POLICE DEPARTMENT
Office of Deputy Commissioner,
Legal Matters
One Police Plaza, Room 1406A
New York, New York 10038

February 4, 2016

Ms. Mariko Hirose
New York Civil Liberties Union
125 Broad Street, 19th Floor
New York, New York 10004

RE: FREEDOM OF INFORMATION LAW
REQUEST: #15-PL-3861

Dear Ms. Hirose:

This letter is in response to your letter dated November 18, 2015, which sought to administratively appeal portions of the Records Access Officer's (RAO) letter dated October 30, 2015, which determined the NYCLU's request for records that pertain to cell site simulators (CSS or CSSs) made by letter dated April 13, 2015, pursuant to the Freedom of Information Law, N.Y. Public Officers Law (POL) §§ 84 *et seq.* (FOIL).

Preliminarily, the administrative appeal, as limited by the terms of the November 18, 2015, letter, stated that it is based on the NYPD's failure to meet its burden of articulating "'particularized and specific justification[s] for withholding" records pursuant to FOIL's exemptions. The appeal on this basis is denied, because the burden on an agency's Records Access Officer is only to grant or deny a FOIL request. See, POL § 89(3)(a). The Court of Appeals has explained that the requirement that an agency articulate particularized and specific justifications for denying access to records only applies to the agency's burden of proof *in litigation* -- not at the administrative level. See, Capital Newspapers v. Burns, 67 N.Y.2d 562, 566 note * (1986). FOIL requires that if an administrative appeal is taken, the appeal determination "fully explain" the reasons for a further denial of the request in the event that the appeal is not granted. See, POL § 89(4)(a). The RAO's letter dated October 30, 2015, and the instant determination, fully comply with these statutory requirements, and this basis for the appeal must be denied.

The November 18, 2015, letter asserts that many of the statutory grounds identified by the RAO as a basis for the partial denial of access are inapplicable, irrelevant, or otherwise inapposite with respect to the FOIL request. However, 6 USC § 482(f)(1), which defines "homeland security information," specifies that it applies to "any information" possessed by a local agency that relates to the threat of terrorist activity, or to the ability to prevent, interdict, or disrupt such activity, or that would improve the response to a terrorist act or assist in the investigation or identification of a suspected terrorist actor. The use of CSS technology by a local law enforcement agency within the context of criminal investigations does not remove

information pertaining to use of CSS equipment from the protection of the statute, since the use of a CSS in a criminal investigation that does not involve terrorism does not diminish the ability of an agency to use a CSS as part of its response to a past, present, or future terrorist act. The public disclosure of such information would allow terrorist actors and other potential investigative subjects to develop and implement countermeasures to these counterterrorism tools and to the nonroutine criminal investigative techniques that are involved in the utilization of this technology. This is precisely the type of disclosure that the exempting statutes were enacted to preclude.

POL 87(2)(a) permits an agency subject to FOIL to deny access to records that are exempt from disclosure pursuant to a state or federal statute. Therefore, in addition to the exemptions specifically defined by the POL, FOIL also incorporates the exemptions from, and prohibitions on, the disclosure of records and/or information that are defined by numerous other statutory provisions.

22 CFR § 121.1 Category XI includes within the United States Munitions List electronic systems and equipment that intercept, identify, or locate sources of intentional or unintentional electromagnetic energy in order to provide threat detection, recognition, targeting, planning, or conduct of future operations, as well as electronic systems, equipment or software specially designed for intelligence purposes that collect, survey, monitor, or exploit, or that analyze and produce information from the electromagnetic spectrum. See, 22 CFR § 121.1 Category XI (a)(4)(i) and 22 CFR § 121.1 Category XI (b). As a regulated defense article pursuant to 22 USC § 2278, CSS technology and details of its operational use or inner workings are also subject to the non-disclosure provisions of the International Traffic In Arms Regulations (ITAR), 22 CFR Parts 120-130.

