Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 2 Article 4

2013

Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy

Adam Schwartz American Civil Liberties Union of Illinois

Recommended Citation

Adam Schwartz, Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy, 11 Nw. J. Tech. & INTELL. PROP. 47 (2013).

https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss2/4

This Article is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy

Adam Schwartz



January 2013 VOL. 11, NO. 2

 $\P 1$

¶2

¶3

¶4

Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy

By Adam Schwartz*

Introduction

The City of Chicago has our nation's most "extensive and integrated" network of government video surveillance cameras, according to former U.S. Homeland Security Secretary Michael Chertoff. The City probably has access to somewhere between 10,000 and 20,000 publicly and privately owned surveillance cameras. In downtown Chicago, virtually every segment of the public way is under constant video surveillance. These cameras have powers that greatly exceed ordinary powers of human observation, including automatic tracking of cars, and magnification of small objects at great distances.

In February 2011, the American Civil Liberties Union of Illinois (ACLU) published the first large-scale, independent analysis regarding this growing threat to our privacy. The ACLU report called for a moratorium on the expansion of Chicago's camera system, pending a thorough and open review of this system, including inquiry into whether to remove any cameras. The ACLU report also proposed new privacy rules for all cameras. Most importantly, the ACLU sought a criminal predicate before targeting any particular civilians: reasonable suspicion to aim a camera at protesters, leafleters, and the like; reasonable suspicion to magnify anyone; and probable cause to automatically track anyone in their car.²

Subsequently, a new Chicago police written policy adopted two of the ACLU's proposed camera rules. First, officers may only use the cameras to monitor areas "where no legally protected reasonable expectation of privacy exists." Second, officers may not base "the use of video enhancement or tracking capabilities on individual characteristics" such as race or national origin.⁴

Unfortunately, in the year since the ACLU published its report, the situation has not otherwise improved. Chicago has not adopted the ACLU's core proposals regarding a criminal predicate for automatic vehicular tracking or magnification. Moreover, the City

^{*} Senior Staff Counsel, American Civil Liberties Union of Illinois

¹ Don Babwin, Cameras Make Chicago Most Closely Watched U.S. City, ASSOC. PRESS, Apr. 6, 2010.

² ACLU of Illinois, Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy, Feb. 2011 (hereinafter ACLU camera report), available at http://il.aclu.org/site/DocServer/Surveillance_Camera_Report1.pdf?docID=3261. See also, e.g., Erin Meyer, ACLU: Chicagoans Among Most-Watched Citizens in U.S., CHI. TRIB., Feb. 8, 2011; Fran Spielman, ACLU Wants City to Stop Putting Up Cameras, CHI. SUN-TIMES, Feb. 8, 2011.

³ ACLU camera report, supra note 2, at 5, 23.

⁴ ACLU camera report, supra note 2, at 4-5, 22-23; Chicago Police Department General Order G03-05 (eff. Feb. 22, 2012) at Parts II(B)(3) & (4).

has installed thousands of new cameras, and announced plans to install even more. Further, a new City ordinance granted the Mayor new power to purchase and install cameras absent City Council approval or review. Also, the Illinois General Assembly failed to enact a bill that would have required state and local government to disclose their total numbers of cameras.

Part I of this article describes the ubiquity, integration, and technological power of Chicago's video surveillance camera system. Part II discusses the lack of government transparency regarding that system.

Part III sets forth the civil liberties dangers posed by Chicago's video surveillance cameras. Most disturbingly, the unregulated use of these cameras can violate our privacy: if the government systematically monitors *where* we are in public places, the government will learn *who* we are. Reasonable people do not expect government officials to monitor whether they are entering a political or union meeting, viewing a controversial movie or art exhibit, visiting a psychiatrist or a fertility clinic or a plastic surgeon, attending church or mosque or synagogue, distributing leaflets, or meeting a criminal defense attorney. Video surveillance cameras are just one part of a larger surveillance infrastructure that empowers the government, if it chooses, to turn all of our lives into open books for official scrutiny. Moreover, government surveillance cameras chill and deter free speech and assembly, can be misused by government employees, and squander scarce law enforcement resources.

Part IV responds to the assertion that Chicago's surveillance cameras make us safer. Part V explains the ACLU's proposed privacy safeguards. Part VI briefly addresses the City's separate red light and speeding cameras.

I. CHICAGO'S SURVEILLANCE CAMERA SYSTEM

Chicago's system of video surveillance cameras has three critical features: their vast numbers, their tight integration, and their powerful abilities to gather and analyze information. Together, these features empower City government to monitor anyone automatically, quickly, easily, inexpensively, and surreptitiously, in all public places and at all times.

