July 24, 2013

Via Electronic Mail only

Oakland City Council
1 Frank Ogawa Plaza, Second Floor
Oakland, CA 94612

Re: Domain Awareness Center, Item 35, July 30, 2013 Agenda

Honorable Members of the Oakland City Council,

The American Civil Liberties Union of Northern California urges you to withhold approval of Item 35 on the City Council's July 30, 2013 agenda, regarding the Domain Awareness Center ("DAC"). Oakland should not approve a system that would allow for widespread warrantless surveillance of Oakland residents. The DAC as currently proposed allows for the collection and stockpiling of comprehensive information about Oakland residents who have engaged in no wrongdoing whatsoever, and lacks any binding privacy protections. Strong, enforceable safeguards are necessary to help to protect privacy rights and must strictly regulate the collection, use, retention, and dissemination of the data collected by the DAC. These safeguards must be in place *before* the City Council authorizes any further development of this surveillance center.

I. The DAC raises significant privacy concerns

The DAC is intended to "consolidate a network of existing surveillance and security sensor data to actively monitor critical City/Port facilities, utility infrastructure, roadways, and other areas."[1] At present, this network includes, among other things, over 700 cameras in Oakland schools, 40 automated license plate readers, 35 CCTV cameras at target locations in the city, an additional 40 cameras providing live video surveillance, 25 red light cameras, over 100 cameras of varying types at the Port, and feeds from external entities such as the California High Way Patrol and Caltrans, among other agencies.[2] The stated goal is "to allow integration of

[1] Request for Proposal for City of Oakland/Port of Oakland Joint Domain Awareness Center (October 2012), page 1 (hereinafter "RFP").
[2] "DAC Technical Requirements," included in City of Oakland and Port of Oakland, "Joint Domain Awareness center (DAC), Project Status Report, May 23, 2013, available at http://www.portofoakland.com/pdf/boar_shee_130523.pdf. A copy of this slide is attached as an Appendix to this letter.

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 DRUMM STREET, SAN FRANCISCO, CA 94111 | T/415.621.2493 | F/415.255.1478 | TTY/415.863.7832 | WWW.ACLUNC.ORG

additional systems in the future."[3] Thus, while the DAC could already collect, given existing networks, comprehensive information about Oakland residents wherever and whenever they go, the DAC has the potential to collect more types of information about more people in more locations in the future.

In addition, the DAC as currently proposed is clearly not intended simply to monitor Oakland residents in "real time." The proposal before you is to design the DAC so that it can "*store*, serve, display, and allow sharing of that data."[4]

The privacy implications are vast. Surveillance technology of the sort contemplated by the DAC enables law enforcement to capture intimate details of an individual's life, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, the synagogue or church, the gay bar and on and on." *United States v. Jones,* _U.S._, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver,* 12 N.Y.3d 433, 442 (N.Y. 2009)). New technology dramatically reduces the normal barriers of cost and officer resources to mount comprehensive surveillance. While an individual's trip along a public road to the doctor is visible to the public (and police), the expenditure of resources to surveil an individual around the clock wherever she goes serves as a deterrent to abuse. When, by contrast, one technician can sit at the police station and monitor hundreds or even thousands of targets continuously and for indefinite periods, strong safeguards are essential to protect privacy and ensure that invasive surveillance is only conducted of those as to whom there is probable cause of criminal activity. For this reason, five Supreme Court justices in the *Jones* case recently held that long-term tracking of the location of an individual using a GPS device constitutes a "search" within the meaning of the Fourth Amendment.

