The Digital Deportation Machine: How Surveillance Technology Undermines Chicago's Welcoming City Policy

June 2021

JUST FUTURES LAW

mijente

OCAD
ORGANIZED COMMUNITIES AGAINST DEPORTATIONS

THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL

ACKNOWLEDGMENTS

Take Back Tech Fellow

Nicole Hallett, University of Chicago Law School

Community Organizing Advisors

Antonio Gutierrez, Organized Communities Against Deportations
Xanat Sobrevilla, Organized Communities Against Deportations
Arianna Salgado

Authors

Jacob Hamburger, University of Chicago Law School
Kathleen Schmidt, University of Chicago Law School

Editors

Kevin Herrera, Just Futures Law
Julie Mao, Just Futures Law

Research Support

Aaron Lackowski
Andy Clarno, University of Illinois, Chicago

Report Design

Jacob Hamburger
Kathleen Schmidt

JUST FUTURES LAW el Comité mijente

TAKE BACK TECH FELLOWSHIP

TABLE OF CONTENTS

INTRODUCTION

The Chicago Police Department (CPD) maintains a vast network of surveillance technologies capable of collecting detailed data about ordinary residents. Using cameras and sophisticated software, police can identify individuals and track their movements. CPD also employs databases that collect thousands of disparate data points under the justification of "predicting" criminal behavior by constructing profiles of who it thinks is likely to be a "gang member." To make use of these various surveillance tools, CPD maintains intelligence centers across Chicago where officers keep a constant watch over the data that the centers collect, in partnership with federal law enforcement agencies.

The sizable trove of information about Chicago residents in the hands of the police creates an enormous danger for the city's immigrant communities. Historically, CPD has been eager to collaborate with Immigration and Customs Enforcement (ICE) as well as other federal agencies to arrest and detain Chicago residents for deportation. After years of intensive organizing by immigrant activists and their allies, the City of Chicago enacted the Welcoming City Ordinance (WCO) in 2012, which limited cooperation with federal immigration authorities. The original WCO prohibited CPD and other city agencies from engaging in immigration enforcement operations—either through direct collaboration on arrests or detention, or by providing information—with ICE based solely on civil immigration violations. But the ordinance had four troubling carveouts: CPD faced no restrictions on collaborating with ICE against individuals with outstanding warrants, felony convictions, or pending felony charges, as well as individuals identified in a law enforcement gang database.

> *CPD continues to use a vast network of surveillance technologies, which ICE can employ to target immigrants despite the WCO's protections.*

In January 2021, thanks to continued pressure by activists, the Chicago City Council passed amendments to the WCO that eliminated these carveouts and provided additional protections against sharing city information with federal agencies. This was an important victory that will provide greater protection for immigrants in Chicago from direct collaboration between city police and federal immigration agencies. The amended WCO goes a long way towards dismantling decades of policy and rhetoric that criminalizes immigrants. It does not mean, however, that the fight to keep immigrant residents safe from deportation is over. CPD continues to use a vast network of surveillance technologies, which ICE can employ to target immigrants despite the WCO's protections.

This report details key aspects of the police surveillance network in Chicago, including secretive "real-time" intelligence centers which deploy technologies that identify and locate individuals, databases that collect, analyze, and store information, and strategic partnerships within and between law enforcement agencies that share and use this information. It highlights the ways in which the amended WCO falls short of protecting Chicago's immigrant communities and demonstrates the need for the City to adopt additional privacy protections to stop data-sharing with ICE that the WCO does not address.

KEY TOPICS EXPLORED

THE CHICAGO FUSION CENTER

The Chicago Fusion Center is also known as the Crime Prevention and Information Center (CPIC). CPIC is a direct partnership between CPD and the Department of Homeland Security (DHS), the agency that houses ICE.[1] CPIC centralizes CPD surveillance and has access to the city's vast network of surveillance cameras, facial recognition, license plate readers, social media surveillance, and various police databases. CPIC was originally created to facilitate collaboration between local and federal officials in antiterrorism matters. Today, CPIC's mandate has expanded to cover a broad array of criminal investigations and general surveillance. DHS's participation in the CPIC raises serious concerns about the implementation and strength of the WCO. CPIC's internal operations are also largely hidden from public view and civilian oversight.

STRATEGIC DECISION AND SUPPORT CENTERS (SDSC)

In the years since CPIC's creation, CPD has expanded its surveillance with new SDSCs in all twenty-two of Chicago's police districts. The SDSCs have similar surveillance capabilities as CPIC. However, because these centers exist at the district level, they allow for more localized surveillance and analysis by police districts, resulting in faster deployment of police officers in response to tech surveillance. It remains unknown whether and to what extent federal agencies including DHS and ICE have access to the twenty-two SDSCs in operation.

INVASIVE TECHNOLOGY AND MASS SURVEILLANCE

CPIC and SDSCs have centralized access to the vast network of surveillance cameras and police body-worn cameras deployed across Chicago. Combined with CPD's use of facial recognition software, this gives law enforcement a powerful tool to track individuals and surveil whole communities. CPIC and SDSCs also use Automatic License Plate Readers (ALPRs), which allow police to locate individuals by cross-referencing license plates scanned by stationary cameras or during traffic stops with other law enforcement databases.

CPD GANG DATABASE

The CPD gang database provides another conduit for information to flow to ICE. CPD promised to dismantle a previous database system designed to identify people suspected of gang involvement after activists demonstrated systemic bias in the system's identification of predominantly Black and Latinx men as "gang members" based on scant evidence. However, the city has yet to implement the promised reformed database, called Criminal Enterprise Information System (CEIS), and CPD continues to rely on the old gang database despite its demonstrated inaccuracies and racial biases. While the recent amendments to the WCO forbid CPD from sharing gang database information with ICE, the newest iteration of the gang database will remain available to partner law enforcement agencies that are not subject to this restriction. As a result, information concerning alleged gang ties collected by CPD may remain available to ICE.

The City of Chicago needs to ensure that the data harvested by surveillance technologies is not used to facilitate deportations through concrete, transparent changes to its approach. To achieve this goal, we suggest a robust implementation of the amended WCO and future legislative efforts to close the loophole for data-sharing by CPD intelligence centers such as CPIC and SDSCs. Furthermore, we must examine why the surveillance systems described in this report exist in the first place, and eliminate tools that have been proven to target poor communities of color, such as the gang database. A truly welcoming city invests in the futures of its Black, Brown, immigrant, and low-income communities, instead of harassing, over-policing, and subjecting them to mass surveillance. Finally, most of how these surveillance technologies and information centers operate remains outside the public view. This surveillance state must ultimately be dismantled, and this process should take place in full, transparent public view.