A. Vast Numbers

When the ACLU published its February 2011 report, the best estimate was that the City of Chicago owned or had access to 10,000 cameras. Many Chicago agencies own and operate cameras directed at the public way, including the Police Department, the Transit Authority, the Public Schools, the Park District, the Housing Authority, the O'Hare and Midway airports, McCormick Place and Navy Pier, and Millennium Park. Moreover, Chicago has emergency access to many privately owned cameras aimed at the public way.⁵

Since then, many cameras have been added to Chicago's network. The Transit Authority added 1,700 cameras during the second half of 2011.⁶ The Police Department

¶5

¶6

¶7

¶8

¶9

⁵ ACLU camera report, supra note 2, at 9-10.

⁶ CTA Ahead of Schedule in Installing Security Cameras, CBS, Nov. 2, 2011; CHI. TRANS. AUTH., Security Camera Installation Project, http://www.transitchicago.com/safety/cameras.aspx.

added hundreds of new "police observation devices," or "PODs," which are the flashing blue light cameras perhaps best known by the general public. The Public Schools added scores of state-of-the-art cameras, and have plans to add hundreds more. The City obtained access to non-City cameras operated by the Board of Trade, the Federal Reserve, and the AT&T switching center.

In September 2011, a Chicago police executive stated that the City has access to 15,000 cameras. In February 2012, a Chicago 911 Center official stated that the City has access to 20,000 cameras.

How many cameras are enough? Chicago's prior Mayor, Richard M. Daley, stated that he wanted a "camera on every corner" of the City. ¹² As to Chicago's current Mayor:

When Mayor Emanuel was asked [at the November 2011 announcement of 1,700 new transit cameras] if there could be a point at which there might be too many cameras, he said, "I measure it not that way, not too many. I measure it, are we giving people the assurance that they need?" ¹³

B. Tight Integration

All of Chicago's various surveillance cameras, and many cameras of other public and private bodies, are tightly integrated into one system, known as "Operation Virtual Shield." This camera network is managed by the Chicago Office of Emergency Management and Communication ("OEMC"), which is sometimes called "the 911 Center." The OEMC has a command center where all the cameras can be monitored. Also, Chicago police officers can view and operate the cameras at their department's headquarters, at local precinct station houses, and on computers in certain squad cars. 16

¶11

⁷ *See* Clearmap: Crime Incidents, CHICAGO POLICE DEPT. http://gis.chicagopolice.org/website/clearMap/viewer.htm. On June 28, 2010, this site listed fewer than 1,300 PODs. On April 25, 2012, it listed more than 1,500 PODs.

⁸ Noreen Ahmed-Ullah, *Chicago Public Schools Officials Eyeing Updated Security Cameras for 14 High Schools*, CHI. TRIB., Jul. 24, 2011.

⁹ Fran Spielman, Chicago Expanding Big Brother Camera Network, CHI. SUN-TIMES, June 15, 2011.

¹⁰ Not All Residents Think Police Cameras are Deterring Criminals, CBS, Sept. 16, 2011 (Jonathan Lewin, Commander of the CPD Information Services Division, stating, in response a resident's complaint that a neighborhood camera was not effective at deterring crime: "With 15,000 cameras, this is one of many, and there are not 15,000 people watching them."), available at http://chicago.cbslocal.com/2011/09/16/not-all-residents-think-police-cameras-are-deterring-criminals/.

¹¹ Hilton Collins, *Video camera networks link real-time partners in crime solving*, GOVT. TECH., Feb, 1, 2012 (citing Ruben Madrigal, OEMC Deputy Director, for the proposition: "In all, police have access to 20,000 video feeds from public and private sources."), *available at* http://www.govtech.com/public-safety/Video-Camera-Networks-Link-Real-Time-Partners-in-Crime-Solving.html.

¹² Fran Spielman, *Chicago Mayor Wants Cameras on Every Corner*, CHI. SUN-TIMES, Mar. 14, 2009. *See also id.* (one of Mayor Daley's OEMC Directors, Ray Orozco, stating: "We're going to grow the system until we eventually cover one end of the city to the other."); *Daley: By 2016, Cameras on "Almost Every Block"*, CHI. SUN-TIMES, Oct. 12, 2006.

¹³ CTA Ahead of Schedule in Installing Security Cameras, CBS, Nov. 2, 2011.

¹⁴ ACLU camera report, supra note 2, at 10.

¹⁵ Id.

¹⁶ *Id*.

C. Powerful Technologies

Chicago's surveillance cameras have numerous technological powers that dramatically increase the ability of the government to watch the public.