Moreover, because the CSS technology is used in intelligence gathering for homeland security and national defense purposes, it is subject to the prohibition on the disclosure of intelligence sources and methods, pursuant to several federal laws incorporated into FOIL pursuant to POL § 87(2)(a), as well as pursuant to the protective provisions within FOIL for confidential and/or non routine investigative techniques and procedures, POL § 87(2)(e)(iii) and (iv). Disclosing details of the use of CSSs is neither required nor permitted because such disclosure would diminish the ability of law enforcement entities to conduct investigations.

The invocation of 47 CFR § 0.457 is appropriate because telecommunications devices are subject to the jurisdiction of the Federal Communications Commission (FCC), and the non-disclosure rules promulgated by the FCC, which preclude the disclosure of records within the FCC's jurisdiction that are not generally available for public inspection, are incorporated to FOIL by way of POL § 87(2)(a). These rules apply to CSSs as well as to cellular telephones.

The denial of access pursuant to 18 USC § 3123 is appropriate and applicable to shield details of any application for an order, or of any order issued that pertains to the use of CSSs. This federal statute prohibits disclosure of information that was sought in the FOIL request, and constitutes a further basis for denial, in addition to the prohibitions on such disclosure contained in Article 705 of the NY Criminal Procedure Law. Both federal and New York pen register statutes provide an exemption from disclosure for the information sought in the FOIL request as

to the specific instances and circumstances in which such orders were sought. Moreover, neither statute pre-empts the other, and each statute provide an independent prohibition on the disclosure of the information requested.

In addition to the foregoing, additional explanations specific to the denial of numbered categories of information specified in the November 18, 2015, letter are set forth below.

Request "1." The RAO's denial of the request for purchase orders, invoices, contracts, loan agreements, and similar records regarding the acquisition of CSSs was properly made because the disclosure of the commercial and technical information contained in such records is exempt pursuant to the statutes cited by the RAO, including those whose applicability is more fully explained herein. First, the public disclosure of commercial information such as price, delivery times, and other contract terms that pertain to specified equipment within a specific business relationship would impair the ability of buyers and sellers to finalize contract negotiations and is not required pursuant to POL § 87(2)(c). Second, such commercial and technical information, which has not previously been disclosed, remains a trade secret that is proprietary to the manufacturer, and is exempt from disclosure pursuant to POL § 87(2)(d). Also, 87(2)(g) exempts predecisional materials that pertain to purchases of equipment and applies to shield such predecisional information from disclosure.

In addition, technical details that are proprietary to the CSS equipment are also exempt under POL § 87(2)(e)(iii) and (iv), in that their disclosure would (1) constitute the disclosure of confidential information that is used in criminal investigations and also (2) reveal non routine criminal investigative techniques, the disclosure of which would permit criminals to evade detection and apprehension.

As a corollary, the availability of such information to kidnappers, terrorists, or other actual or potential perpetrators of serious crimes could endanger the life or safety of a victim, of bystanders, and of numerous others if a perpetrator is able to evade detection as a result of engaging in countermeasures enabled through knowledge of such technical or proprietary details. Furthermore, CSS equipment is a type of information technology asset in the hands of law enforcement, and the disclosure of detailed information pertaining thereto would make it impossible to guarantee the security of such information technology, and is therefore not required pursuant to POL § 87(2)(i).

For the reasons explained earlier in this letter, the information requested in Request "1" is also prohibited from disclosure under 6 USC § 482(f)(1), under the ITAR, and pursuant to 47 CFR 0.457, which federal provisions are incorporated into FOIL by POL § 87(2)(a).

Request "3." The RAO's diligent search located the two pages which were provided in redacted form. The search failed to locate a copy of a non-disclosure agreement (NDA) between the NYPD and the FBI regarding CSSs. The bases for the redaction of proprietary information from this document are POL § 87(2)(c) and (d), as well as the federal provisions cited in the previous paragraph, the applicability of which is fully explained hereinabove. In addition, to the extent that your office has already obtained an unredacted copy

of the NDA applicable to Harris Corporation sales to municipal entities, as evidenced by the Exhibit annexed to the November 18, 2015, letter, your request is moot.

Request "5."