THE WELCOMING CITY ORDINANCE AND THE DATA-SHARING LOOPHOLE

The Welcoming City Ordinance (WCO), first passed by the City Council in 2012, was a major step forward for immigrants' rights in Chicago. While the city had enacted various policies limiting cooperation with federal immigration enforcement in the past, the WCO for the first time barred CPD from assisting ICE by arresting or detaining immigrants in order to hold them for deportation.[2] However, the original version of the WCO contained four carveouts that gave CPD wide latitude to collaborate with ICE: the ordinance's limitations on collaboration did not apply when the subject of police investigation (1) had an outstanding criminal warrant; (2) had been convicted of a felony; (3) was a defendant in a pending felony case; or (4) was "identified as a known gang member either in a law enforcement agency's database or by his own admission."[3] Due to the disproportionate effects of the criminal punishment system on poor communities of color—as well as the overly broad reach of the city's gang database—these carveouts meant that the WCO did not prevent CPD from working with ICE to deport many of the people that the agency targeted.[4]

In January 2021, following years of organizing by immigrant advocates in the city, the Chicago City Council passed an amendment to the WCO eliminating the four criminal carveouts and further strengthening the law. As a result, CPD is now prohibited in all circumstances from assisting ICE, including Homeland Security Investigations (HSI), and Customs and Border Patrol (CBP) in arresting or detaining a person in order to enforce civil immigration law.[5] The ordinance also forbids granting ICE access to people in CPD custody, and places restrictions on how CPD may communicate with ICE.[6] The elimination of the carveouts is an important victory for immigrants' rights, because it no longer allows police to take advantage of non-citizens' increased exposure to the criminal justice system in order to subject them to the added punishment of the deportation machine.

However, an important loophole remains in the current WCO that allows CPD to assist with ICE investigations. While the WCO bans CPD from "provid[ing] direct access to any database or data-sharing platform" maintained by the city to any federal agency, this ban only applies if CPD determines "that the purpose of such access is for the enforcement of civil immigration law."[7] CPIC's internal policies also allow providing information to outside law enforcement agencies—including ICE—as long as the agency's request provides a "criminal predicate."[8] CPIC does not define the term "criminal predicate, and its Memorandum of Agreement (MOA) with DHS makes no mention of this restriction on sharing information. As a result, if ICE seeks access to surveillance data collected by CPD and claims a tangential connection to a criminal investigation, the WCO and CPIC policy give CPD wide latitude to cooperate fully with ICE. This loophole allows police to share data and collaborate with ICE as long as the agency has a minimal basis to assert some nexus to a "criminal" investigation—or under the MOA, no nexus at all. The line between a criminal and a civil immigration enforcement action is often difficult to distinguish due to concurrent legal jurisdiction, and both can lead to deportation.

THE JANUARY 2021 WCO AMENDMENTS:

- **Prohibits CPD from assisting ICE to arrest or detain people in order to enforce civil immigration law in any situation, eliminating the four "carveouts" that existed in the previous law**
- **Introduces more inclusive language throughout Chicago's Municipal Code, replacing "citizen" with words like "resident" or "person"**
- **Maintains existing bans on responding to ICE requests for information or providing access to police data for civil immigration enforcement purposes**

REAL-TIME INTELLIGENCE CENTERS: DIRECT COLLABORATION BETWEEN CPD AND FEDERAL LAW ENFORCEMENT

Despite the City of Chicago's stated policy of protecting immigrants from federal law enforcement, CPD operates numerous intelligence centers where it collaborates directly with federal agencies, including those tasked with immigration enforcement. Created in order to centralize information on potential terrorist attacks, these centers emerged out of the post-9/11 build-up of surveillance technology. Over the years, their mission has expanded beyond counter-terrorism, using digital surveillance to attempt to predict criminal activity in general, especially in communities of color. The expansion of surveillance technology through these centers puts vast amounts of information in the hands of CPD, which is able to share it directly with ICE and other DHS agencies via the data-sharing loophole.

CHICAGO'S FUSION CENTER: THE CRIME PREVENTION AND INFORMATION CENTER

The first fusion centers were created in 2003 in response to the September 11 terrorist attacks, as law enforcement agencies around the country sought to develop new surveillance tools and inter-agency collaborations. Though operated by local police departments (and sometimes involving collaboration with private entities), fusion centers receive federal funding and establish extensive partnerships with agencies such as DHS—which contains Immigration Customs and Enforcement (ICE), its subdivision Homeland Security Investigations (HSI), and Customs and Border Protection (CBP)—as well as the Federal Bureau of Investigations (FBI). As early as 2007, the American Civil Liberties Union (ACLU) observed that because of the loose regulatory framework governing fusion centers, they quickly experienced a "mission creep," expanding their focus from antiterrorism to an "all crimes, all hazards policy."[9] The project of centralizing surveillance efforts by local police in direct collaboration with federal law enforcement agencies soon became a part of general crime prevention policy.

Chicago's Fusion Center, the Crime Prevention and Information Center (CPIC), was created in 2007. According to the most recent directive governing CPIC, the purpose of the Fusion Center is "to enable local, state, and tribal governments to gather, process, analyze, and share information and intelligence relating to all crimes and hazards."[10] The jurisdiction of CPIC is sweeping and not limited to investigating specific criminal cases. Official policy directs CPIC to maintain a vast amount of situational awareness and surveillance through the City of Chicago such as monitoring "any significant or newsworthy event occurring within the city," "information concerning strikes, labor-management incidents, or union controversies," or "available camera feeds to provide information to field and investigative personnel."[11]

Furthermore, CPIC hosts DHS agents on a full-time basis, as well as personnel from the FBI and the Illinois State Police. The official policy of CPIC is to host personnel from ICE, HSI,[12] and CBP as well as other federal, state, and local agencies to "work in the CPIC on a rotational basis."[13] The existence of a permanent law enforcement collaboration between CPD and DHS including its component agencies ICE and CBP presents a major concern in light of the recent amendments to Chicago's Welcoming Cities Ordinance. As discussed above, under the current WCO, CPD is prohibited from providing access to its surveillance technologies and databases with federal law enforcement agencies—including ICE, CBP, and other DHS agencies—if the purpose is to further a civil, rather than criminal, immigration investigation. As a mass surveillance system, CPIC focuses on maintaining situational awareness of the major daily events in the city—it does not solely conduct criminal investigations.

Providing ICE, its subagency HSI, and CBP with access to the immense surveillance power of CPIC is therefore incredibly dangerous. First, this partnership between CPD and these DHS agencies could simply violate the WCO outright. ICE and CBP regularly conduct civil actions as part of their core missions, and CPIC hosts agents from ICE and CBP at the fusion center on a rotational basis. Presumably, CPIC grants ICE and CBP personnel access to at least some of its databases and surveillance capabilities, which are not exclusively used for criminal investigations but for mass surveillance monitoring of "any significant or newsworthy event" in the city. Such close collaboration provides an opportunity for ICE to coordinate directly with local police officers in arresting and detaining non-citizens for civil immigration enforcement purposes despite the ordinance's ban on such collaboration.

CPIC hosts DHS agents on a regular basis. The existence of a permanent law enforcement collaboration between CPD and ICE presents a major concern in light of the amendments to the Welcoming City Ordinance.