First, Chicago's camera system can automatically track cars. That is, the system can automatically search for the image of a particular car, and then automatically track its movements, following the car out of the range of one camera and into the range of the next. This power, combined with the great density of cameras in downtown Chicago, is demonstrated by the police investigation of the 2009 gunshot death of the former school board president under a downtown bridge. The police watched his car, automatically jumping from one camera to the next, and thereby determined that he was alone, and thus that his death was a suicide. This system could be used to track any or all of our vehicular movements.¹⁷

Second, many of Chicago's cameras have the power to magnify—or to zoom in—to clearly see small objects from great distances. 18

Third, the City of Chicago has sought facial recognition technology for its camera system. Facial recognition uses computer software to reduce pictures of faces to a set of measurements, such as nose length, and then uses the measurements to find a match in a face-shot database. In May 2010, when the City announced its plan to install thousands of new transit cameras: "CTA officials said the cameras would be capable of facial recognition and would be linked real-time to . . . the city's 911 Center." Likewise, a "technology update" prepared by a Chicago police executive states that the City's "camera implementation plan" includes the need to "add analytics" for "facial recognition." In February 2011, when the City publicly responded to the ACLU's camera report, it stated that its cameras do not now have facial recognition, but the City has not stated whether it is still seeking facial recognition.

II. THE ABSENCE OF TRANSPARENCY

Under Chicago's prior Mayor, Richard Daley, there was very little transparency regarding the City's video surveillance camera system. For example, when the ACLU sent a Freedom of Information Act (FOIA) request to the City regarding its camera system, the City refused to state whether there had been any alleged misuse of the cameras, and did not disclose any electronic data regarding the cameras' alleged effectiveness. Likewise, there was no public information available regarding the total

¶14

¶15

¶16

¹⁷*Id*. at 11.

¹⁸ Id.

¹⁹ Lucas D. Introna & Helen Nissenbaum, Facial Recognition Technology: A Survey of Policy and Implementation Issues (2009), 11, 15-17, available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.
²⁰ All CTA Stations to Have Cameras by End of May, CBS 2 Chicago, May 21, 2010.

²¹ Jonathan Lewin (Commander of the CPD Information Services Division), *Technology Update*, Frame #87, http://www.scribd.com/doc/24309724/Chicago-CLEAR-Tech-Update-Pervasive-Surveillance. *See also id.* at Frames #122, #131 (further discussing the future role of facial recognition in Chicago's camera system).

²² Chicago OEMC, City of Chicago response to ACLU camera report, Feb. 8, 2011 (hereinafter Chicago camera response),

http://www.cityofchicago.org/city/en/depts/oem/provdrs/edu/news/2011/feb/city_of_chicago_responsetoacl ureportonsurveillancecameras.html.

number of cameras, the location of most cameras, the total amount of money spent on the cameras, and the sources of that money. Moreover, the City repeatedly failed to respond to the ACLU's requests for permission to visit the OEMC's operations center, and repeatedly failed to respond to the ACLU's letters proposing new regulations.²³

As a Mayoral candidate, Rahm Emanuel supported more transparency about Chicago's cameras. In February 2011, responding to a question about the ACLU camera report, he stated: "The city has an obligation for a level of trust between those who provide public safety to the public, which means more transparency and information about those cameras."²⁴

However, Mayor Emanuel proposed and obtained an ordinance giving him blanket power, during the first half of 2012, "to execute agreements with public and private entities for goods, work, or services regarding planning, security, logistics, and other aspects of hosting" the NATO summit in May 2012. Among other things, this ordinance allowed the Mayor to purchase and deploy new surveillance cameras without any approval from, or even notice to, the City Council. Previously, there had been some reporting by the Mayor to the City Council regarding camera purchases. The ACLU unsuccessfully advocated against this ordinance.

Another setback for camera transparency took place in the Illinois General Assembly in 2011. The ACLU advocated for a bill that would have required every government agency that operates or has access to outdoor or transit surveillance cameras to annually disclose their total number of cameras, and any camera privacy policies. Also, a state agency would have been required to publicly post this information on its website. The bill unanimously passed both legislative chambers. Unfortunately, the Governor issued an amendatory veto with recommendations for change; the bill's sponsor was barred from moving to concur in those changes, because a legislative committee determined that those changes altered the legislative scheme; the bill's sponsor instead moved to override the amendatory veto; but that override was opposed by executive agencies, and ultimately there was no override vote. Hopefully a similar bill will be enacted in the future.²⁸

¶19

¶20

²³ ACLU camera report, supra note 2, at 7, 12.

²⁴ Lisa Balde, *No more cameras: ACLU*, NBC 5 Chicago, Feb. 8, 2011, http://www.nbcchicago.com/news/local/No-More-Cameras-ACLU-115550559.html.

