County of Union, Illinois
Office of the Chief Information Officer
309 W. Market—Room 115
Jonesboro, IL 62952

Rollie Hawk, CIO
(618) 925-2470
cio@unioncountyil.gov
@unioncountycio

January 26, 2015

[Sent via email]

Mark Birhanu c/o Khadine Bennett
Roger Baldwin Foundation of ACLU, Inc. 180 N. Michigan Avenue
Suite 2300
Chicago, IL 60601-1287

kbennett@aclu-il.org

Ms. Bennett:

Please consider this our response to your January 20, 2015 Freedom of Information Act request:

> *We write to seek information about Automatic License Plate Reader ("ALPR") technology and StingRay technology pursuant to the Freedom of Information Act ("FOIA"). 5 ILCS 140/1 et seq. ALPR technology is also sometimes referred to as Automatic Vehicle Identification, Car Plate Recognition, or License Plate Recognition technology. This records request uses ALPR in reference to any technology which is described by these terms or is substantially similar to the technology so described. StingRay technology is also sometimes referred to as IMSI-catcher (International Mobile Subscriber Identity) technology, portable technology such as a Kingfish or Cell Site Simulators. This records request uses StingRay in reference to any technology which is described by these terms or is substantially similar to the technology so described.*

The Union County Sheriff's Office does not use any of the technology noted in your request and has not during the period from July 30, 2012 through today. As such, we have no records responsive to your request.

We feel this completes your request. If we may be of further assistance, please let me know.

Sincerely,

Rollie Hawk, Chief Information Office

Enclosure

Cc: Tyler Edmonds, State's Attorney
Scott Harvel, Sheriff

AMERICAN CIVIL LIBERTIES
UNION OF ILLINOIS

180 NORTH MICHIGAN AVENUE
SUITE 2300
CHICAGO, IL 60601
T/312.201.9740
F/312.201.9760
WWW.ACLU-IL.ORG

Received
2015-01-20

January 9, 2015

VIA FACSIMILE AND U.S. MAIL

Union County, Illinois
Rollie Hawk
Chief Information Officer
309 W. Market
Room 115
Jonesboro, IL 62952

Re: FOIA request regarding police department deployment of Automatic License Plate Reader ("ALPR") technology and StingRay technology

Dear Freedom of Information Officer:

We write to seek information about Automatic License Plate Reader ("ALPR") technology and StingRay technology pursuant to the Freedom of Information Act ("FOIA"). 5 ILCS 140/1 *et seq.* ALPR technology is also sometimes referred to as Automatic Vehicle Identification, Car Plate Recognition, or License Plate Recognition technology. This records request uses ALPR in reference to any technology which is described by these terms or is substantially similar to the technology so described. StingRay technology is also sometimes referred to as IMSI-catcher (International Mobile Subscriber Identity) technology, portable technology such as a Kingfish or Cell Site Simulators. This records request uses StingRay in reference to any technology which is described by these terms or is substantially similar to the technology so described.

The time period for the request is from July 30, 2012 until the time of the production of the information.

Specifically, we seek the following records[737]:

---

[737] The term "records" as used herein includes, but is not limited to, all documents or communications of any kind preserved in electronic or written form, including but not limited to, correspondence, documents, data, videotapes, audiotapes, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, audits, studies, inquiries, examinations, inspections, investigations, probes, surveys, rules, technical manuals, technical specifications, training manuals, and/or computer files and databases.

1. All records sufficient to show whether your police department has an ALPR.

2. All records regarding your policies, practices, and procedures relating to ALPR technology, including but not limited to:

    a. Your agency's policies, practices and procedures for procuring and using ALPR technology;
    b. Your agency's policies, practices and procedures for storing, accessing and sharing data obtained through ALPR technology.

3. All records regarding the procurement of ALPR technology, including but not limited to:

    a. sources of funds used to pay for ALPR technology;
    b. local government approval for any ALPR purchase.

4. Records sufficient to show the following regarding the use of ALPR technology:

    a. what types of data are obtained by the use of ALPR technology;
    b. number of license plates scanned and/or read for each month in the time period;
    c. number of ALPR units or systems acquired;
    d. number of ALPR units or systems which are actively deployed;
    e. method and location of that deployment for each unit or system actively deployed (e.g. mobile vehicle, street location of red light camera, etc.);
    f. technical capabilities of the ALPR units;
    g. number of "hits" (alerts provided by the ALPR system that it has scanned a license plate flagged for surveillance by your department or a cooperating document) which have occurred since your implementation of ALPR technology;
    h. categorization of all "hits" by reason vehicle was flagged for surveillance (e.g. unpaid parking tickets; outstanding warrant; etc.).

5. Records sufficient to show the following regarding the sharing of data obtained through ALPR technology:

    a. what type of data is shared;
    b. which databases your agency puts collected ALPR data into;
    c. third parties, governmental or private, that may access your agency's ALPR data, including what procedures third parties must go through in order to access the data and any restrictions placed on third parties regarding further sharing of your ALPR data;
    d. any agreements to share ALPR data with outside agencies, corporations or other entities.

6. All training materials used to instruct members of your agency in ALPR deployment, data management, or operation of automated records systems that contain ALPR data to

which any member of your agency has access, including regional or shared ALPR databases.