The NYPD serves court orders directing the implementation of pen registers and/or trap and trace devices upon wireless service providers, and communications providers send bills for implementing such orders. There are no communications between the NYPD and wireless service providers regarding the use of CSS technology in any particular investigation or about the use of such technology in general. CSS technology is used in just a small fraction of the investigations in connection with which a court has ordered the use of a pen register and/or trap and trace device. The court orders and the service thereof are prohibited from disclosure pursuant to POL § 87(2)(a) and NY Criminal Procedure Law (CPL) § 705.30, which provides that a pen register order must direct that the order be sealed, and that the person or entity that obtained the order and any entity providing assistance in connection with the implementation of the order be prohibited from disclosing information about the investigation that resulted in the issuance of the order. Included within the information prohibited from disclosure is the billing information, which pertains to each implementation of a pen register and/or trap and trace device order. Similar statutory protection is also afforded by 18 USC § 3123. Since each time a particular order of the court is served on a wireless service provider it includes some identifiable subscriber information, privacy concerns were properly identified by the RAO as a further basis for denying access. This is also the case when the service provider sends an invoice. The significant privacy concerns that apply to each intercept, regardless of the outcome of the investigation and/or prosecution, are therefore protected from disclosure by POL §§ 87(2)(b) and 89(2)(b). The confidential and nonroutine nature of the investigatory records were also properly claimed by the RAO as a basis for exemption.

Requests "8" and "9." The RAO's October 30, 2015, letter granted Requests 7 and 8 to the extent of providing information about all NYPD investigations which led to an over-the-air intercept. The information provided identified the NYPD unit conducting the investigation, the wireless carrier that serviced the target number, the results of the intercept, and the top charge for those cases that resulted in an arrest. The RAO explained that as a rule, court orders pursuant to CPL Article 705 were obtained prior to attempting an over-the-air intercept, and the RAO provided information about investigations involving exigent circumstances wherein a court order had not been obtained prior to the initiation of the interception attempt. The RAO's response provided information in tabular form, providing charts which reflect the number of investigations wherein CSSs were utilized, as well as the nature of the authorization obtained prior to the investigative use of cell site simulators and the number of investigations that resulted in prosecutions. The materials provided by the RAO listed the cases where due to exigent circumstances a court order had not been obtained prior to attempting the intercept, and identified the crime or situation that gave rise to the exigent circumstances in each case. The RAO provided the top charge for cases where intercepts led to prosecutions. Accordingly, the RAO's response provided all of the information sought in Request number 7, and all of the information sought in Request number 8 except for a list of court docket numbers for each of the intercepts.

The RAO properly denied the request for a list of court docket numbers for cases stemming from CSS intercepts because the NYPD does not maintain such a list and the further ground that such a list could not be compiled with reasonable efforts. These grounds also apply to cases pursuant to which an application for a pen register and/or trap and trace device order was made. In addition, even if a list containing this information had been in existence, it would not be subject to disclosure because the court docket numbers sought in Request number 8 would be sufficient to identify the defendant, and thereby would violate the provisions of CPL §§ 705.30, 705.35 and 18 USC § 3123, as well as of the court orders issued pursuant to such statutory authority, which prohibit such disclosure. This information is also exempt from disclosure pursuant to POL § 87(2)(e)(i) and (ii) in that its disclosure would result in interference with the conduct of criminal prosecutions and deprive persons of the right to a fair trial and/or impartial adjudication. Moreover, such information would violate privacy rights protected from disclosure by POL §§ 87(2)(b) and 89(2)(b), and is further exempt from disclosure because it would tend to reveal confidential information relating to criminal investigations, the disclosure of which is precluded by POL § 87(2)(e)(iii).

Moreover, the court orders that directed the installation of each pen register and/or trap and trace device prohibit, by their own terms, the disclosure of this information. This information is also exempt from disclosure pursuant to POL § 87(2)(a) and CPL § 705.35.

Other exemptions under FOIL may also apply. You may seek judicial review of this determination by commencing an Article 78 proceeding within four months of the date of this decision.

Sincerely,

Jonathan David
Records Access Appeals Officer

c: Committee on Open Government