#### OFFICE OF INDEPENDENT POLICE MONITOR

# CITY OF NEW ORLEANS



## SUSAN HUTSON INDEPENDENT POLICE MONITOR

November 28, 2017

VIA EMAIL

Councilmember-at-Large Stacy Head City Hall, Room 2W40 1300 Perdido Street New Orleans, LA 70112

Councilmember-at-Large Jason Rogers Williams City Hall, Room 2W50 1300 Perdido Street New Orleans, LA 70112

Councilmember Susan Guidry City Hall, Room 2W80 1300 Perdido Street New Orleans, LA 70112

Councilmember/Mayor Elect LaToya Cantrell City Hall, Room 2W10 1300 Perdido Street New Orleans, LA 70112

Nadine M. Ramsey City Hall, Room 2W70 1300 Perdido Street New Orleans, LA 70112

Councilmember Jared C. Brossett City Hall, Room 2W20 1300 Perdido Street New Orleans, Louisiana 70112

Councilmember James Austin Gray II City Hall, Room 2W60 1300 Perdido Street New Orleans, LA 70112

RE: Letter Regarding Citywide Public Safety Improvements Plan Proposed by Mayor Landrieu on Jan. 23, 2017

This letter addresses the <u>Citywide Public Safety Improvements</u> (PSI) Plan<sup>1</sup> authored by Mayor Landrieu on January 23, 2017. As part of its responsibility to respond to community concerns about public safety, to "review the adequacy of data collection and analysis" and conduct risk

 $<sup>^{1}</sup>$  New Orleans City Wide Public Safety Improvements. The City Of New Orleans, 23 Jan. 2017, www.nola.gov/city/new-orleans-public-safety-final\_012317



management reviews" <sup>2</sup>, OIPM began engaging the PSI when a community group<sup>3</sup> made the OIPM staff aware of its concerns. Through the process of researching the implementation of similar technologies and plans in other cities, the OIPM has catalogued a few issues that the council may want to consider as this PSI moves forward.

There are a few potential risks to public safety and individual privacy raised by this community group. In addition, OIPM's research shows that there may be some high-level risks in the form of civil liability, unintended public safety outcomes, and fiscal waste. In this letter, OIPM suggests some procedural and policy steps that may mitigate these risks.

### Surveillance and Data Collection Technology Oversight

As with any law enforcement data system housing private information about citizens, there is a potential for mismanagement, poor information security, public records law compliance challenges and user abuse. Although the Mayor's proposed Plan would significantly expand NOPD's surveillance and data collection capabilities, it does not earmark resources or personnel to monitor the implementation of the Plan. OIPM recommends the council consider how these surveillance and data collection systems will be monitored. A failure to build in monitoring and oversight may expose The City of New Orleans to a civil liability risk. In the event that evidence in these systems is used for prosecution, these systems could also present a risk unconstitutional criminal justice practices as well. As recently as 2016, the Department of Justice warned that departments should not expand their electronic surveillance capabilities until they have addressed core problems of corruption, poor oversight, and inadequate training.<sup>4</sup>

### **Potential for Abuse**

The potential for abuse is an important reason for OIPM oversight and monitoring. Unregulated systems have the potential to jeopardize the expensive and hard-won police reforms of the past ten years. The list of potential abuse falls into three categories: (a) Improper focus on a person's body; (b) Disparate racial impact; and (c) Retention and improper release of images. a) Improper focus on a person's body

A review of 592 hours of government-run CCTV monitoring system footage in London found that 10% of surveillance of women lasted more than one minute, and 15% of surveillance of women for shorter periods was voyeuristic. In 2007, a police supervisor in Worcester, England was suspended after improperly manipulating surveillance cameras to focus in on women's breasts and buttocks.<sup>5</sup>

Rampant misuse has already presented itself within similar systems in the U.S.A. In a 2017 public records request revealed that in California, rates of misuse of surveillance technologies by

<sup>&</sup>lt;sup>5</sup> Andrew Parker, Surveillance of CCTV Operator, THE SUN, Feb. 14, 2007 via ACLU report



<sup>&</sup>lt;sup>2</sup> Municipal Code of Ordinances, Part II, Chapter 2, Article XIII - Office of Inspector General, Sec. 2-1121 - Office of Independent Police

