

5 April 2019

**IN THE FIRST TIER TRIBUNAL  
GENERAL REGULATORY CHAMBER  
(INFORMATION RIGHTS)**

**Appeal nos: EA.2018.0164 and 0170**

**B E T W E E N :**

**PRIVACY INTERNATIONAL**

**Appellant**

**-and-**

**(1) THE INFORMATION COMMISSIONER'S OFFICE**

**(2) COMMISSIONER OF THE METROPOLITAN POLICE**

**(3) POLICE AND CRIME COMMISSIONER FOR WARWICKSHIRE**

**Respondents**

---

**FIRST WITNESS STATEMENT OF  
NATHAN FREED WESSLER**

---

I, Nathan Freed Wessler, staff attorney, American Civil Liberties Union Speech, Privacy and Technology Project, 125 Broad Street, 18th Floor, New York, NY 10004, say as follows:

**INTRODUCTION**

1. I make this statement in relation to the appeal to the First-tier Tribunal by the Appellant challenging the Information Commissioner's Office's decisions upholding various public bodies' refusals to confirm or deny the existence of records responsive to Freedom of Information Act requests about purchase and use of IMSI Catchers.
2. Where the contents of this statement are within my knowledge, I confirm that they are true; where they are not, I have identified the source of the relevant information, and I confirm that they are true to the best of my knowledge and belief.
3. I exhibit to this statement a consecutively paginated bundle of documents labelled "NW1/x/y", where 'x' is the exhibit number and 'y' is the page number.
4. I am a staff attorney with the Speech, Privacy, and Technology Project of the American

Civil Liberties Union (“**ACLU**”), based in New York City. Founded in 1920, the ACLU is a non-governmental organization with more than 1.5 million members dedicated to defending the civil liberties and civil rights guaranteed by the United States Constitution. Among the issues on which the ACLU focuses is ensuring that U.S. law enforcement agencies’ uses of surveillance technologies comply with civil liberties and human rights standards set out in the Constitution and laws of the United States. In service of this goal, the ACLU often seeks records from the law enforcement agencies pursuant to the U.S. Freedom of Information Act and its state-law analogues.

5. I have particular expertise in issues of law and policy involving police use of surveillance technologies and police access to sensitive digital data, as well as the use of freedom of information laws to obtain information from government agencies about their policies and practices in this area. I have considerable experience in issues raised by the use of “IMSI Catchers” by police in the United States to locate, track, and surveil mobile phones. I have briefed and litigated numerous cases involving law enforcement use of surveillance technologies and searches of digital data, including cases involving mobile phone tracking and IMSI Catchers. In 2017, I argued *Carpenter v. United States* in the United States Supreme Court, a landmark case that established that under the Fourth Amendment to the U.S. Constitution, police must obtain a search warrant before seeking mobile phone location records from a person’s cellular service provider. I have filed briefs and/or presented oral argument as *amicus curiae* in cases challenging the warrantless use of IMSI Catchers across the United States,<sup>1</sup> and have filed numerous requests under the federal Freedom of Information Act and state public records laws for records involving law enforcement agencies’ purchase and use of that technology. Finally, I have significant experience with government agencies refusing to confirm or deny the existence of records responsive to Freedom of Information Act requests, and have published one of the few law review articles on the subject in the United States.<sup>2</sup> A copy of this article is exhibited to my statement as NW1/1/17-51.

6. In summary, in the United States, law enforcement agencies have overwhelmingly

---

<sup>1</sup> See, e.g., *Jones v. United States*, 168 A.3d 703 (D.C. 2017); *State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016); *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016); *United States v. Harrison*, No. 1:14-CR-00170-CCB (D. Md. 2014).

<sup>2</sup> Nathan Freed Wessler, Note, “*We Can Neither Confirm Nor Deny The Existence or Nonexistence of Records Responsive To Your Request*”: *Reforming the Glomar Response Under FOIA*, 85 N.Y.U. L. Rev. 1381 (2010).

responded to freedom of information requests seeking information about purchase and use of IMSI Catchers by identifying records, releasing many records in whole or in part, and withholding other records only after acknowledging their existence. Very few law enforcement agencies in the United States have responded to such requests by stating that they could neither confirm nor deny (“**NCND**”) whether they held the requested information, and even fewer have maintained that position after being challenged.