²⁵ Amendment of Chapters 2-84 and 10-36 of Municipal Code for associated authorization regarding upcoming NATO and G-8 summits, Ordinance #SO2011-9743, (Jan. 18, 2012) *available at* http://chicago.legistar.com/LegislationDetail.aspx?ID=1019529&GUID=B8CE27E0-919A-4849-BABE-C95FDEA9C2F4&Options=ID|Text|Attachments|&Search=nato.

²⁶ See, e.g., Chicago City Council Journal, *Proceedings of the Committee on Police and Fire*, July 19, 2007, at 4739-81 (reviewing \$4 million spent to install cameras at Navy Pier).

²⁷ ACLU of Illinois, *ACLU of Illinois continues opposition to amended ordinances on demonstration rules, urges City Council to expand oversight of surveillance cameras*, (Jan. 18, 2012) http://www.aclu-il.org/aclu-of-illinois-continues-opposition-to-amended-ordinances-on-demonstration-rules-urges-city-council-to-expand-oversight-of-surveillance-cameras/.

²⁸ HB1948, 97th General Assembly, (Ill. 2011) *available at* http://ilga.gov/legislation/BillStatus.asp?DocNum=1948&GAID=11&DocTypeID=HB&LegID=59149&Se ssionID=84&SpecSess=&Session=&GA=97.

III. CIVIL LIBERTIES PROBLEMS

Chicago's ubiquitous, integrated, and technologically powerful video surveillance camera system can invade our privacy, chill and deter freedom of speech and association, be misused by government employees, and squander scarce law enforcement resources.

A. Privacy

The personal habits of daily life are often carried out on our public streets and sidewalks. More primitive camera systems tracked only how some people spent some of their time in some public places. But Chicago's cutting-edge camera system empowers City government, if it chooses, to track how any or all people spend all of their time in all public places. Without proper regulation, each of us must wonder whether the government is watching and recording us when we walk into a book store, a political meeting, or a psychiatrist's office.

Chicago's surveillance cameras are just one of many tools now used by government to scrutinize what we are doing in public places. For example, the District of Columbia has built a network of hundreds of automatic license plate readers that captures the movements of millions of cars, and archives all of that location information for years, all in the absence of any criminal predicate. Likewise, hundreds of police departments nationwide learn our whereabouts by seizing cell phone records, often with no judicial oversight, showing the geographic position of our cell phones in relation to cell phone towers. Automated location tracking is just one part of a growing culture of government surveillance, which includes police fusion centers that mine vast databases of our sensitive personal information, and expanding police powers to seize our financial and communications records. Taken together, these government surveillance powers, if unregulated, would allow government to know what all of us are doing all the time, and with whom.

Fortunately, the U.S. Supreme Court earlier this year issued a groundbreaking decision regarding automated government tracking of our movements in public places. In *United States v. Jones*, the Court unanimously held that the police performed a search, triggering Fourth Amendment protections, when they placed a global position system ("GPS") device on a suspect's car, and used that device to monitor the car's movements for 28 days.³¹ The Court left many questions unanswered, including whether such a search requires a warrant, and whether other kinds of automated location tracking also

¶22

¶24

²⁹ Allison Klein, *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns*, WASH. POST. (Nov. 19, 2011), *available at* http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html. *See also* Jay Stanley, *License Plate Scanners Logging Our Every Move*, ACLU (Nov. 21, 2011), *available at* http://www.aclu.org/blog/technology-and-liberty/license-plate-scanners-logging-our-every-move.

³⁰ Eric Lichtblau, *Police are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (March 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?pagewanted=all. *See also, Cell phone location tracking public records request*, ACLU (April 6, 2012), *available at* https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request; Catherine Crump, *Justice Department Avoid Decision on Warrantless Cell Phone Tracking*, ACLU (Dec. 16, 2011), *available at* http://www.aclu.org/blog/technology-and-liberty/justice-department-avoids-decision-warrantless-cell-phone-tracking.

³¹ United States v. Jones, 132 S. Ct. 945 (2012).

comprise a search. On the whole, however, the *Jones* decision is an important step forward for privacy.

Justice Sotomayor's concurring opinion in *Jones* contains a forceful explanation of how unchecked government use of GPS devices threatens our privacy:

¶26

¶27

¶28

GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The Government can store such records and efficiently mine them for information years into the future. . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility. . . .

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may alter the relationship between citizen and government in a way that is inimical to democratic society. ³²

Justice Sotomayor's warning is equally true of automated location tracking by means of government surveillance camera systems like those in Chicago.