The collection and potential stockpiling of comprehensive information also raises significant concerns under the California Constitution, which provides even more robust privacy protections than the federal constitution. The voters of California enacted the Privacy Initiative precisely to prevent the indefinite stockpiling of personal information. *See Hill v. N.C.A.A.*, 7 Cal. 4th 1, 17 (1994) (California privacy initiative "prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us") (citation omitted). In *White v. Davis,* 13 Cal.3d 757 (1975), the California Supreme Court addressed a challenge to a program of surveilling classes at UCLA by the Los Angeles Police Department, including undercover police attendance in public classes. Thus, *White* recognizes that privacy implications arise, even when the conduct at issue occurs "in public." And the California Attorney General has interpreted the state constitutional right to privacy to prohibit the collection and storage of so-called "intelligence" information "absent an articulable criminal predicate for the gathering of

[3] RFP at page 6 (emphasis added).
[4] RFP at page 6 (emphasis added).

[the] information." "Criminal Intelligence Systems: A California Perspective," California Department of Justice, Division of Law Enforcement at 16-17 (September 2003).[5]

There are serious questions whether a system such as the DAC – which is intended to collect and store vast amounts of information about Oakland residents who have engaged in no wrongdoing – should ever be approved. But what is even more troubling is that the City has not yet developed *any* guidelines on privacy and data retention. Although the City's contract for the DAC takes pains to prescribe in minute detail the precise manner in which, for example, metal framing systems are to be installed (studs are to be placed not more than 2 inches from abutting walls),[6] there are no privacy provisions in place at all. Oakland's information technology manager Ahsan Baig was reported as saying these policies would be developed during the next year.[7] But just as the City Council would not approve the DAC without knowing its financial price tag, the DAC should not approve the DAC without knowing its privacy costs. The City Council should withhold approval for any further development of this system until privacy concerns are fully vetted.

II. Privacy safeguards need to be developed before any further approval of the DAC

It is essential to develop strong privacy safeguards at the outset. The DAC cannot be meaningfully evaluated without information about how the data would be collected, used, retained, and disseminated. Creating a strong privacy framework up front, *before* approval of the DAC, ensures that elected leaders and the community understand and actually endorse the contemplated uses of the new technology and its privacy implications. Strong privacy safeguards, especially provisions delineating the specific purposes for which the DAC is to be used, helps prevent "mission creep," a common feature of data collection schemes. For example, in a recent incident, police in Germany said that drones would be used to monitor traffic and for serious kidnapping situations, but it was later revealed that drones were secretly used to monitor an anti-nuclear protest.[8]

Wide recognition of the need to protect privacy of information led to the development of "Fair Information Practices" or "Fair Information Practice Principles" (FIPPs). Internationally, the FIPPs are codified in the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, which "have had a significant impact on the development of national laws in North America, Europe, and East Asia." In the United States, federal agencies are mandated

---

[5] The Attorney General's Report is available at http://www.aclunc.org/library/documents/criminal_intelligence_systems_a_california_perspective.shtml

[6] *See* City of Oakland Domain Awareness Center, Project #A12.022, October 12, 2012 – Bridging Documents, 05 40 00 – 2, Part 3-1-C.

[7] *See* Ali Winston, "Oakland surveillance center progresses amid debate on privacy, data collection," Center for Investigative Reporting, July 18, 2013, available at http://cironline.org/reports/oakland-surveillance-center-progresses-amid-debate-privacy-data-collection-4978.

[8] Christian Watien, *5 Uses for Drones that Don't Involve Fighting Terrorists*, EPOCH TIMES (Nov. 10, 2012), www.theepochtimes.com/n2/world/5-uses-for-drones-that-don-t-involve-fighting-terrorists-313051-print.html

under The Privacy Act of 1974 to follow Fair Information Practices. The FIPPs are "at the core of the Privacy Act of 1974 and [are] mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations." Similar principles are also reflected in California's Information Practices Act. *See* Cal. Civ. Code §1798 *et seq*. The most complete and practical formulation of the FIPPs – first adopted by the Department of Homeland Security, and now by other agencies such as the California Public Utilities Commission and the Office of Science and Technology Policy – organizes them into a set of eight key principles to regulate databases containing personal information, such as those that would be created by the DAC. Any privacy policy should address at a minimum each of the following:

1. Transparency – Data holders should be transparent and provide notice regarding the collection, use, dissemination, and maintenance of data.