Even if the letter of the WCO is respected, however, the ordinance's broad data-sharing loophole as well as CPIC's request for information policy allow any ICE assertion of a criminal investigation, however tangential, to serve as a pretext for passing information to ICE. This encompasses investigations into immigration-related crimes within ICE's purview that often end in deportations: illegal entry and reentry.[14] A large number of undocumented immigrants could be charged with one or both of these crimes. Other undocumented immigrants could be investigated based on the suspicion that they committed one of these offenses, even if they did not. As a result, ICE effectively has a mandate to investigate virtually any undocumented person as a "criminal suspect" whom it might otherwise target for civil immigration enforcement, even if it does not ultimately charge that person with a crime. While entry and reentry offenses are simply immigration enforcement dressed up as criminal investigations, any other suspected offenses as well as CPIC's general surveillance tactics may also justify sharing information with ICE.

While CPD is barred from sharing information directly with ICE for the purpose of civil immigration enforcement, nothing in the WCO prevents it from sharing information as part of a criminal or security-related investigation. The CPIC Fusion Center provides a channel for direct information-sharing between CPD and ICE as well as other federal law enforcement agencies that may target immigrants. The directive also allows for ICE personnel to work within CPIC on a rotating basis.[15] The existence of a permanent law enforcement partnership and information-sharing project between CPD and DHS is a clear obstacle to Chicago's efforts to end police collaboration with federal immigration enforcement efforts.

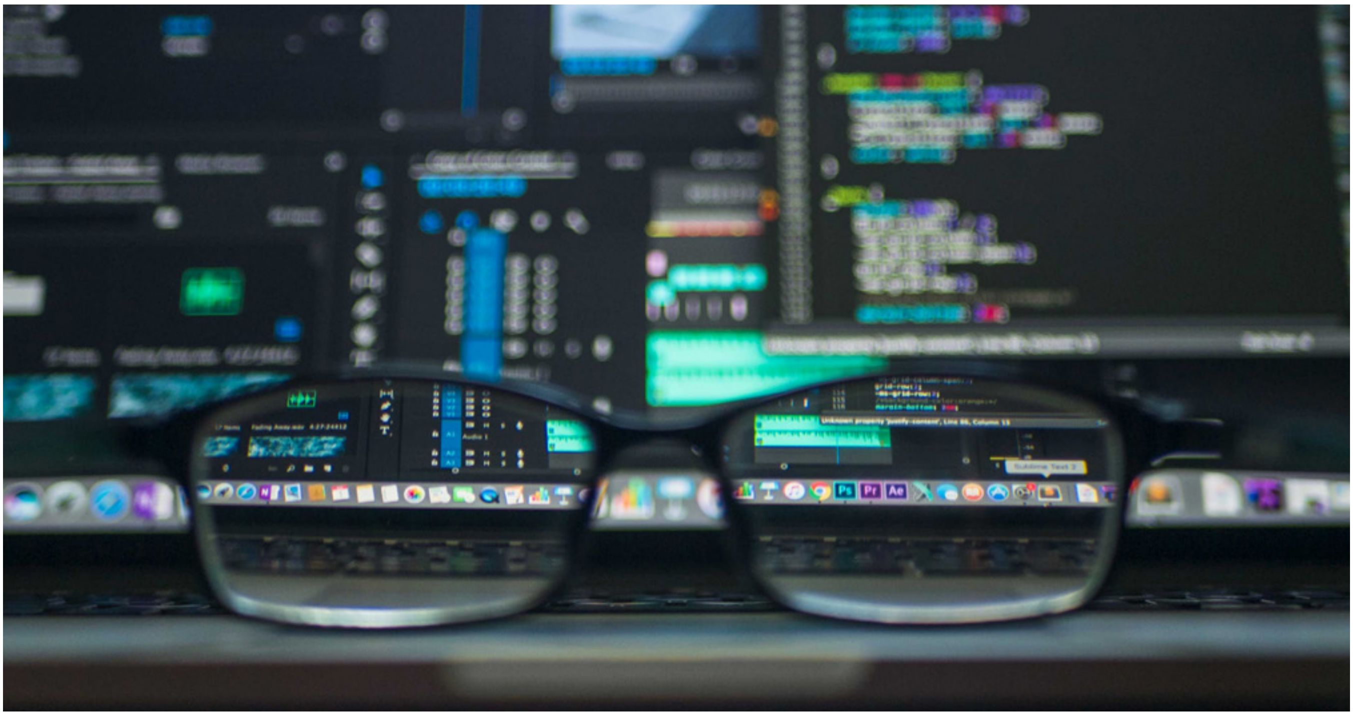
STRATEGIC DECISION AND SUPPORT CENTERS: LOCAL SURVEILLANCE AGGREGATORS

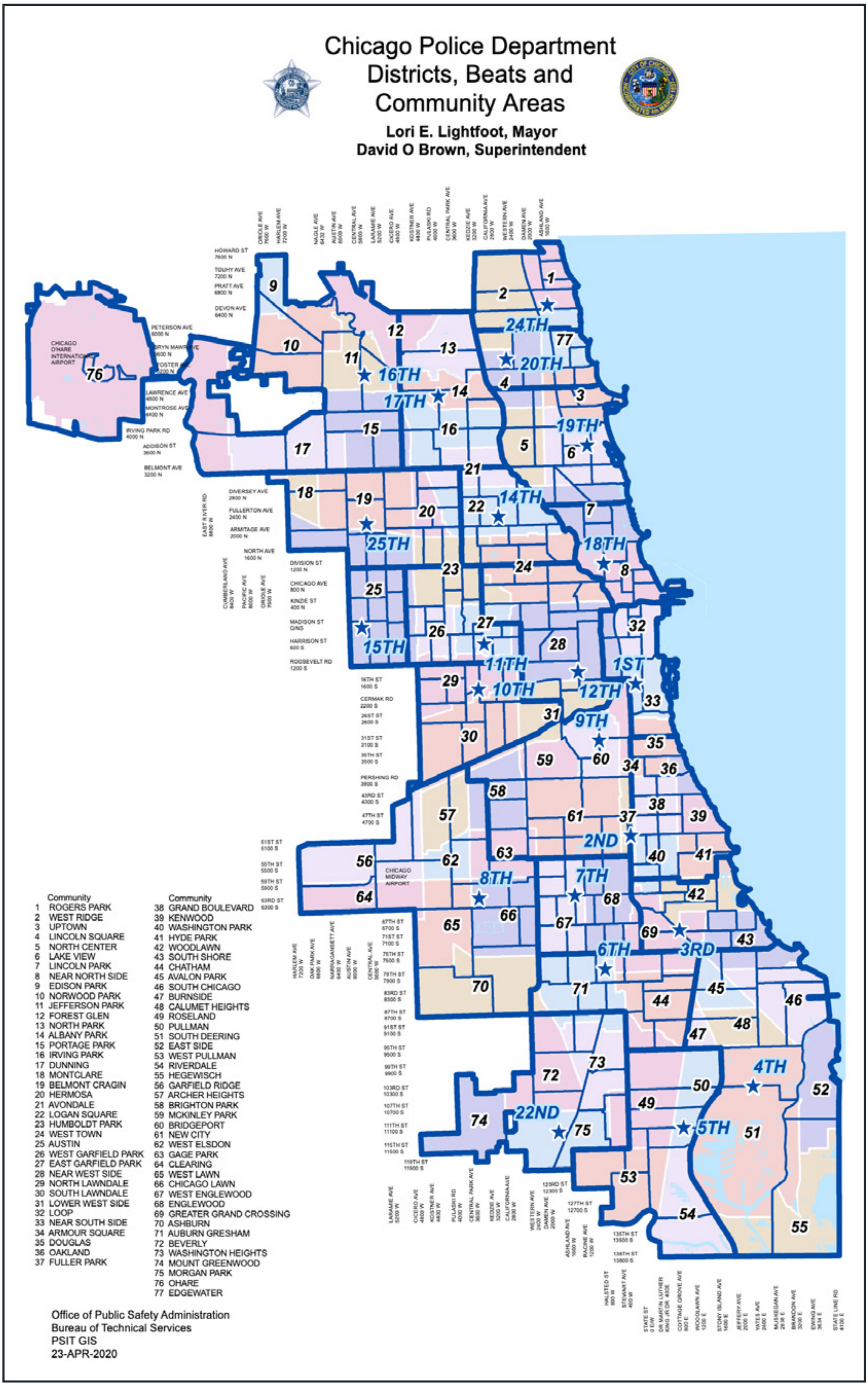
Strategic Decision Support Centers (SDSCs) were created in 2017 in light of the increasing amount of surveillance data processed by CPIC. Additionally, CPD sought to decentralize surveillance data collection for faster police deployment.[16] SDSCs are more localized versions of the CPIC model. There are twenty-two SDSCs in Chicago—one for each district. SDSCs are specialized rooms within CPD district stations that operate around the clock. Most contain four computers and three large screens. They are run by CPD civilian analysts, but there are always two patrol officers and a room supervisor who is either a sergeant or lieutenant.[17]