B. Freedom of Speech and Association

Chicago has a long history of unlawful political spying.³³ From the 1920s through the 1970s, the notorious police "Red Squad" infiltrated and maintained dossiers about thousands of law-abiding individuals and groups. The ACLU and other groups sued, and eventually settled with the City. That agreement regulated the City's collection of information about people based on their First Amendment activity, such as joining a civil rights group or marching in a parade. Unfortunately, these regulations were lightened in 2001, and lifted in 2009.

Today, Chicago does not meaningfully limit when its police officers may collect information about lawful speech and association. For example, the City allows police to video record activities protected by the First Amendment—even marching in a political demonstration—so long as a supervisor believes there is a "proper law enforcement

³² *Id.* at 955-56 (citations and internal quotations omitted). *Accord* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (Ginsberg, J.) ("A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts."); United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from the denial of rehearing en banc) ("[T]here's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention. . . . [T]hese two technologies alone [GPS and cell phone tracking] can provide law enforcement with a swift, efficient, silent, invisible and cheap way of tracking the movements of virtually anyone and everyone they choose.").

³³ See Alliance to End Repression v. City of Chicago, 237 F.3d 799, 801 (7th Cir. 2001).

purpose."³⁴ That standard is excessively nebulous and difficult to monitor. Moreover, the City requires video recordings of First Amendment activity to be retained for at least 60 days, and allows such recordings to be retained even longer.³⁵ Further, police supervisors may approve the audio recording of First Amendment activities³⁶ – though fortunately, the City's current system of fixed surveillance cameras apparently lacks the technological capacity to capture audio.

Given the vast, integrated, and powerful nature of Chicago's surveillance camera system, and the City's history of abusive political spying, many people will be afraid to join in First Amendment activity in public places, because they fear they will be watched, and their activity documented in government files.

C. Employee Misuse

In many other cities, government employees have misused surveillance cameras. Male camera operators have ogled female civilians. Other operators have wrongfully disclosed sensitive images. A statistical study in England found a racially disparate impact in whom camera operators were choosing for closer scrutiny. Unfortunately, the City of Chicago has declined to disclose whether any of its employees have been accused of abusing the camera system.³⁷

D. Opportunity Costs

The City of Chicago has declined to state the total cost of its camera network. However, publicly available information shows the expenditure of at least \$60 million. Meanwhile, funding cuts have forced a sharp reduction in the number of Chicago police officers on the streets. In a department with an authorized force of 13,500 officers, there are more than 1,000 vacancies, not including the 1,000 officers out on leave. Chicago also has reduced its spending on community policing. Yet beat officers and community trust often will be far more effective than cameras at deterring, investigating, and prosecuting crime. Thus, every new camera comes with an opportunity cost.³⁸

In response to the ACLU's camera report, the City stated that federal grants paid for cameras, and that those grants could not be used to pay for officers. No doubt, the federal government has spent tens of millions of dollars on Chicago's camera network. But the City has never asserted that *no* City funds have been used to purchase any cameras. Moreover, after purchase, the City must pay out-of-pocket for many camera-

¶29

¶30

³⁴ CPD Special Order S02-01-01 (eff. Oct. 26, 2011) at Part IV(B). *See also* CPD General Order S03-05 (eff. Feb. 22, 2012) at Part II(B)(1) (stating that officers may use the City's cameras when they have "a proper law enforcement purpose").

³⁵ CPD Special Order S02-01-01 at Part IV(B)(4).

³⁶ *Id.* at Part IV(B).

³⁷ ACLU camera report, supra note 2, at 16-17.

³⁸ ACLU camera report, supra note 2, at 17-18. See also Fran Spielman, Will City Hire New Officers Next Year?, CHI. SUN-TIMES (Oct. 6, 2011) ("A two-year hiring slowdown has left the Chicago Police Department more than 2,300 officers a day short of authorized strength, including vacancies and officers on medical leave and limited duty."), available at http://www.suntimes.com/news/metro/8069575-418/city-to-hire-new-police-officers-next-year-supt-mccarthy-says.html.

³⁹ Chicago camera response, supra note 22.

⁴⁰ ACLU camera report, supra note 2, at 9 & n.5.

related costs, including installation, maintenance, and monitoring. Public discussion of the costs and benefits of Chicago's camera system would be greatly advanced by the City's disclosure of the total amount of City funds spent to date on all aspects of the cameras – but this has not happened. Finally, the people of Chicago pay federal as well as city taxes, and they are entitled to rational use of federal funds. In 1994, President Clinton's anti-crime bill paid for 100,000 new local police officers. Today, the federal government should not be issuing grants that can pay for cameras but not officers.