7. All records sufficient to show whether your police department has a StingRay.

8. Records sufficient to show the following regarding your policies, practices, and procedures relating to StingRay technology, including but not limited to:
    a. Your agency's policies,[738] practices, training records,[739] and procedures for procuring and using StingRay technology, including but not limited to: (a) restrictions on when, where, how, and against whom they may be used; and (b) guidance on when a warrant or other legal process must be obtained;
    b. Your agency's policies, practices and procedures for storing, accessing and sharing data obtained through StingRay technology, including but not limited to (a) limitations on retention and use of collected data; and (b) rules governing when the existence and use of StingRay technology may be revealed to the public, criminal defendants, or judges.

9. All records regarding the procurement of StingRay technology, including but not limited to:

    a. sources of funds used to pay for StingRay technology;
    b. local government approval for any StingRay purchase;
    c. records regarding any offers, arrangements, or agreement with any local, county, or regional law enforcement agencies to loan, provide use of, or otherwise utilize cell site simulators owned or possessed by your agency;
    d. all nondisclosure agreements regarding the possession and use of cell site simulators, with companies providing the devices, and with any local, state, or federal agencies.

10. Records sufficient to show the following regarding the use of StingRay technology, including but not limited to:
    a. what types of data are obtained by the use of StingRay technology;
    b. communication or agreements with any wireless service provider concerning the use of StingRay technology;
    c. communication or agreements with any government agency concerning the use of StingRay technology;
    d. number of times StingRay's Cell Site Simulator capability was deployed;
    e. number of times each StingRay device established a new connection with a cellular device for each month in that time period;

---

[738] The term "policies" as used herein includes, but is not limited to, all general orders, special orders, bulletins, notices, directives, pronouncements, forms, memoranda, legal standards, rules, and regulations.

[739] The term "training records" as used herein includes, but is not limited to, all records regarding or relating to training, including but not limited to all orders, manuals, instructions, guidelines, course curricula, lesson plans, presentations, handouts, videotapes, audiotapes, DVDs, and similar materials in electronic or written form.

f. number of times the IMSI, ESN, or other identifying data from each of the devices connected to the StingRay was downloaded for each month in that time period;
g. number of times specific surveillance was conducted on a target device located by the StingRay which have occurred since your implementation of StingRay technology;
h. categorization of all specific surveillance on a target device;
i. number of investigations in which StingRay technology has been used, and the number of those investigations that have resulted in prosecution;
j. all applications submitted to state or federal courts for search warrants or orders authorizing use of StingRay technology in criminal investigations, as well as any warrants or orders, denials of warrants or orders, and returns of warrants associated with those applications. If any responsive records are sealed, please provide the date and docket number for each sealed document;
k. all records regarding use of StingRay technology in closed investigations;[740]
l. number of times a StingRay conducted a GSM Active Key Extraction to obtain the target device's stored encryption key;
m. number of times an encryption key to authenticate the StingRay to the service provider as being part the target device was used to forward signals between the target device and cell site while decrypting and recording communications content;
n. number of times a StingRay conducted base station surveys;
o. number of times a StingRay jammed radio devices.

11. All records regarding the storage of data obtained using StingRay technology, including but not limited to:

    a. what types of data are stored for any period longer than an hour;
    b. how long data is stored;
    c. when data must be discarded;
    d. how many IMSIs or equivalent identifiers your agency currently stores.

12. All records regarding access to StingRay data, including but not limited to:

    a. the legal justification required before an individual accesses StingRay data;
    b. purposes for which the data may be accessed;
    c. purposes for which the data may *not* be accessed;
    d. who may access the data, what procedures they must go through to obtain access, and who must authorize access;
    e. the existence or non-existence of a system that records who accesses the data and when the data is accessed.

[740] The ACLU does not seek records relating to open investigations. The ACLU does seek records relating to investigations that have been closed, but where judicial proceedings relating to prosecution or appeal are still pending.

13. All training materials used to instruct members of your agency in StingRay deployment, data management, or operation of automated records systems that contain StingRay data to which any member of your agency has access, including regional or shared StingRay databases.

Please send the requested materials to:

Mark Birhanu
Roger Baldwin Foundation of ACLU, Inc.
180 N. Michigan Avenue
Suite 2300
Chicago, Illinois 60601-1287

As you know, the Illinois FOIA requires that you make available for inspection and copying all public records, except certain exempt records, within five working days of receipt of a written request.

If you determine that portions of the requested records are exempt from the Act, we expect that you will delete such exempted material and send copies of the remaining non-exempt material within five working days. Also, if all or any part of this request is denied, please provide in writing the specific exemption(s) under the Act on which you rely to withhold the records.

We are prepared to pay reasonable copying costs for reproducing the requested materials, but request that you waive any such fees under the provision of FOIA that authorizes you to waive copying fees when release of requested information is "in the public interest." In compliance with section 6(b) of the amended FOIA, I represent to you that the documents are sought to determine information concerning the legal rights of the general public and this request is not for the purpose of personal or commercial benefit. Accordingly, a waiver of fees is in the public interest as defined by section 6(b).

If you deny the request for waiver, please notify me before compiling records for which the copying charge will exceed $50.00 so that we can discuss narrowing the request to cover only the information I seek.

Please contact me at 312/201-9740 ext. 332, or via email at kbennett@aclu-il.org, if you have any questions regarding this request. Thank you for your prompt attention.

Sincerely,

Khadine Bennett
Staff Attorney

AMERICAN CIVIL
LIBERTIES UNION OF
ILLINOIS
180 NORTH MICHIGAN AVENUE
SUITE 2300
CHICAGO, IL 60601

S SUBURBAN
IL 604
13 JAN '15
PM 4 L

Union County, Illinois
Rollie Hawk
Chief Information Officer
309 W. Market
Room 115
Jonesboro, IL 62952

62952123940