SDSC analysts collect data from the district using various CPD surveillance technologies, especially street video feed, ALPRs, ShotSpotter (gunshot detection devices), and social media monitoring.[18] Analysts use this information to produce a daily briefing for the district, which police commanders then use to make resource and personnel allocation decisions.[19] Patrol officers in some districts may have access to smartphones that are linked to their district's SDSC, allowing for information collected by the SDSC to be quickly accessed by officers on the ground.[20]

While CPIC and SDSCs both have access to some of the same technologies, such as street cameras, an SDSC focuses on several specific tools deployed in its district, whereas CPIC gathers notifications from many sources on a wide variety of issues throughout the city. SDSCs must report to CPIC any information it gathers involving homicides, shootings, street gatherings, and other newsworthy events that occur in the SDSC's district.[21] Meanwhile, CPIC must forward any real-time, operational information it receives that might need an immediate response to the relevant SDSC.[22] While federal officers can request information from an SDSC, it is more common for federal officers to work with the CPIC, due to its mandate over the entire city of Chicago, rather than a single district, and its emphasis on larger scale threats.

By placing surveillance tools like ALPRs and ShotSpotter in each city police district, SDSCs fuel over-policing in certain neighborhoods, and cause increased psychological harm to residents.[23] In addition, by taking responsibility for local surveillance, SDSCs enhance CPIC's ability to process the information it receives. Finally, because SDSCs share the information they collect with CPIC, SDSCs broaden the scope of CPIC's mission creep and CPD's surveillance network.





Chicago Police Department
Districts, Beats and
Community Areas

Lori E. Lightfoot, Mayor
David O Brown, Superintendent

Community		Community	
1	ROGERS PARK	38	GRAND BOULEVARD
2	WEST RIDGE	39	KENWOOD
3	UPTOWN	40	WASHINGTON PARK
4	LINCOLN SQUARE	41	HYDE PARK
5	NORTH CENTER	42	WOODLAWN
6	LAKE VIEW	43	SOUTH SHORE
7	LINCOLN PARK	44	CHATHAM
8	NEAR NORTH SIDE	45	AVALON PARK
9	EDISON PARK	46	SOUTH CHICAGO
10	NORWOOD PARK	47	BURNSIDE
11	JEFFERSON PARK	48	CALUMET HEIGHTS
12	FOREST GLEN	49	ROSELAND
13	NORTH PARK	50	PULLMAN
14	ALBANY PARK	51	SOUTH DEERING
15	PORTAGE PARK	52	EAST SIDE
16	IRVING PARK	53	WEST PULLMAN
17	DUNNING	54	RIVERDALE
18	MONTCLARE	55	HEGEWISCH
19	BELMONT CRAGIN	56	GARFIELD RIDGE
20	HERMOSA	57	ARCHER HEIGHTS
21	AVONDALE	58	BRIGHTON PARK
22	LOGAN SQUARE	59	MCKINLEY PARK
23	HUMBOLDT PARK	60	BRIDGEPORT
24	WEST TOWN	61	NEW CITY
25	AUSTIN	62	WEST ELSDON
26	WEST GARFIELD PARK	63	GAGE PARK
27	EAST GARFIELD PARK	64	CLEARING
28	NEAR WEST SIDE	65	WEST LAWN
29	NORTH LAWNDALE	66	CHICAGO LAWN
30	SOUTH LAWNDALE	67	WEST ENGLEWOOD
31	LOWER WEST SIDE	68	ENGLEWOOD
32	LOOP	69	GREATER GRAND CROSSING
33	NEAR SOUTH SIDE	70	ASHBURN
34	ARMOUR SQUARE	71	AUBURN GRESHAM
35	DOUGLAS	72	BEVERLY
36	OAKLAND	73	WASHINGTON HEIGHTS
37	FULLER PARK	74	MOUNT GREENWOOD
		75	MORGAN PARK
		76	OHARE
		77	EDGEWATER

Office of Public Safety Administration
Bureau of Technical Services
PSIT GIS
23-APR-2020

INVASIVE SURVEILLANCE TECHNOLOGIES USED BY REAL-TIME INTELLIGENCE CENTERS

SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

The most recent available estimates suggest CPD has access to thousands of cameras throughout the Chicago area. According to the Associated Press, **Chicago has the largest network of surveillance cameras of any city in the U.S., with 35,000 cameras in 2019.**[25] Former DHS Secretary Michael Chertoff even praised Chicago for having the most "extensive and integrated camera network" in the U.S.[26] These cameras include[27]:

- **Blue light cameras placed in strategic locations throughout the city**
- **Cameras in public transit locations including those operated by Chicago Transit Authority (CTA) and the Transportation Security Administration (TSA)**
- **Cameras in schools and operated by Chicago Public Schools (CPS)**
- **Cameras in Chicago Housing Authority residential buildings and in public places**
- **Private security cameras to which CPD has gained access via an initiative through the Office of Emergency Management and Communications**
- **Traffic cameras**
- **Police dashboard cameras**
- **Body-worn cameras carried by CPD officers**

CPD couples this vast network of surveillance cameras with facial recognition software that can identify individuals on surveillance cameras, photos, and across social media. Facial recognition software is a fast-developing component of police departments' technological arsenals. This technology has the capacity to analyze the vast number of photos that exist on the Internet and in other electronic sources available to police, and use this information to compare and identify a person captured by photo or video.

