANYONE CAN SET UP A CAMERA, PAIR IT WITH LOW-COST ALPR SOFTWARE, RECORD THEIR NEIGHBORS’ MOVEMENTS, AND SELL THE DATA.

Department reported a hit rate of 0.00032%;¹¹⁰ Bremerton Police Department returned a hit rate of 0.00189%.¹¹¹ These low rates of efficacy are not unusual: the ACLU estimates that nationwide, less than 0.2 percent of plate scans are linked to criminal activity or vehicle registration issues.¹¹²

Perhaps for these reasons, multiple law enforcement agencies including Walla Walla Sheriff’s Office, Sunnyside Police Department, Lake Stevens Police Department and Everett Police Department reported they had discontinued use of systems originally made available to them by WATPA grants. And Bellingham Police Department, in its report to the WATPA after the systems were purchased, wrote, “We continue to have technological problems with all our vehicles.... 20% misread rate...;”¹¹³ 28000 reads with about a 20% misread occurrence;¹¹⁴ and, “Officers were originally enthusiastic about it, but that declined because of all the technical problems.”^{115,116} While marketed as a tool to solve crimes in order to make communities safer, unregulated ALPR systems may in fact create new vulnerabilities that threaten a wide swath of Washington’s population.

Today, the gathering of ALPR data in Washington state is entirely unregulated, meaning that anyone can set up a camera, pair it with low-cost ALPR software, record their neighbors’ movements, and sell the data. There is no registry of ALPR systems in use by private associations in our state, no way to know how that data is managed or into whose hands it falls. Even for publicly-owned ALPR systems,

109 Data from 2014. Bellingham Police Department, “WATPA Combined Semi Annual Report: July-December 2014,” 7, January 2015, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/WAPTA_REPORT_2.pdf.

110 Data from 2009-2010. Monroe Police Department, “WATPA Automated License Plate Reader (ALPR) Questionnaire,” 2, 2011, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/ALPR_WATPA_WSU.docx.pdf.

111 Data from 2019. “2019 Reads Statistics Report,” BOSS3, 23, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Read-Misreads-report-3-10-21.pdf>

112 “Street-Level Surveillance,” EFF.

113 Bellingham Police Department, “WATPA Combined Semi Annual Report: July-December 2014,” 7, January 2015, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/WAPTA_REPORT_3.pdf.

114 Bellingham Police Department, “WATPA Combined Semi Annual Report: January-June 2014,” 7, July 2014, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/WAPTA_REPORT_4.pdf.

115 Bellingham Police Department, “Bellingham Police Department Memorandum: Report on ALPR,” March 2, 2015, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2022/11/Memo_ALRP.pdf.

116 Toni Fulton, email message to UWCHR, October 13, 2022.

the responses by many Washington law enforcement agencies to the lawful inquiries by UWCHR researchers should give us pause. Policies governing the retention and sharing of ALPR data are poorly understood and ill enforced, if they are enforced at all; as a result, many Washingtonians' data winds up in the hands of private groups and law enforcement agencies beyond the reach of our state's laws.

If our state is committed to making sure its pledges to provide sanctuary are upheld, we can begin by:

- Conducting audits of all law enforcement ALPR systems operational in Washington state, and making the results publicly available. Most agencies who acquired this technology have already adopted policies that commit them, in principle, to conducting audits. For example, WATPA's policy instructs grantee agencies, "LPR data must be accessible only through a CJIS compliant authentication system which documents who accessed the information by identity, date and time";¹¹⁷ WATPA's interagency agreement binds Washington law enforcement agencies to maintain records available for review by WATPA, the Office of the State Auditor, and/or state and federal officials.¹¹⁸ This means that audits can be performed of this authentication system to gain better understanding of how these technologies are being used, and what dangers they pose to populations whose rights are currently at risk.

117 Washington Association of Sheriffs and Police Chiefs, *Guidelines*, 2017.

118 "Washington Auto Theft Prevention Authority Inter-agency Agreement," 5.

- Conducting audits of the Washington State Patrol's ACCESS system¹¹⁹ to determine the extent to which the "hot lists" it provides to Washington ALPR systems include those suspected of immigration violations¹²⁰ or those suspected of accessing reproductive health services. If suspected civil immigration violations lead a vehicle to be included on a hot list, and state and local law enforcement in Washington act upon such notifications, they likely violate Washington's Keep Washington Working Act.

The practice of wide data-sharing made possible by ALPR technologies means that the confidentiality of data gathered by any one agency is only as sound as the practices of the least protective agency with which it shares information. This means all Washingtonians have an interest in improved policies to address the problem, yet up until now we have relied on piecemeal protections—if any—in each jurisdiction. In our increasingly interconnected world, this no longer makes sense.

119 WATPA's 2008 policy explains that for law enforcement jurisdictions in Washington, "hot list" data for comparison to ALPR data will be provided by "an NCIC hot file via ACCESS (A Central Computerized Enforcement Service System), currently managed by the Washington State Patrol (WSP). NCIC contains national stolen vehicle and plate data published daily by the FBI. The WSP places the NCIC file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information." Washington Association of Sheriffs and Police Chiefs, *Guidelines*, 5, 2008.

120 See, for example, the discussion of NCIC offender categories: Minnesota Department of Public Safety, "License Plate Recognition (LPR) User Guide," October 2009, [https://www.aclu.org/sites/default/files/field_document/alprpra_minnesotastatepatrol_stpaulmn_1%20\(5\).pdf](https://www.aclu.org/sites/default/files/field_document/alprpra_minnesotastatepatrol_stpaulmn_1%20(5).pdf).



Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights | Facebook, Twitter: @uwchr