<sup>&</sup>lt;sup>3</sup> Official MaCCNO Statement: Proposed Citywide Safety Plan Invites Profiling, Damages Culture

<sup>&</sup>lt;sup>4</sup>Bouche, Kenneth, et al. "USDOJ Report on Calexico." *Electronic Frontier Foundation*, 28 Apr. 2017, www.eff.org/document/usdoj-report-calexico

police officials are increasing annually, having gone up by 50% overall from 2011 to 2017.  $^6$ Just this month, an officer in New York was caught using law enforcement databases and surveillance system to harass and stalk his ex-partner, directing others in the department to gather surveillance of the victim and her family. Finally, in 2015 a police sergeant in Ohio pleaded guilty to felony charges of aggravated assault, tampering with evidence, menacing by stalking and other crimes, illegally using a police department computer to target and threaten women.8

Not only is this type of police misconduct, a risk to the Police Department and Public Safety. these types of activities could be precursors to more serious misconduct among officers and also promulgate a culture of sexual misconduct. A year-long investigative report from the Associated Press revealed that in a six-year period, 1,000 officers lost their licenses for perpetrating sexual assault. The statistic, a low estimate due to vastly underreported instances of sexual assault, indicates a nation-wide problem with sexual misconduct among police officers. Louisiana, a state that rarely decertifies officers, seems unlikely to self-report any misconduct. <sup>10</sup> An unregulated surveillance system may exacerbate this issue that already has limited oversight.

## *b)* Disparate racial impact <sup>11</sup>

In the aforementioned study in England, of 592 hours of camera monitoring, the researchers found that black people were between 1.5 and 2.5 times more likely to be watched than one would expect from their presence in the population being monitored. Further, black people were disproportionately placed under such surveillance for "no obvious reason" – 68% of all surveillance of blacks, compared to 35% of all surveillance of whites. 12

According to a 2017 study from the House Committee on Oversight and Government Reform<sup>13</sup>, other technologies implied by the plan but not explicitly mentioned, such as facial recognition cameras, have been shown to disproportionately misidentify black people as suspects. Given the demographics of the twenty neighborhoods selected for special monitoring as part of this plan,

<sup>&</sup>lt;sup>13</sup> Committee To Review Law Enforcement's Policies on Facial Recognition Technology, House of Representatives, 115th Cong. (2017) https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/



<sup>&</sup>lt;sup>6</sup> David Mass, California Authorities Are Failing to Track and Prevent Abuse of Police Databases, Electronic Frontier Foundation, May 14, 2017, https://www.eff.org/deeplinks/2017/05/california-authorities-still-ignoringrising-abuse-police-databases

<sup>&</sup>lt;sup>7</sup> Kaley Lynch, "Former Irondequoit police officer pleads guilty to cyberstalking ex-girlfriend." News 4 Digital Producer, 5 October 2017,

http://wivb.com/2017/10/05/former-irondequoit-police-officer-pleads-guilty-to-cyberstalking-ex-girlfriend/ <sup>8</sup> Ed Meyer, "Former Akron police sergeant pleads guilty to stalking former girlfriend." 10 September 2015,

https://www.ohio.com/akron/news/former-akron-police-sergeant-pleads-guilty-to-stalking-former-girlfriend <sup>9</sup> Sedensky, Matt, and Nomaan Merchant. "Betrayed by the Badge." Associated Press, 1 Nov. 2015,

interactives.ap.org/2015/betrayed-by-the-badge/?SITEID=apmobile

<sup>&</sup>lt;sup>10</sup>Stole, Bryn, and Rebekah Allen. "Louisiana Less Likely to Strip Law Enforcement Officers of Credentials than Any Other State; Lawmakers Aim to Change That." The Advocate, 3 June 2017,

www.theadvocate.com/baton\_rouge/news/crime\_police/article\_e3f12332-464b-11e7-a4f4-f369e513d850.html

<sup>&</sup>lt;sup>11</sup> City of N.Y. v. Hassan, 2015 NY Slip Op 03781, 128 A.D.3d 419, 8 N.Y.S.3d 211 (App. Div.)