The ubiquity of surveillance cameras combined with the city's use of facial recognition technology has given rise to fears that CPD could identify individuals subject to immigration enforcement in real time, including at public protest actions, and that this information may become available to ICE despite the restrictions in the WCO. This fear is well founded given CPIC and SDSCs roles in surveilling protesters. For example, in 2018, CPIC submitted reports to ICE about protesters who had gathered in Chicago to call for abolishing the agency. During this time, CPIC had access to facial recognition technology developed by Clearview AI, which compares surveillance images with billions of photos from across the Internet, including social media photos.[24]

Clearview AI ended its contract with the City of Chicago in April 2020 in anticipation of litigation under Illinois's Biometric Information Privacy Act. However, CPD still has access to facial recognition software provided by another developer, Dataworks Plus. Using Dataworks Plus, CPD officers can compare surveillance images to photos in the Chicago Mugshot Database, although CPD training documents state that this technology is not to be used for real-time identification. Even this more limited technology remains a concern, however, since officers retain the ability to compare CPD's own mugshot images against photos posted to social media and historical video data from surveillance cameras.

How does this technology fuel deportations?

Facial recognition technology is a powerful tool that CPD can use to identify individuals based on surveillance images or social media posts. CPIC is the agency with access to and responsible for monitoring this vast network of surveillance cameras, and has authority to operate facial recognition technology. Moreover, CPIC grants access to ICE, CBP or other federal agencies to the center. There is serious concern that this technology and data can be accessed by DHS component agencies enforcing immigration law and put individuals at risk of immigration enforcement. Additionally, CPIC has a history of using facial recognition technology to target and retaliate against activists who oppose deportation and the carceral immigration enforcement system. CPD's record of collaborating with DHS to surveil immigration-related protest activity suggests that this technology will remain a pressing concern despite the restrictions of the WCO.

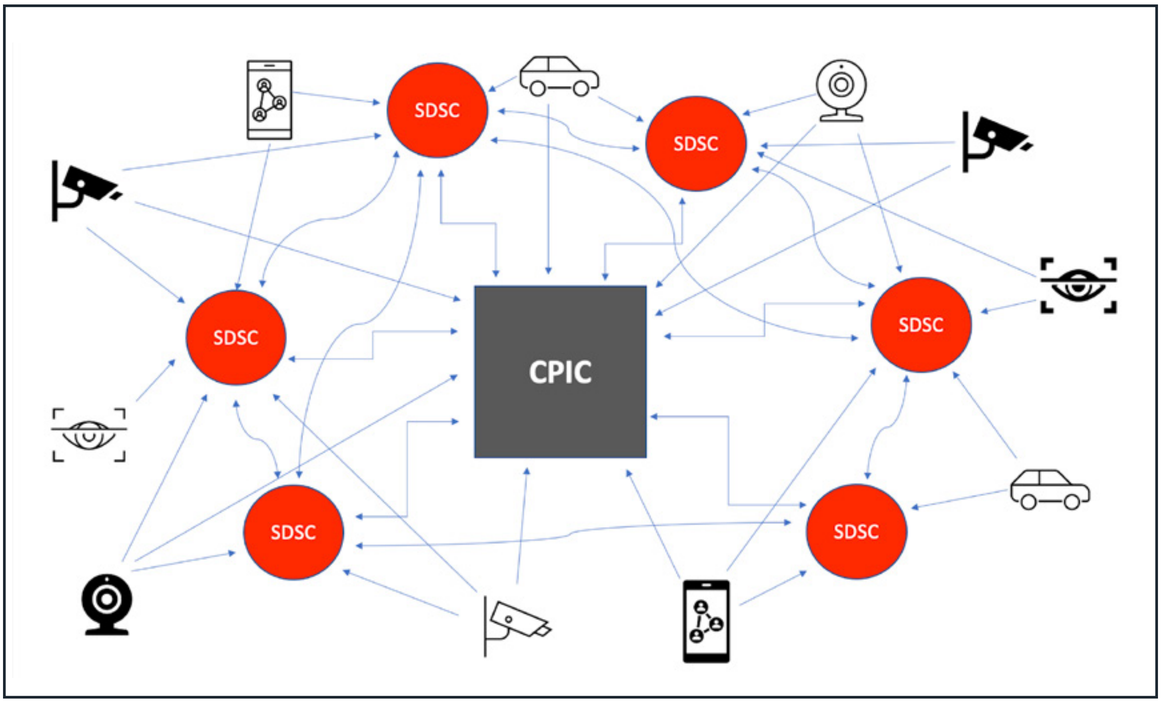
AUTOMATIC LICENSE PLATE READERS

Automatic License Plate Readers (ALPR) are a technology that scans car license plates and compares the plate numbers against local and national databases (known as "hot lists"). Databases can include those for stolen vehicles, AMBER Alerts, or gang databases.[28] ALPRs log the time and date of the scan, the GPS coordinates of the car, and a picture of the vehicle.[29] CPD retains ALPR scans for one year.[30] This information is stored in a database called the Law Enforcement Archival and Reporting Network (LEARN). Both LEARN and the ALPR technology itself are products of Vigilant Solutions, which is part of Motorola Solutions.[31] The ALPR data collected by CPD and stored in LEARN is under the command of the CPIC.[32] ALPRs are located throughout the state of Illinois. Their pervasiveness in both Chicago and Illinois, combined with the nature of the data collected—dates, times, and locations—along with their year-long retention in LEARN means that CPD can develop detailed knowledge of drivers' whereabouts and routines. ALPR data is also used frequently by SDSCs, where it can be combined with other technologies like ShotSpotter or street video surveillance and sent to officers' smartphones in real time.

In Chicago, 240 ALPRs are placed inside police vehicles, to be used during traffic stops. When a police officer pulls a car over, the ALPR scans the license plate of the stopped car to search local and national databases. This information is transmitted to the officer in the car in real time. In addition to vehicle-mounted ALPR, there are an unknown number of fixed ALPRs, which are permanently attached to a structure like a pole or bridge. There are also portable ALPRs that can be moved as needed.[33] In 2019 alone, these ALPRs collected the data from the license plates of more than 179 million people in Chicago.[34]

How does this technology fuel deportations?