### **UNITED STATES FREEDOM OF INFORMATION ACT & STATE FREEDOM OF INFORMATION LAWS**

7. Like the United Kingdom’s Freedom of Information Act 2000, the Freedom of Information Act in the United States (“**FOIA**”), 5 U.S.C. § 552, provides a mechanism by which members of the public can request records from government agencies. Under FOIA, an agency must release requested records unless they fall within one of nine enumerated exemptions (as set out in § 552(a)(8) and (b)). Among other categories of records, those exemptions cover: classified national security information; information exempted by other statutes, including statutes protecting certain types of records held by U.S. intelligence agencies; confidential trade secrets; information that would invade personal privacy if released; and records or information compiled for law enforcement purposes that would “*disclose techniques and procedures for law enforcement investigations*”, which are exempt from disclosure “*if such disclosure could reasonably be expected to risk circumvention of the law*”: § 552(b). Where an agency believes an exemption applies, the agency must generally identify the record it seeks to withhold and justify the reason for the withholding.<sup>3</sup>
8. Unlike the Freedom of Information Act 2000 in the U.K., FOIA does not specifically provide the option for agencies to issue an NCND response. However, courts in the United States have interpreted FOIA to allow for NCND responses in the narrow circumstances where confirming the existence or nonexistence of records would itself reveal information protected by an enumerated statutory exemption.<sup>4</sup> In the United States, the decision to NCND the existence of records is generally called a “Glomar response”, after the earliest case recognizing the response.<sup>5</sup>

---

<sup>3</sup> See *Vaughn v. Rosen*, 484 F.2d 820, 826–28 (D.C. Cir. 1973).

<sup>4</sup> See *Phillippi v. Central Intelligence Agency*, 546 F.2d 1009, 1012 (D.C. Cir. 1976); Wessler, 85 N.Y.U. L. Rev. at 1386–87.

<sup>5</sup> See Wessler, 85 N.Y.U. L. Rev. at 1386–87.

9. FOIA applies to requests for records held by any federal government agency, including intelligence agencies, law enforcement agencies, prosecutorial agencies, and the military.
10. Requests to state and local government agencies are governed by separate state public records laws. Although those laws differ in some particulars, they generally take the same form as the federal FOIA: a right of any person to request and receive governmental records unless those records fall within a specified exemption to disclosure.<sup>6</sup> Most state courts have not addressed whether it is proper to assert an NCND response under state public records laws, although at least two courts have allowed such responses.<sup>7</sup>
11. In this statement, the term “FOIA request” refers to requests made under the federal FOIA. The term “public records request” refers to requests made under any public records law, whether the federal FOIA or an analogous state law.

#### **PUBLIC RECORDS REQUESTS FOR IMSI CATCHER INFORMATION IN THE UNITED STATES**

12. IMSI Catchers are a class of technology, also known as “cell site simulators”, “Stingrays”, and other names, that are able to track, locate, and monitor nearby mobile phones. IMSI Catchers function by mimicking mobile phone towers and forcing mobile phones in the area to communicate with the IMSI Catcher rather than with the actual mobile phone network.
13. Although information about the function and use of IMSI Catchers in the United States was once shrouded in secrecy, in recent years public records requests submitted by the ACLU, other non-governmental organizations, and members of the press have revealed significant details about law enforcement agencies’ policies and practices around IMSI Catcher use. We now know, for example, that at least 75 state and local law enforcement agencies located in 27 states and the District of Columbia own IMSI

---

<sup>6</sup> See generally, Reporters Committee for Freedom of the Press, *Open Government Guide*, <https://www.rcfp.org/open-government-guide> (providing information about every state’s public records law) (last accessed 4 April 2019).

<sup>7</sup> See *Abdur-Rashid v. N.Y.C. Police Dep’t*, 100 N.E.3d 799 (N.Y. 2018) (permitting NCND response under New York State Freedom of Information Law); *N. Jersey Media Grp. Inc. v. Bergen Cty. Prosecutor’s Off.*, 146 A.3d 656 (N.J. Super. Ct. App. Div. 2016) (recognizing narrow application of NCND response under New Jersey Open Public Records Act in limited circumstances).

Catchers, as do at least 14 federal law enforcement, military, and intelligence agencies.<sup>8</sup> This information has been gathered together in the ACLU publication, ACLU, *Stingray Tracking Devices: Who's Got Them?* (last updated in November 2018 and exhibited to this statement at NW1/2/53-55).