<sup>&</sup>lt;sup>12</sup> Clive Norris & Gary Armstrong, CCTV and the Social Structuring of Surveillance (1999),163, http:// www.popcenter.org/library/CrimePrevention/Volume 10/06-NorrisArmstrong.pdf

there is a risk of further criminalization of people of color in New Orleans. Oakland rejected predictive policing in 2014 for these same reasons. <sup>14</sup>

c) Retention and improper release of images 15

The collection of images and data of New Orleans residents and visitors may expose both the City and individuals to risks. Proposed programs such as the "threat analytics platform" to be housed in the Centralized Command Center serve the same function as predictive policing technologies which compute crime reports and other statistics to generate potential suspects or predict crime "hot spots". <sup>16</sup> Clear plans may need to be created to determine how police departments can best make use of such information.

Additionally, the retention of images and data may increase the likelihood of misuse and improper release whether from hackers, surveillance personnel, or police officers anxious to gather evidence. Retaining images increases the likelihood of violating our 4th Amendment rights to privacy through the practice of "tracking" citizen's movement and identity. <sup>17</sup> Additionally, Louisiana's fairly permissive public records law may present a challenge to the City, if and when members of the public and the press wish to obtain such data.

### **Insecure Systems Will Expose the City to Liability**

In 2015, the Electronic Frontier Foundation (EFF) conducted a nationwide investigation of automatic license plate readers (ALPRs) and found that more than a hundred ALPR cameras were exposed online, often with totally open web pages accessible by anyone with a browser. <sup>18</sup> In five cases, EFF was able to track the cameras to their sources: St. Tammany Parish Sheriff's Office, Jefferson Parish Sheriff's Office, and the Kenner Police in Louisiana; Hialeah Police Department in Florida; and the University of Southern California's public safety department <sup>19</sup>. This particular risk exposure further supports the argument that all the new surveillance and data collection systems should be monitored and have strong security features.

#### **Fiscal Waste**

<sup>&</sup>lt;sup>18</sup>Quintin, Cooper, and Dave Maass. "License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech." *Electronic Frontier Foundation*, 3 Nov. 2015, www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive. <sup>19</sup> *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212 (N.D. Cal. Aug. 30, 2017).



<sup>&</sup>lt;sup>14</sup> Thomas, Emily. "Why Oakland Police Turned Down Predictive Policing." *Motherboard*, 28 Dec. 2016, motherboard.vice.com/en\_us/article/minority-retort-why-oakland-police-turned-down-predictive-policing <sup>15</sup> *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212 (N.D. Cal. Aug. 30, 2017).

<sup>&</sup>lt;sup>16</sup> Robinson, David, and Logan Koepke. "Stuck In A Pattern: Early Evidence on Predictive Policing and Civil Rights." *Upturn*, Aug. 2016, www.teamupturn.com/reports/2016/stuck-in-a-pattern

<sup>&</sup>lt;sup>17</sup> Guidelines for Public Video Surveillance." *The Constitution Project*, 2007, p. 27., DOJ: www.constitutionproject.org

The City of Chicago spent over \$60 million of taxpayer's dollars on 10,000 surveillance cameras, the presence of which have not conclusively proven to deter or reduce crime. <sup>20</sup> Even the city of Chicago's claim that its surveillance cameras aided in 4,500 arrests over a period of 4 years is unremarkable, given that these 4,500 arrests accounted for less than 1% of arrests during that period. <sup>21</sup> In our own city, taxpayers have financed a failed and unregulated crime camera system. A bribery scheme between Mark St. Pierre's technology companies (*Imagine Software*, and *Ciber Inc.*) and former Nagin administration Chief Technology Officer Greg Meffert cost the city millions in taxpayer-funded contracts <sup>22</sup> for an ineffective and malfunctioning crime camera network. <sup>23</sup> Over a period of seven years, the crime camera network yielded only six indictments. <sup>24</sup> Without an adequate oversight system, taxpayers could bear the financial brunt of another private sector corruption scandal.