By scanning, photographing, and logging the license plates of each passing vehicle, ALPRs provide law enforcement with roadmaps of people's lives. ICE could gain access to LEARN (housed within CPIC) via information requests sent to CPIC. If this is the case, and CPIC grants the requests (using the data-sharing loophole for example), ICE could use the LEARN database containing all of Chicago's ALPR scans to investigate, track, detain, and deport immigrants. Indeed, ICE has a history of using ALPR data to locate those targeted for civil immigration enforcement.[35]



CRIMINAL ENTERPRISE INFORMATION SYSTEM (GANG DATABASE)

The Chicago Police Department maintains a patchwork of twenty-seven different databases, visualization tools, and computer applications where gang information is entered, stored, and accessed.[36] This collection of tools is collectively and popularly known as the CPD "gang database." In 2019, after organizing campaigns, legal challenges, mounting public pressure, and a scathing report from the Office of the Inspector General (OIG), CPD announced that it would create a replacement for the gang database, to be called the Criminal Enterprise Information System (CEIS). CPD claimed that the CEIS would solve the most blatant constitutional violations of the original gang database, which had been highlighted by activists and the OIG report. Two years after CPD made this commitment, however, the Department has made minimal efforts toward creating the CEIS system and continues to rely on the old gang database system.

The gang database was shared with over 500 external agencies, including immigration officials. Between 2009 and 2018, external agencies made over one million searches in the gang database systems. Immigration agencies accounted for 32,224 of those searches.[37] While the version of the WCO in place at the time offered protections from ICE for undocumented immigrants, an undocumented immigrant designated as a gang member in the gang database system lost WCO protection.[38] Gang designation also creates barriers to those seeking immigration relief through Deferred Action for Childhood Arrivals (DACA) and other forms of relief that allow undocumented immigrants to stay in the United States or seek more permanent immigration status.[39]

DHS made 32,224 searches in the gang database between 2009 and 2018. Despite its promises, CPD has made few efforts to replace it.

The gang database contains well-documented inaccuracies and often does not include sufficient information to determine whether someone has an affiliation with a gang or not. For example, 15,174 individuals were designated as gang members, but no gang was listed on the Gang Arrest Card.[40] On 24,151 Gang Arrest Cards, no reason was given for why a person had been designated as a gang member.[41] Almost sixteen percent of those designated as a gang member had multiple birthdates listed in the database. People as young as nine and as old as seventy-five were designated as gang members.[42] Furthermore, CPD had no mechanism to correct inaccurate data or delete false data.[43] CPD did not require any review or approval of a gang member designation.[44] Once a person has been designated as a gang member, they are not informed. Even if they are able to learn that they have been designated, there is no way to appeal a gang designation.[45] On top of these inaccuracies, the gang database disproportionately targets people of color. Ninety-five percent of the 134,242 people designated as gang members are Black or Latinx.[46] Individuals classified as Black or African American by CPD made up 69.8 percent of those identified as gang members, while only 30.5 percent of Chicago residents are Black or African American.[47] Meanwhile, 32.7 percent of Chicago's population is white, yet only four percent of individuals in the gang database were identified as white.[48]

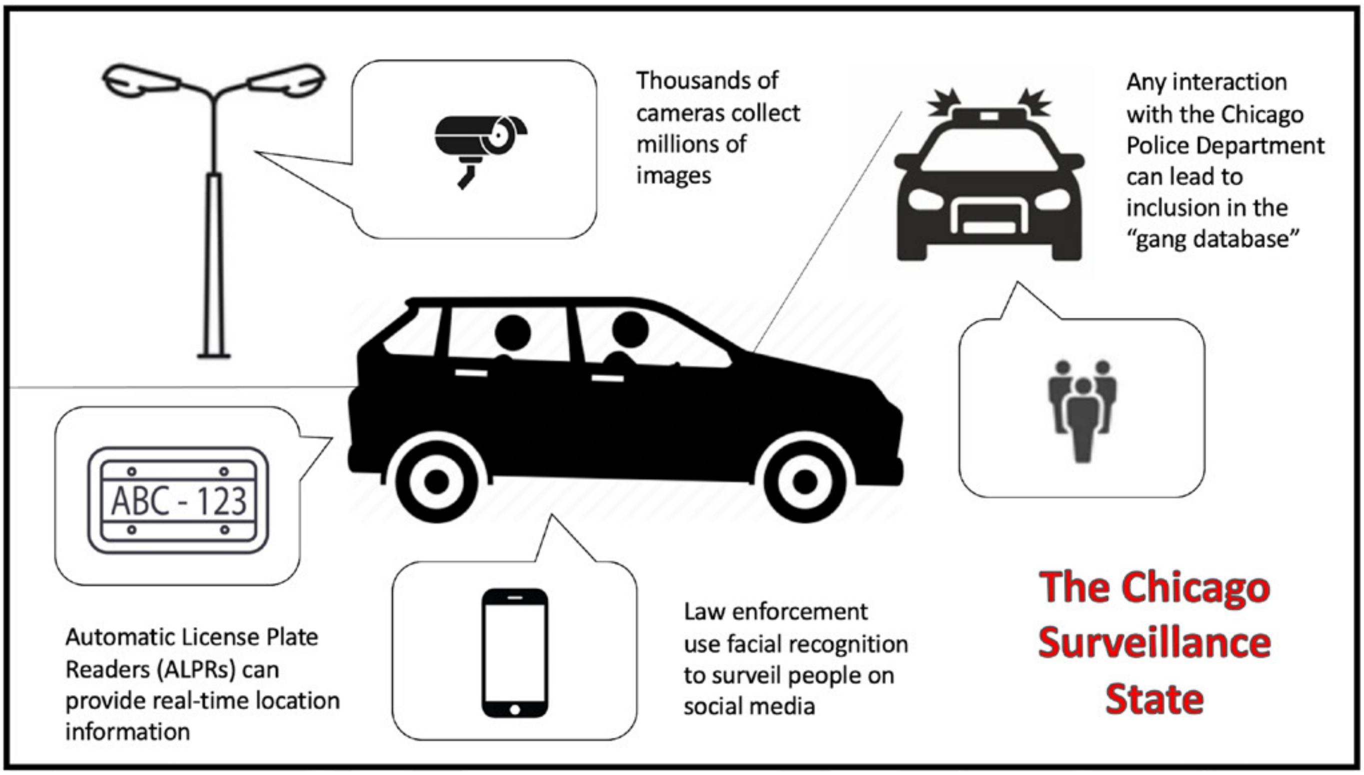
CPD acknowledged many of the problems highlighted by the OIG report. In reaction to the report and community pressure, CDP agreed to fully implement eighteen of the OIG's twenty-seven recommendations, agreed to partially implement eight more, but rejected one.[49] Most importantly, CPD proposed a new database that would be a single, unified location for gang information. The new system would ostensibly assure that the information be updated and vetted, would purge outdated information, and would create a process for the public to find out if they are in the database and appeal their designation if they were.[50] CPD also said that it would create regulations on information sharing with third parties. In February 2020, CPD proposed the Criminal Enterprise Information System (CEIS) as the mechanism to carry out the database reforms. On October 29, 2020, CPD Superintendent David Brown admitted that the transition from the old gang database system to the new CEIS was still ongoing.[51]

A follow-up OIG report released on March 31, 2021 has found that CPD has, in fact, made few efforts to develop a new gang database with the promised safeguards in place. Specifically, CPD has not committed to a timeline for the completion of the CEIS. No managerial responsibility for the project has been assigned.[52] There is confusion within CPD over the drafting status of the proposal creating the CEIS, which has been through several iterations. The drafting order itself is unclear on how CEIS will work in practice and how it will address community concerns. Finally, CPD is continuing to collect and rely on seriously flawed data.