IV. DO CAMERAS MAKE US SAFER?

Whether or not Chicago's surveillance camera system makes us safer, the City should adopt the critical privacy protections discussed below (*see infra* Part V) to solve the grave civil liberties problems discussed above (*see supra* Part III). These privacy protections would have no effect on the camera system's ability to fight crime. Even if they did, unregulated law enforcement techniques like the ones here extract too high a civil liberties price, even if they provide some measure of safety.

In any event, there is no compelling evidence that Chicago's surveillance camera system significantly contributes to deterring crime, or to arresting or prosecuting wrongdoers.

First, numerous studies by independent scholars have concluded that video surveillance cameras do not reduce violent crime, and only in limited circumstances reduce property crime (such as in parking garages). These include a University of Southern California study of cameras in Los Angeles in 2008, a University of California at Berkeley study of cameras in San Francisco in 2009, and dozens of other studies of cameras in the United States and England.⁴²

In September 2011, the Urban Institute published a study finding that Chicago's cameras reduced crime in the Humboldt Park neighborhood, but not in the West Garfield Park neighborhood. This study does not control for the substantial gentrification in Humboldt Park during the study period (2001 through 2006). Nor does this study control for other police initiatives; yet the Chicago police department mandates new police enforcement initiatives in the immediate vicinity of new cameras. Thus, it

¶33

¶34

¶35

⁴¹ U.S. Dept. of Justice, *Fact Sheet: Violent Crime Control and Law Enforcement Act of 1994*, https://www.ncjrs.gov/txtfiles/billfs.txt.

⁴² ACLU camera report, supra note 2, at 19.

⁴³ Nancy La Vigne, Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention, URBAN INSTITUTE (Sept. 2011) (hereinafter Urban Institute camera study), available at http://www.urban.org/UploadedPDF/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.pdf .

⁴⁴ See, e.g., Johnathon Briggs, *Housing boom's 2 sides detailed*, CHI. TRIB. (Jan. 2, 2006) (citing a study by the Loyola University Center for Urban Research, commissioned by the Chicago Commission on Human Relations, for the propositions that gentrification in Humboldt Park "often means tear-downs of houses," and that "low-income Hispanic residents fear displacement by white middle-class homeowners"), *available at* http://articles.chicagotribune.com/2006-01-02/news/0601020110_1_gentrification-humboldt-park-urban-research-and-learning.

⁴⁵ Specifically, the CPD's "POD placement request" form instructs: "list all other resources you are going to use to ensure that the 330 foot area covered by the POD will resolve the specific problem/crime." It then provides a checklist of such resources, including "directed missions," and community policing programs. Likewise, the CPD's "POD camera information" form requires a statement of "what additional city/police resources will be used to ensure crime reduction after POD camera removal." *See* "POD

remains unclear whether it was the cameras or other factors that reduced crime in Humboldt Park.

Second, Chicago's cameras have contributed to a very small fraction of all arrests. The City asserts that its camera network led to 4,500 arrests in the $4\frac{1}{2}$ years from 2006 through May 2010. But this is less than 1% of the 646,255 police arrests in just the three years from 2006 through 2008.

Third, Chicago's cameras have not been valuable to prosecutors in securing convictions:

Sally Daly, a spokeswoman for Cook County State's Attorney Anita Alvarez, said footage from the surveillance cameras is regularly reviewed in criminal investigations. "When it comes to blue light cams, they almost never capture the crimes that we review," Daly said. "No one I spoke to here can recall a case where we utilized these cameras to gain a conviction."

Likewise, according to the Urban Institute study: "Both investigators and prosecutors lamented the fact that video quality is often poor, rendering the identification of suspects and witnesses difficult and making a less than persuasive case in trials." ⁴⁸

V. THE ACLU'S PROPOSED CAMERA REGULATIONS

The City of Chicago should enter a moratorium on installation of new cameras, pending a thorough and open review of its entire camera system, including inquiry into whether to remove any cameras. The City also should adopt new safeguards for its camera system. These safeguards will address the civil liberties problems discussed above, without diminishing the camera's effectiveness. These safeguards have been adopted in other big American cities, and are contained in Model Legislation endorsed by former FBI Director William S. Sessions.⁴⁹ These safeguards also were endorsed in a *Chicago Sun-Times* editorial.⁵⁰

A. Automatic Tracking of Cars

Chicago's camera network can automatically track cars. The ACLU is not aware of any Chicago police or OEMC rules that specifically limit this power, and the City disclosed none in response to either the ACLU's FOIA request or the ACLU's camera report. Automatic vehicular tracking goes far beyond the powers of ordinary human

¶37

Placement Request," CPD form #21.965 (Oct. 2005); "POD Camera Information," CPD form #21.966 (Oct. 2005).