In addition to the risk exposures listed above, there are several community concerns worthy of attention:

# Abusing the right to privacy $^{25}$ :

The Musician's Coalition and its partners have expressed a concern that the addition of surveillance cameras will impact New Orleans' time-honored cultural traditions and use of public space. In a community where our culture is such a large part of our economy, we encourage the council to consider the impact of public surveillance and the value of preserving the individual freedom to be anonymous in public space.

## **Financial Sustainability**

The proposed plan totals \$40 million, but the strategy for long term funding of the system's maintenance is unclear and is currently estimated to cost at least \$3.8 million a year. <sup>26</sup> When similar programs have been implemented in other parts of the country. Police departments have begun relying on money from civil asset forfeiture and other sources lacking sufficient oversight and transparency. <sup>27</sup>

# **Cameras May Not Deter Crime**

<sup>&</sup>lt;sup>27</sup> Martinez, Freddy, et al. "Opening the Chicago Surveillance Fund." *MuckRock*, www.muckrock.com/project/opening-the-chicago-surveillance-fund-25/.



<sup>&</sup>lt;sup>20</sup> Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy. ACLU of Illinois, Feb. 2011, www.aclu-il.org/wp-content/uploads/2012/06/Surveillance-Camera-Report1.pdf+

<sup>&</sup>lt;sup>21</sup> Ibid

Hammer, David. "Greg Meffert, Wife, City Hall Vendor Charged with More than 60 Counts in Bribery Scheme." *NOLA.com*, Times Picayune, 9 May 2011, www.nola.com/crime/index.ssf/2009/11/meffert.html.

<sup>&</sup>lt;sup>23</sup> Times-Picayune, David Hammer The. "Mayor Mitch Landrieu Wants to Dump City's Crime Cameras." *NOLA.com*, The Times Picayune, 14 Oct. 2010,

 $www.nola.com/politics/index.ssf/2010/10/new\_orleans\_crime\_camera\_progr.html~^{24}~Ibid.$ 

<sup>&</sup>lt;sup>25</sup> State v. Jones, 2017 S.D. 59.

<sup>&</sup>lt;sup>26</sup> Rainey, Richard. "Worry over New Orleans Security Plan's Future Trumped by Questions about Its Startup Costs." *NOLA.com*, Times Picayune, 7 Mar. 2017,

www.nola.com/politics/index.ssf/2017/03/worry\_over\_new\_orleans\_securit.html.

A 2008 study by the University of Southern California ("USC") found that Los Angeles' camera network made no statistically-significant impact on reducing violent crime, property crime, or quality of life crime, such as prostitution or public drunkenness. <sup>28</sup> Similarly, a 2009 study by the University of California at Berkeley found that San Francisco's cameras made no statistically significant impact on reducing violent crime, drug crime, or quality of life crime, while only making some impact on reducing property crime. <sup>29</sup> A 2005 review of 13 studies in England found no statistically-significant impact on reducing violent crime, and a statistically-significant reduction in property crime in only two of the thirteen locations studied, one of which was a parking lot. <sup>30</sup> A 2008 review by USC of 44 studies in the United States and abroad concluded that none of the domestic studies found a statistically-significant impact on reducing crime, and that any impact found in foreign studies was limited to property crime. <sup>31</sup>

Reports with a more favorable view of surveillance cameras, like one from the Urban Institute, could not conclusively prove that the presence of surveillance cameras always deters crime. In its study, Humboldt Park, a Chicago neighborhood experienced a decrease in crime after the installation of surveillance cameras while another neighborhood, West Garfield Park, experienced no measurable changes. Further weakening this study, a report from the ACLU alleged that the Urban Institute used flawed methodology to calculate its results. Although crime may decrease in the area in front of a security camera, criminal activity may simply be displaced to another area of the city.

