

REPORTERS COMMITTEE

FOR FREEDOM OF THE PRESS

1156 15th St. NW, Suite 1020
Washington, D.C. 20005
(202) 795-9300
www.rcfp.org

Bruce D. Brown
Executive Director
bbrown@rcfp.org
(202) 795-9301

STEERING COMMITTEE CHAIRMAN

STEPHEN J. ADLER, *Reuters*

STEERING COMMITTEE MEMBERS

J. SCOTT APPLEWHITE
The Associated Press

WOLF BLITZER
CNN

DAVID BOARDMAN
Temple University

THEODORE J. BOUTROUS, JR.
Gibson, Dunn & Crutcher LLP

MASSIMO CALABRESI
Time Magazine

MANNY GARCIA
Austin American-Statesman

EMILIO GARCIA-RUIZ
San Francisco Chronicle

JOSH GERSTEIN
POLITICO

ALEX GIBNEY
Jigsaw Productions

SUSAN GOLDBERG
National Geographic

JAMES GRIMALDI
The Wall Street Journal

LAURA HANDMAN
Davis Wright Tremaine

DIEGO IBARGÜEN
Hearst

KAREN KAISER
The Associated Press

DAVID LAUTER
The Los Angeles Times

MARGARET LOW
WBUR

JANE MAYER
The New Yorker

COLLEEN MCCAIN NELSON
The McClatchy Company

MAGGIE MULVIHILL
Boston University

JAMES NEFF
The Philadelphia Inquirer

NORMAN PEARLSTINE
New York, New York

THOMAS C. RUBIN
Stanford Law School

CHARLIE SAVAGE
The New York Times

JENNIFER SONDAG
Bloomberg News

NABIHA SYED
The Markup

ADAM SYMSON
The E.W. Scripps Company

PIERRE THOMAS
ABC News

SAUNDRA TORRY
Freelance

VICKIE WALTON-JAMES
NPR

JUDY WOODRUFF
PBS/The NewsHour

HONORARY LEADERSHIP COUNCIL

CHIP BOK
Creators Syndicate

DAHLIA LITHWICK
Slate

TONY MAURO
American Lawyer Media, ret

ANDREA MITCHELL
NBC News

CAROL ROSENBERG
The New York Times

PAUL STEIGER
ProPublica

*Affiliations appear only
for purposes of identification.*

By web portal

February 25, 2021

Commissioner Dermot F. Shea
City of New York Police Department
1 Police Plaza
New York, NY 10038

Deputy Commissioner John J. Miller
Office of the Deputy Commissioner, Public Information
City of New York Police Department
1 Police Plaza
New York, NY 10038

Re: Comment on proposed impact and use policies for
surveillance technologies

Dear Commissioner Shea and Deputy Commissioner Miller:

The Reporters Committee for Freedom of the Press respectfully submits these comments in response to the January 11, 2021, proposed impact and use policies for certain surveillance technologies utilized by the New York Police Department.

The Reporters Committee was founded by leading journalists and media lawyers in 1970 when the nation's news media faced an unprecedented wave of government subpoenas forcing reporters to name confidential sources. Today, its attorneys provide pro bono legal representation, amicus curiae support, and other legal resources to protect First Amendment freedoms and the newsgathering rights of journalists.

The Reporters Committee supports the requirement in the Public Oversight of Surveillance Technology Act that the NYPD publicly promulgate and establish policies to regulate how surveillance technologies can be used. The comments below suggest improvements to the draft impact and use policies to ensure they protect newsgathering and address the First Amendment risks posed by surveillance technologies.

Specifically, the comments below include one global recommendation—that all of the proposed impact and use policies include language reaffirming First Amendment protections for newsgathering and precluding the use of surveillance technologies in a manner that would weaken those protections.

We also recommend that the NYPD establish strict guidelines for the use of surveillance technologies to gather confidential journalist work product or identify anonymous sources, similar to those in place at the United States

Department of Justice. *See* 28 C.F.R. § 50.10. Among other critical protections for the press, these federal news media guidelines require notice to an affected news organization or journalist when records are gathered from third parties, § 50.10(a)(4); attorney general approval for most uses of investigative tools to gather evidence from journalists, § 50.10(c)(1); and that the government make all reasonable attempts to obtain the information from alternative non-media sources, §50.10(c)(4)(iii).

Finally, we offer brief recommendations to improve the proposed policies in three areas: 1) cell-site simulators; 2) social media monitoring and news aggregation; and 3) drone detection systems.

I. First Amendment protections for newsgathering should explicitly inform surveillance policy.

As a general matter, law enforcement surveillance technologies create unique risks for newsgathering and the exercise of other First Amendment rights that protect the free press. Surveillance technologies can directly implicate newsgathering rights through the interception of communications content and the monitoring of the activity of journalists. Such technologies can also more subtly chill the free flow of information.