STOP THE SURVEILLANCE OF BLACK AND BROWN CHICAGOANS
ERASE THE GANG DATABASE
ALTO A LA VIGILANCIA DE COMUNIDADES DE COLOR

How does this technology fuel deportations?

As of the writing of this report, CPD does not have an actual operational system to replace the gang database.[53] Because of this, the concerns and problems with the original gang database and its relationship to immigration enforcement persist. The 2021 amendments to the WCO, which removed the gang carveout,[54] are a step in the right direction, but it is unclear whether CPD has cut off ICE's access from the gang database or how CPD ensures that ICE is not accessing the data for civil immigration enforcement purposes. If ICE has access to the gang database, it could look to see if a person has been designated as a gang member. If they have been, then they could be denied DACA or other immigration relief.[55] The gang database can also be used as a tool to track or locate immigrants, and then target them for deportation.[56] And because CPD continues to rely on the old gang database system with its many documented inaccuracies and biases as it makes minimal progress toward the new CEIS, the problems of the old system persist and the risk of deportation of undocumented immigrants may be compounded by the data-sharing loophole.


Thousands of cameras collect millions of images
Any interaction with the Chicago Police Department can lead to inclusion in the "gang database"
ABC - 123
Automatic License Plate Readers (ALPRs) can provide real-time location information
Law enforcement use facial recognition to surveil people on social media
The Chicago Surveillance State

RECOMMENDATIONS AND CONCLUSION

A true welcoming city is one that invests in and protects all of its residents. The City of Chicago must ensure that the many surveillance technologies deployed by CPD throughout the city are not used to deport people from Chicago's immigrant community. To achieve this goal, we suggest a robust implementation of the amended WCO and future legislative efforts. In addition, the City of Chicago must halt the ever-expanding web of surveillance technology blanketing the city, and instead move toward dismantling this surveillance for the sake and safety of all its residents—especially immigrants.

First, the data-sharing loophole in the WCO must be closed, lest it become an exception that swallows the rule. The amended WCO provides essential protections from information-sharing with ICE for those who might be subject to civil immigration enforcement. But for others who might be subject to criminal immigration investigation for unauthorized reentry, all WCO protection evaporates. Under the aegis of conducting a criminal investigation, ICE could access myriad CPD databases and technologies to investigate and deport undocumented Chicagoans. While we advocate for federal decriminalization of immigration offenses, in the meantime and at the local level, the City of Chicago can protect its immigrant community by closing the data-sharing loophole in the WCO. An amendment to Section 030(b) of the WCO should explicitly forbid CPD from granting federal agents' requests for information or to access city digital platforms in order to investigate illegal entry (8 U.S.C. § 1325) and illegal reentry (8 U.S.C. § 1326) offenses. The amendment should also ban complying with requests for information or granting this access to ICE as well as CBP for any reason, including conducting generalized surveillance.

Second, CPD should abandon the gang database/CEIS system entirely. CPD has made very few efforts to actually establish the CEIS. The project lacks purpose, direction, and commitment. CPD has not explained how it will solve the problems that plague the current gang database system by establishing the CEIS. As CPD drags its feet on gang database changes, it continues to rely on the inaccurate and biased gang database that was the focus of so much community activism, litigation, and several OIG reports—the findings of which CPD itself largely agreed. Instead of this halfhearted attempt to reform a system riddled with problems and of dubious utility, CPD should abolish the gang database system entirely.

Finally, CPD's information centers and use of digital surveillance technology in general must be made fully transparent. There is very little publicly available information on the full extent of the technologies used by police and federal agency personnel at CPIC and the SDSCs, or on how these centers operate. If CPD and the city's civilian leadership believe that these technologies and institutions are truly vital to keeping Chicagoans safe, they should be prepared to explain why and how. The City of Chicago must defund, decriminalize, and decarcerate. Chicago should invest in the futures of its residents, instead of subjecting them to harassment, over-policing, and mass surveillance. The City must do more to restrain and dismantle CPD's surveillance web so as to ensure that its residents do not risk deportation by federal immigration authorities.

> “
> ***The City of Chicago must defund, decriminalize, and decarcerate. Chicago should invest in the futures of its residents, instead of subjecting them to harassment, over-policing, and mass surveillance.***

ENDNOTES

[1] Chicago Police Department, “Crime Prevention and Information Center (CPIC),” Special Order S03-04-04 (August 10, 2020), available at ***http://directives.chicagopolice.org/directives/data/a7a57bf0-13ed7140-08513-ed71-4cecd9c-378c05dec.html*** (accessed May 21, 2021).

[2] Welcoming City Ordinance, Municipal Code of Chicago, 2-173 §§ 042(a)-(b) [Added Coun. J. 9-12-12, p. 33041, § 1].

[3] Welcoming City Ordinance, Municipal Code of Chicago, 2-173 §§ 042(c) [Added Coun. J. 9-12-12, p. 33041, § 1].

[4] See section IV below for more information on the gang database.

[5] Welcoming City Ordinance, Municipal Code of Chicago, 2-173 § 020(a).

[6] Welcoming City Ordinance, Municipal Code of Chicago, 2-173 §§ 020(a)(2), (b).

[7] Welcoming City Ordinance, Municipal Code of Chicago, 2-173 § 043(c).

[8] Chicago Police Department Deployment Operations Center, Special Order 11-08, Crime Prevention and Information Center (CPIC) Fulfillment of Requests for Information (January 12, 2011).

[9] American Civil Liberties Union, “What’s Wrong with Fusion Centers?” (December 2007).

[10] Chicago Police Department, Special Order S03-04-04, Crime Prevention and Information Center (CPIC). Emphasis added.

[11] Id. Emphasis added.

[12] HSI is an investigative agency housed within ICE and carries out both criminal and civil immigration investigations.

[13] Chicago Police Department, Special Order S03-04-04, Crime Prevention and Information Center (CPIC).

[14] 8 U.S.C. §§ 1325, 1326.

[15] Chicago Police Department, Special Order S03-04-04, Crime Prevention and Information Center (CPIC).

[16] John S. Hollywood, et al., "Real-Time Crime Centers in Chicago: Evaluation of the Chicago Police Department’s Strategic Decision Support Centers," RAND Corporation, 17, (2019), available at ***https://www.rand.org/pubs/research_reports/RR3242.html*** (accessed May 21, 2021).

[17] Chicago Police Department, Special Order S03-02-01, Strategic Decision Support Centers: Operations and Accountability (July 26, 2019), available at ***http://directives.chicagopolice.org/directives/data/a7a57b85-16c2efbe-c2416-c2fa-edbba6051837c01c.html?hl=true*** (accessed May 21, 2021).

[18] Id. at IV.A.