Finally, there is no evidence to support that the threat analytics platform, the proposed predictive policing technology, will yield a measurable decrease in crime. A report published by the RAND corporation found that predictive policing does not reduce crime. <sup>33</sup> In another report from Upturn, the authors found that law enforcement often trusts predictive technology as fact rather than a suggestion or an aid in an investigation. <sup>34</sup> Without accurate data inputs the resulting prediction may be erroneous. <sup>35</sup>

<sup>&</sup>lt;sup>34</sup> Robinson, David, and Logan Koepke. "Stuck In A Pattern: Early Evidence on Predictive Policing and Civil Rights." *Upturn*, Aug. 2016, www.teamupturn.com/reports/2016/stuck-in-a-pattern <sup>35</sup> Rand Corporation. 2013



<sup>&</sup>lt;sup>28</sup> Aundreia Cameron et al., Measuring the Effects of Video Surveillance on Crime in Los Angeles, at 29-30 (University of Southern California, May 5, 2008)

<sup>&</sup>lt;sup>29</sup> Jennifer King, et al., An Evaluation of the Effectiveness of San Francisco's Community Safety Cameras, at 11-12 (University of California, Berkeley, Dec. 17, 2008) [hereinafter "Berkeley Report"]

<sup>&</sup>lt;sup>30</sup> Martin Gill & Angela Spriggs, Assessing the impact of CCTV, at 23-25 (Home Office Research, Development and Statistics Directorate, Feb. 2005) [hereinafter "English Camera Study of 2005"].

<sup>&</sup>lt;sup>31</sup> USC Study, supra note 93, at 14-16.

<sup>&</sup>lt;sup>32</sup>La Vigne, Nancy G, et al. "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention." *The Urban Institute*, Sept. 2011, www.urban.org/sites/default/files/publication/27546/412401-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention-A-Summary.PDF.

<sup>&</sup>lt;sup>33</sup> Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, 2013, <a href="http://www.rand.org/pubs/research">http://www.rand.org/pubs/research</a> reports/RR531.html

OIPM recommends that The City engage the community in a discussion and/or education process about why surveillance may make our community safer and what the unintended consequences of surveillance may be.

## **Process and Community Engagement**

The published version of the City's plan leaves room for interpretation. Several community groups have reached out to OIPM to express their concerns and to seek clarity about details of the plan, particularly around privacy and public input. OIPM is aware of a community-led petition calling for a halt to implementation of all aspects of the plan until public meetings are held that are accessible to residents throughout the City. <sup>36</sup>

#### II. POLICY RECOMMENDATIONS

With these concerns in mind, OIPM researched and recommends the following best practices and policies to accompany the installation of any new security cameras and surveillance equipment included in the Mayor's <u>Citywide Public Safety Improvement Plan</u>. We advise the implementation of rules and regulation to ensure strong oversight and to limit the potential for abuse.

- Prohibit magnification of an individual's face without reasonable suspicion or threat to public safety and monitor compliance.
- Prohibit aiming the camera at an individual's or group's activity without reasonable suspicion or threat to public safety and monitor compliance.
- Require camera operators to adhere to the same 4<sup>th</sup> Amendment-informed NOPD policies regarding reasonable suspicion and monitor compliance.
- Prohibit pointing cameras into private homes and monitor compliance.
- Balance the need for public information against public privacy when setting rules on dissemination and duration of image retention and monitor compliance.
- Monitor NOPD to ensure consistent enforcement of camera policies and discipline those who violate policy.
- Private cameras linked to the command center feeds must follow the same rules and regulations as public cameras.

In addition, the OIPM recommends that the council consider the following processes:

- A series of community engagement meetings about the City's plans, how they will be financed and implemented, and the community's concerns about this plan.
- OIPM recommends the council consider how these surveillance and data collection systems will be monitored. As recently as 2016, the Department of Justice warned that

<sup>&</sup>lt;sup>36</sup>Join the Opposition to New Orleans \$40 Million 'Security Plan'." *MaCCNO*, The Music and Culture Coalition of New Orleans, 2017, www.maccno.com/join-the-opposition-to-new-orleans-40-million-security-plan/



departments should not expand their electronic surveillance capabilities until they have addressed core problems of corruption, poor oversight, and inadequate training.<sup>37</sup>

The OIPM can be a resource to the council on this and other public safety issues. Should you have any questions or concerns about this letter or wish to discuss it further, the OIPM staff are at your disposal.

Sincerely,

Ursula Price

**Acting Police Monitor** 

504-304-5825

<sup>&</sup>lt;sup>37</sup>Bouche, Kenneth, et al. "USDOJ Report on Calexico." *Electronic Frontier Foundation*, 28 Apr. 2017, www.eff.org/document/usdoj-report-calexico