⁴⁶ ACLU camera report, supra note 2, 20 & n.105.

⁴⁷ Frank Main, *Blue-Light Cameras Get Mixed Reviews on Deterring Crime*, CHI. SUN-TIMES (Sept. 19, 2011), *available at* http://www.suntimes.com/news/crime/7696390-418/blue-light-cameras-get-mixed-reviews-on-deterring-crime.html.

⁴⁸ Urban Institute camera study, supra note 43, at p. 72.

⁴⁹ The Constitution Project, *Guidelines for Public Video Surveillance* (2007) at ix, 43-84 (endorsers list and Model Legislation),

http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf
⁵⁰ Editorial: Transparency must cover both sides, Chi. Sun-Times, Feb. 8, 2011, available at
http://www.suntimes.com/opinions/3703349-474/editorial-transparency-must-cover-both-sides.html.

observation, and is highly invasive of privacy. Pittsburgh requires probable cause for automatic tracking, and the Model Legislation recommends that approach.⁵¹ Notably, the U.S. Supreme Court in *Jones* recently held that certain GPS tracking of cars is a search that triggers Fourth Amendment protections. Automatic tracking of cars by Chicago's surveillance camera network is at least as invasive of privacy as the GPS tracking in *Jones*.

Accordingly, the City of Chicago should require probable cause either of criminal activity or of a threat to public safety, before using the camera system to automatically track a particular car.

B. Zooming and Aiming the Cameras

Most Chicago surveillance cameras give operators the power to aim the cameras at particular members of the public, and to zoom in to see small objects at great distances. This power goes far beyond ordinary human powers of observation. Moreover, it carries the inherent danger of abuse, as illustrated by the experience in other cities. Yet the current Chicago police department policy allows aiming and zooming at civilians, including those engaged in First Amendment activity, based on a mere "proper law enforcement purpose." This standard is too nebulous to guide officer discretion, or to provide a meaningful framework for later review. Accordingly, Pittsburgh requires reasonable suspicion for zooming, and the Model Legislation recommends that approach. Similarly, the District of Columbia and Salt Lake City require reasonable suspicion to zoom or aim at First Amendment activity. 52

Accordingly, the City of Chicago should require reasonable suspicion either of criminal activity or of a threat to public safety, before a camera operator (1) zooms in on any person or their possessions, or (2) aims at or zooms in on any activity protected by the First Amendment.

C. Storing and Disclosing Images

The City of Chicago's camera system has, or easily could be adjusted to have, the technological capacity to indefinitely retain for lengthy periods of time a virtually unlimited quantity of captured images of persons going about their business in public places. These images document sensitive information about us, including who we are with, and where we have been (such as a psychiatrist's office or a political demonstration). There is an inherent danger of accidental or wrongful disclosure of these sensitive images, as has occurred in other cities.

The current Chicago police department policy creates a presumption that camera images will be destroyed after 3 or 15 days (depending upon whether the camera was wireless), subject to retrieval requests by department personnel.⁵³ Unfortunately, this policy allows retention of camera images for lengthier periods in the absence of any criminal predicate. Moreover, while a separate Chicago police department policy forbids

¶41

¶43

¶44

⁵¹ ACLU camera report, supra note 2, at 22-23.

⁵² ACLU camera report, supra note 2, at 21-22.

⁵³ CPD Department Special Order S02-04-01 (eff. Feb. 23, 2012) at Part III.

"unauthorized . . . retention . . . or distribution" of camera images, 54 that policy does not limit when department personnel may authorize such retention and distribution. Further, the OEMC apparently has no current policy limiting retention or distribution.

New York City, Pittsburg, and San Francisco have adopted restraints on disclosing images. Likewise, the Model Legislation suggests a reasonable suspicion standard for retaining camera images, and restraints on disclosing images.⁵⁵

Accordingly, the City of Chicago should bar retention of camera images beyond a short period of time (such as 7 days), unless a supervisor determines that (a) there is reasonable suspicion that the images in question contain evidence of criminal activity, or (b) the images are relevant to an ongoing investigation or pending criminal trial.

Likewise, the City should bar dissemination of camera images to third parties, except that a supervisor can disseminate images:

- 1) To another governmental agency, if (a) there is reasonable suspicion that the images in question contain evidence of criminal activity, or (b) the images are relevant to an ongoing investigation or pending criminal trial.
- 2) To a criminal defendant, if the images in question are related to the pending charges.