[19] See Id. at IV; compare to Chicago Police Department, Special Order S03-04-04, Crime Prevention and Information Center (CPIC) at IV.E-G.

[20] Chicago Police Department, Special Order S03-02-01, Strategic Decision Support Centers: Operations and Accountability.

[21] Id. at V.C.3.

[22] Id. at V.H.1.

[23] Abigail Sewell, et al., "Living Under Surveillance: Gender, Psychological Distress, and Stop-Question-and-Frisk Policing in New York City," Social Science & Medicine (April 22, 2016).

[24] Open the Government, "The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers," available at ***https://www.openthegovernment.org/dhs-fusion-centers-full-report/*** (last consulted April 11, 2021); Tom Schuba, "CPD Using Controversial Facial Recognition Program that

[16] Scans Billions of Photos from Facebook, Other Sites," Chicago Sun Times (January 29, 2020), available at ***https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd*** (last consulted April 5, 2021); Ryan Mac, et al., "Surveillance Nation," Buzzfeed News (April 6, 2021), available at ***https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition*** (accessed April 28, 2021).

[25] Mitch Dudek, "New phones will let Chicago beat cops tap the city's 35,000 surveillance cameras," Chicago Sun Times (August 21, 2019), available at ***https://chicago.suntimes.com/2019/8/21/20827153/chicago-police-officers-samsung-smartphones-surveillance-cameras-pilot-program*** (accessed April 28, 2021).

[26] "Chicago's thousands of surveillance and 'red light' smart cameras," WBEZ Chicago (March 12, 2012), available at ***https://www.wbez.org/stories/chicagos-thousands-of-surveillance-and-red-light-smart-cameras/64125112-7e57-41a4-b144-944206a26e99*** (accessed April 21, 2021).

[27] See Chicago Police Department, Special Order S03-04-04, Crime Prevention and Information Center (CPIC); Lucy Parsons Labs, "Police Surveillance in Chicago: Video Surveillance," available at ***https://www.redshiftzero.com/policesurveillance/tactics/video-surveillance.html*** (last consulted April 11, 2021); Office of Emergency Management and Communications, "Link Your Cameras into OEMC (Private Sector Camera Initiative)," available at ***chicago.gov/city/en/depts/oem/provdrs/tech/svcs/link_your_cameras.html*** (last visited April 11, 2021).

[28] Angel Diaz and Rachel Levinson-Waldman, "Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use," Brennan Center for Justice (Sept. 10, 2020).

[29] Id.

[30] Chicago Police Department, Special Order S03-20, Automated License Plate Reader (ALPR) Systems (April 23, 2018), available at ***http://directives.chicagopolice.org/CPDSergeantsExam_2019/directives/data/a7a57b85-162f3a0b-bf716-2f3a-0f157507dc6ad98b.html*** (accessed May 21, 2021).

[31] Motorola Solutions, License Plate Recognition (LPR) Camera Systems, available at ***https://www.motorolasolutions.com/en_us/video-security-analytics/license-plate-recognition-camera-systems.html?utm_source=vigilantsolutions.com&utm_medium=referral&utm_campaign=vigilantsolutions_redirect*** (accessed May 21, 2021).

[32] Chicago Police Department, Department Notice D13-12, Law Enforcement Archival and Reporting Network (LEARN) – Pilot Program (Sept. 12, 2013), available at ***http://directives.chicagopolice.org/CPDSergeantsExam_2019/directives/data/a7a57bf0-14107ef9-14c14-107e-fe790a4a652a3d37.html*** (accessed May 21, 2021).

[33] Chicago Police Department, Special Order S03-20, Automated License Plate Reader (ALPR) Systems.

[34] Michael Buresh, "Discriminatory Placement of Chicago's Automated License Plate Reader Cameras," Transparency Chicago (December 23, 2020), available at ***https://www.transparencychicago.org/blog/the-discriminatory-placement-of-chicagos-automated-license-plate-reader-cameras#_ftn1*** (accessed May 17, 2021).

[35] Department of Homeland Security, Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service (March 19, 2015), available at ***https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf*** (accessed May 21, 2021).

[36] City of Chicago Office of the Inspector General, Review of the Chicago Police Department's "Gang Database (April 2019), 2, available at ***https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf*** (accessed May 21, 2021).

[37] Id. at 25.

[38] Id. at 28.

[39] The January 2021 amendment to the WCO eliminated this loss of protection. See infra.

[40] Office of the Inspector General, Review of the Chicago Police Department's "Gang Database," 38. When a CPD officer arrests a person who they believe to be a gang member, or who admits to being a gang member, the officer may fill out and file a Gang Arrest Card, which is then entered into a database. While there are eighteen different CPD forms and systems to report gang information, the Gang Arrest Card is a common method. Id. at 31.

[41] Id. at 39.

[42] Id. at 47.

[43] Id. at 43.

[44] Id.

[45] Id. at 46.

[46] Id. at 44.

[47] Id. at 34.

[48] Id. at 35.

[49] City of Chicago Office of the Inspector General, Follow-Up Inquiry on the Chicago Police Department's "Gang Database," (March 2021), 10, available at ***https://igchicago.org/wp-content/uploads/2021/03/OIG-Follow-Up-Inquiry-on-the-Chicago-Police-Departments-Gang-Database.pdf***. CPD rejected extra protections for juveniles (accessed May 21, 2021).

[50] Id. at 10.

[51] Id. at 11.

[52] Id. at 21. When OIG informed CPD of the imminent release of the follow-up report, CPD's Office of Legal Affairs notified OIG that two members of CPD had been newly assigned managerial responsibility over the CEIS project, that an outside vendor had been selected to build the CEIS and that its work "build[ing] out" the CEIS was nearly finished.

[53] Id. at 35, 37.

[54] Id. at 24.

[55] See United States Citizenship and Immigration Services, Consideration of Deferred Action for Childhood Arrivals (DACA), available at ***https://www.uscis.gov/humanitarian/consideration-of-deferred-action-for-childhood-arrivals-daca*** (accessed May 21, 2021).

[56] Jacqueline Serrato, Chicago Police Admits Gang Database Error That Enabled ICE Raid, Chicago Tribune (Dec. 6, 2017), available at ***https://www.chicagotribune.com/hoy/ct-chicago-police-admits-gang-database-error-20171206-story.html*** (accessed May 21, 2021).

IMAGE CREDITS

"Surveillance" by Jonathan McIntosh (CC BY-SA 2.0)

"Caméra de vidéo-surveillance" by zigazou76 (CC BY 2.0)

"Surveillance" by Jonathan McIntosh (CC BY-SA 2.0)

"Sanctuary for All" by Organized Communities Against Deportations (Used with permission)

"Fusion Centers in Illinois" by ACLU of Illinois (Fair use)

"Black Framed Eyeglasses in Front of Laptop Computer" by Kevin Ku from Pexels

"Community Map" by Chicago Police Department (Fair use)

"Erase the Database" by Organized Communities Against Deportations, BYP100, Mijente (Used with permission)