As such, the Reporters Committee often files friend-of-the-court briefs explaining that, unless surveillance technology is subject to appropriate checks, its use can, for instance, dissuade journalistic sources from disclosing information in the public interest. *See, e.g.*, Brief for the Reporters Committee and Nineteen Media Organizations as Amicus Curiae, *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018), <https://perma.cc/7PT2-PFL7> (arguing for a warrant requirement for cell-site location data); Brief for the Reporters Committee and Eight Media Organizations as Amici Curiae, *U.S. v. Moore-Bush*, Nos. 19-1582, 19-1583, 19-1625, 19-1626 (1st Cir. 2021), <https://perma.cc/A2NV-L7LT> (same for persistent, targeted video surveillance).

Accordingly, we recommend that the impact and use policies explicitly protect newsgathering and other First Amendment rights regarding the press, including the First Amendment right to document police activity in public and protections against First Amendment retaliation. We recommend adding specific references to these First Amendment rights as limitations on surveillance authority to the language about constitutional limits already included in each draft policy.

The drafts reference federal and state constitutional protections as limitations on surveillance action broadly and with respect to racial bias. For instance, many drafts include this limiting language: “[Surveillance technology] must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.” *See, e.g.*, Proposed Policy, Cell-Site Simulators, at 2. Many drafts also include the following, or similar, language: “The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution.” *See, e.g.*, Proposed Policy, Cell-Site

Simulators, at 5. Adding language to the effect of, “surveillance technology must be used in a manner consistent with federal and state constitutional and statutory protections for newsgathering,” would underscore for both the NYPD and the public the importance of these rights.

Additionally, some draft policies would limit the use of the relevant technology with respect to certain political activity. For instance, the Facial Recognition policy states: “The NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies.” Proposed Policy, Facial Recognition Technology, at 3. We recommend adding language specifically limiting the use of surveillance technologies against journalists or news organizations. For instance, facial recognition or location tracking technologies should not be used to identify reporters’ sources or track reporters’ movements when they are engaged in lawful newsgathering.

Many policies are right to include mention of the *Handschu* agreement, a 1985 consent decree governing NYPD investigations into political activity, which is a particularly important check on First Amendment violations in the surveillance context. Several draft policies, however, do not include language about the *Handschu* agreement.¹ While this may be an oversight, we recommend including such language in all policies governing technologies that could be used to surveil political activity. Alternatively, if a technology is exempt from the *Handschu* decree, the policy should explicitly explain why. Moreover, while the *Handschu* agreement is a critical framework to protect associational rights, we recommend that the policies expressly include protections for newsgathering and the First Amendment rights of the press, as discussed above.

Further, we urge the NYPD to consider revising the relevant surveillance policies to include measures modeled on the United States Department of Justice’s news media guidelines, or to adopt a set of guidelines governing all NYPD investigative activity. *See* 28 C.F.R. § 50.10. Such additions should include, as the federal guidelines do, requirements for high-level approval before the NYPD initiates surveillance on or gathers evidence from journalists, as well as notice to affected news organizations and journalists if surveillance technologies are used to collect communications content or records from third parties.

The notice provisions are particularly important for journalists in the context of electronic surveillance; without them, journalists may never know their records have been collected, which can compromise the identities of confidential sources beyond the scope of the relevant investigation. *See, e.g.,* Linda Moon and Brendan Stautberg, *DOJ News Media Guidelines Notice Requirement is a Crucial Protection for News Media*, Reporters Committee for Freedom of the Press (Oct. 1, 2019), <https://perma.cc/277S-C7JT>.

¹ The following policies do not include language about the *Handschu* consent decree’s applicability: Case Management Systems, Criminal Group Database, Domain Awareness System, Drone Detection System, Iris Recognition, Mobile X-Ray Technology, ShotSpotter, Thermographic Cameras, and Vehicle Mounted Cameras.

The other critical feature of the federal guidelines is a requirement that the government make all reasonable attempts to obtain information from alternative, non-media sources before seeking to use investigative authorities to collect information from the news media. That requirement should likewise apply to the use of surveillance technologies to collect information from journalists or news organizations by the NYPD.

The Reporters Committee coordinates a dialogue between the Justice Department and news organizations regarding the implementation of the federal guidelines and can serve as a resource to other government entities in formulating similar policies.