D. Other Safeguards

First, the City of Chicago should conduct an annual audit of its camera system, to identify and evaluate: (1) the effectiveness of the cameras at reducing crime; (2) the impact of the cameras on privacy and other liberties; and (3) any misuse of the cameras, and the corrective action. The audits should be publicly disclosed, including all electronic statistical data used to evaluate camera effectiveness. Such audits would advance a healthy public dialogue regarding the cameras. New York and the District of Columbia require periodic audits of camera effectiveness and/or policy compliance, and provide public access to information in the audits. The Model Legislation recommends such audits.⁵⁶

Second, the City should provide public notice and an opportunity to be heard prior to the installation of new cameras. Residents should have an opportunity to comment regarding the future level of surveillance in their own neighborhoods. Such notice is required in Denver, San Francisco, and the District of Columbia, and recommended by the Model Legislation.⁵⁷

Third, the City should disclose the location of all cameras linked to its camera network. While the Chicago police discloses this information, many other City agencies do not. People should be able to protect their privacy by refraining from activities they do not want other people to watch while in the vicinity of a camera. Such disclosure is required in Denver, New York City, Pittsburgh, and San Francisco, and it is recommended by the Model Legislation.⁵

58

¶46

¶47

¶48

¶49

¶50

⁵⁴ CPD Department General Order G03-05 (eff. Feb. 22, 2012) at Part II(B)(1).

⁵⁵ ACLU camera report, supra note 2, at 23-24.

⁵⁶ *Id.* at 24-25.

⁵⁷ *Id.* at 25-26. ⁵⁸ *Id.*

Fourth, the City should adopt a rule providing that all private cameras linked into the City's network are subject to all the rules herein, and all other privacy safeguards. The City's contracts regarding access to private cameras do not contain such guarantees. Pittsburgh and the District of Columbia have adopted this rule, and the Model Legislation recommends it.⁵⁹

VI. CHICAGO'S TRAFFIC CAMERAS

Separate from the law enforcement and public safety surveillance cameras discussed throughout this report, the City of Chicago has installed an extensive system of traffic enforcement cameras to detect those who run red lights. The City plans in the near future to expand this system to document and punish driving too fast in the vicinity of schools and parks. There is ongoing debate regarding whether such traffic enforcement cameras decrease traffic accidents.

Properly regulated, typical traffic cameras raise fewer civil liberties concerns than typical law enforcement cameras. The former are automatic, and only capture traffic violations. The latter are manual (allowing human misuse), and can capture an infinite variety of images. Nonetheless, unregulated traffic cameras might invade our privacy. For example, such cameras systems might be programmed to record the license plates of all passing cars, and to retain this information for years, allowing for subsequent analysis of where particular people spend their time, or which people visit particular places. That's how the automatic license plate readers work in the District of Columbia, as discussed above.

¶55 In response to the ACLU's camera report, the City of Chicago disclosed the following privacy rules regarding its traffic cameras:

- 1) The cameras only take pictures of the rear of the vehicle, including its plate.
- 2) The pictures are only used to issue red light citations.
- 3) All intersections with red light cameras are clearly marked with signs, and listed on the City's website.
- 4) All images of non-violations are erased after 3 days, and all violation images are erased after two years. ⁶³

These traffic camera rules are a good start. The City should also prohibit its traffic cameras from taking pictures in the absence of a traffic violation. Moreover, the City

⁵⁹ *Id.* at 26-27.

⁶⁰ City of Chicago, Red-Light Camera Enforcement,

http://www.cityofchicago.org/city/en/depts/cdot/supp_info/red-light_cameraenforcement.html; OMEC, *Red Light Cameras*,

 $http://www.cityofchicago.org/dam/city/depts/oemc/general/PDF/redlight_camera_brochure 2.pdf.$

⁶¹ Kristen Mack, Emanuel speed camera ticket measure approved, CHI. TRIB. (Apr. 18, 2012).

⁶² See, e.g., Bob Secter, Mayor's speed camera stats sketchy, CHI. TRIB. (Mar. 14, 2012); Rajiv Shah, Effectiveness of Red Light Cameras in Chicago: An Exploratory Analysis (June 17, 2010), http://www.eyeingchicago.com/red-light-camera-study/.

⁶³ See Chicago camera response, supra note 22.

should require the destruction of such images upon completion of the enforcement of a traffic infraction. These protections are required by a State of Washington statute.⁶⁴

VII. CONCLUSION

In 1984, George Orwell imagined a dystopia where an all-powerful government used surveillance cameras and similar tools to scrutinize and dominate a submissive populace. We are not living in that world. But Chicago's current surveillance camera system—vast, integrated, and powerful—is a significant and troubling step towards a world where "Big Brother is watching you." The time is now to adopt the necessary privacy safeguards to help ensure that our national values thrive during the ongoing technological revolution.

⁶⁴ WASH. REV. CODE §§ 46.63.170(1)(d), (g), & (h).