2. Individual participation – Data holders should provide mechanisms for individuals to access and correct personal data and seek individual consent for its collection, use, dissemination, and maintenance.

3. Purpose specification – Data holders should specifically articulate and provide notice of the purpose for which the data will be used.

4. Data minimization and retention – Data holders should only collect data that is necessary to accomplish the specified purpose and only retain data for as long as is necessary to fulfill the specified purpose.

5. Use limitation – Data holders should use data solely for the purpose specified in the notice.

6. Data quality and integrity – Data holders should ensure that data is accurate, relevant, timely, and complete.

7. Security – Data holders should protect data through security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. Accountability and auditing – Data holders should implement accountability mechanisms for complying with these principles, including providing training to all employees and contractors who use the data, and auditing the actual use of the data.

* * *

For the reasons discussed above, there are serious questions about whether the long-term comprehensive surveillance enabled by the DAC can ever be conducted consistent with state and federal constitutional privacy protections, and whether certain uses of the DAC would trigger the need to obtain a warrant under the Fourth Amendment. But at a minimum, the City should fully

examine the privacy impact of such a system and adopt an enforceable privacy framework that addresses each of the elements discussed above.

We urge the City Council not to write a blank check. The City Council should withhold any further approval of the DAC until such time as the City has fully addressed privacy concerns and developed meaningful, enforceable privacy safeguards.

Respectfully submitted,

Linda Lye
Staff Attorney
American Civil Liberties Union
of Northern California

Encl.

DAC Technical Requirements

OAKLAND CITY

CCTV CAMERAS AT TARGET LOCATIONS

~35 CAMERAS

ITS NETWORK LIVE VIDEO SURVEILLANCE

~40 CAMERAS

POLICE SHOT SPOTTER SYSTEM

>100 SENSOR SITES

POLICE & FIRE CAD & RECORDS MGT SYSTEMS

MOTOROLA COMPATIBLE

40 VEHICLES
OPD AUTOMATIC LICENSE PLATE READER MONITORING

OAKLAND CITY POLICE AVL **(ALL)**

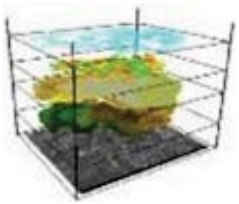
OAKLAND CITY FIRE TRUCK AVL **(ALL)**

25 SITES
OAKLAND CITY PHOTO ENFORCEMENT

700 + CAMERAS
OAKLAND CITY SCHOOLS CCTV

OAKLAND CITY PUBLIC SAFETY INTRANETS

GIS MAP LAYERS



EOC DAC

OAKLAND PORT

INTEGRATED SECURITY CCTV SYSTEM

77 PERIMETER DETECTION CAMS

34 THERMAL INTRUSION DETECTION CAMS

21 PAN-TILT-ZOOM CAMS

PORT VIEW

GEO SPATIAL SECURITY MAPPING SYSTEM (GSMS-GIS)

TRUCK MANAGEMENT SYSTEM (TMS)

Registry of
6000 trucks
300 LMCs
6000 Drivers

OTHER EXTERNAL

USGC VESSEL TRAFFIC SERVICE

~ 40 HWY CAMERAS

~ 50 HWY CAMERAS

~ 20 HWY CAMERAS

84 READERS
BAY AREA TRAFFIC MONITORING

USGS

US GEOLOGICAL SURVEY SEISMIC MONITORING

NOAA

NATIONAL WEATHER SERVICE

NO. CALIFORNIA REGIONAL INTELLIGENCE CENTER

CBRNE

CHEMICAL, BIOLOGICAL, NUCLEAR, RADIOLOGICAL & EXPLOSIVE MONITORING

ARIES

AUTOMATED REGIONAL INFORMATION EXCHANGE SYSTEM