II. Policy-specific recommendations.

A. Cell-site simulators.

The cell-site simulator draft policy currently states “cell-site simulators are not used to collect the contents of any communication or any data contained on the device itself. Cell-site simulators also do not capture emails, texts, contact lists, images or any other data from the device.” *See* Proposed Policy, Cell-Site Simulators, at 1. We understand this language to reflect either current practice or the current technological capabilities of the specific devices used by NYPD. We recommend changing the language to “cell-site simulators may not be used” and “cell-site simulators also may not capture” to reflect an affirmative limitation on use. This change would also ensure that cell-site simulators may not be used to collect content or data present on the device, were future generations of the NYPD’s technology to have that capability.

Separately, the data-retention portion of the cell-site simulator draft policy currently reads, “As the NYPD does not record, store, or retain any of the data processed [by] cell-site simulators, there are no policies or procedures relating to retention, access, and use of collected data.” Proposed Policy, Cell-Site Simulators, at 3. Elsewhere, the draft policy states that cell-site simulators “support[] locating missing persons, victims of abductions, and criminal suspects.” Proposed Policy, Cell-Site Simulators, at 1.

We understand the former statement to reflect a policy of non-retention. If, in fact, some data returned from cell-site simulators is retained for specific investigations, we recommend that be explained in the policy. Conversely, if data returned from cell-site simulators is always discarded, even when relevant to a specific investigation, that should also be expressly stated in the policy.

The use of cell-site simulators raises important First and Fourth Amendment considerations, as they can collect information from devices other than the target device (including reporters who are in the vicinity of the target device), and their location-tracking capabilities are particularly potent. *See, e.g., People v. Gordon*, 58 Misc. 3d 544, 551 (Sup. Ct. Kings Cty. 2017) (“By its very nature, then, the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping, and requires a separate warrant supported by probable cause rather than a mere pen register/trap and trace order such as the one obtained in this

case by the NYPD.”). Accordingly, greater clarity is needed in the proposed policy in terms of how the information generated by cell-site simulators is actually used to determine whether the NYPD’s lack of a retention, use, or access policy for this technology is appropriate.

B. Protections for social media monitoring and media aggregation.

Social media network analysis tools, as described, allow the NYPD to review, process, and retain information on social networking platforms, including when the information at issue is deleted. Media aggregation services search public sources of information for pieces relevant to the NYPD, alert the NYPD, and provide associated details, including if a social media user on a specified platform posted the information.

We recommend amending these policies to include strong protections for the First Amendment activity that takes place via these mediums, especially by journalists. These protections should underscore, as one example, that the NYPD will not track journalist activity or generate journalist social media or news “watchlists” or other law enforcement products based on reporting perceived as critical. Even “open source” tracking of journalist activity can raise significant First Amendment considerations. *See, e.g.,* Wendi C. Thomas, *The Police Have Been Spying on Black Reporters and Activists for Years. I Know Because I’m One of Them*, ProPublica (Jun. 9, 2020), <https://perma.cc/Y8AX-EPRP> (describing Memphis Police Department social media monitoring of a journalist); Shane Harris, *DHS Compiled ‘Intelligence Reports’ on Journalists who Published Leaked Documents*, Wash. Post (Jul. 30, 2020), <https://perma.cc/U73C-7TRG> (describing DHS intelligence reports on two journalists who tweeted leaked but unclassified documents about federal law enforcement efforts during the 2020 protests).

C. Protections for drone journalism.

Unmanned aerial systems are powerful newsgathering tools. Journalists use drones to cover events and provide reporting in the public interest in ways that would not otherwise be possible. The draft use policy for drone detection systems indicates that the NYPD uses this technology to “detect, identify, and monitor UAS flying within New York City airspace posing a credible threat to public safety, city facilities, and critical infrastructure.” Proposed Policy, Drone Detection Systems, at 1.

Drone monitoring capabilities carry the risk of improper government surveillance of newsgathering activities. We recommend the NYPD develop a system that would exclude newsgathering drones from the monitoring capabilities of drone detection systems. Such a system could, for instance, halt the real-time tracking of news drones that have been identified as such. *Cf.* Comments of the News Media Coalition to the FAA re Remote Identification of Unmanned Aircraft Systems (May 2, 2020), <https://perma.cc/HUT6-2BGU>. To the extent location information on news drones is collected in an NYPD database, the impact and use policy should also include strict limitations on access and retention, specific to that information.

* * *

As explained above, the Reporters Committee recommends that the NYPD's impact and use policies for surveillance technologies include robust, affirmative protections for newsgathering and the First Amendment rights of the press. Please do not hesitate to contact Maily Fidler, Technology and Press Freedom Fellow at the Reporters Committee, with any questions. She can be reached at mfidler@rcfp.org.

Sincerely,

Bruce D. Brown
Executive Director, Reporters Committee for Freedom of the Press

Gabe Rottman
Director, Technology and Press Freedom Project

Maily Fidler
Technology and Press Freedom Legal Fellow

Grayson Clary
Stanton Foundation National Security/Free Press Fellow