14. In response to public records requests, law enforcement agencies in the United States have generally acknowledged whether they possess records about IMSI Catchers. Indeed, I am aware of only a few law enforcement agencies in the United States that have asserted NCND responses when presented with a request for information about IMSI Catchers. The police departments in Sunrise, Florida, and Kansas City, Missouri, initially asserted NCND responses, but both agencies quickly retreated from those responses when challenged.<sup>9</sup> The Sunrise Police Department originally justified its response on the grounds that confirming or denying the existence of records could “*reveal the existence of confidential surveillance techniques*” and could “*compromise both active and future criminal investigations*”. However, after the ACLU explained that the agency was interpreting the Florida Public Records Act too expansively, and that the City of Sunrise had *already* confirmed the existence of records by making public certain IMSI Catcher purchasing information as part of its normal procurement process, the agency reversed course, acknowledged the existence of certain records, and stated its intent to search for additional documents. The Kansas City Police Department initially responded to a public records request from a privacy activist by explaining that an NCND response was proper to “*maintain confidentiality of covert operations and sensitive equipment*”. However, after receiving a similar request from a reporter, the agency changed tack without explanation, acknowledging the existence of records and releasing a number of records pertaining to the purchase and use of IMSI Catchers. The Maine State Police also issued an NCND response, but provided no explanation or

---

<sup>8</sup> ACLU, *Stingray Tracking Devices: Who's Got Them?* (Nov. 2018), <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them> (last accessed 4 April 2019).

<sup>9</sup> See Nathan Freed Wessler, *Local Police in Florida Acting Like They're the CIA (But They're Not)*, ACLU Free Future (25 Mar. 2014), <https://www.aclu.org/blog/local-police-florida-acting-theyre-cia-theyre-not>; Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, ACLU Free Future (22 Feb. 2015), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida>; Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, Kansas City Star, 5 Sept. 2015, <https://www.kansascity.com/news/business/technology/article34185690.html> (all last accessed 4 April 2019).

justification, either initially or in response to an appeal letter.<sup>10</sup> An NCND response from the United States Fish and Wildlife Service merely cited the need to “*protect[] law enforcement records*”.<sup>11</sup> Neither of the latter NCND responses was challenged in court.

15. Unlike these few agencies that have asserted NCND responses, the vast majority of agencies have acknowledged whether they have responsive records. This is true of major federal law enforcement agencies such as the Federal Bureau of Investigation and the Drug Enforcement Administration and smaller federal agencies such as the Criminal Division of the Internal Revenue Service; of state police agencies from states large and small, from the Florida Department of Law Enforcement to the Delaware State Police; and of police departments in cities ranging in size from New York City, Los Angeles, and Chicago, to Lakeland, Florida, and Rochester, New York. I am aware of many dozens of law enforcement agencies that have responded to public records requests by acknowledging whether they possess records regarding IMSI Catchers. In most cases, the duty to acknowledge the existence of IMSI Catcher records is so clear that it is not contested in any way by the agency. This is true even for agencies, such as the New York City Police Department and the Federal Bureau of Investigation, that have issued NCND responses in reaction to other public records requests on different topics. Even agencies that refuse to release any records regarding IMSI Catchers have acknowledged their duty to explain “*that records are in existence, but that they are not subject to public disclosure*”.<sup>12</sup>
16. An agency’s decision not to issue an NCND response does not mean, of course, that it must necessarily release all of its records pertaining to IMSI Catchers. Law enforcement agencies have routinely determined that some records pertaining to the use of IMSI Catchers should be withheld in full or in part. For example, some agencies have released invoices, purchase orders, and other records documenting their purchase of IMSI Catchers, but have redacted information about the specific IMSI Catcher model

---

<sup>10</sup> Curtis Waltman, *Maine State Police “Can Neither Confirm Nor Deny” Use of Cellphone Surveillance*, Muckrock (9 Nov. 2016), <https://www.muckrock.com/news/archives/2016/nov/09/msp-glomar/> (last accessed 4 April 2019).

<sup>11</sup> *Does Cellphone-Sweeping “StingRay” Technology Go Too Far?*, CBS News (27 Nov. 2017), <https://www.cbsnews.com/news/does-cellphone-sweeping-stingray-technology-go-too-far/> (last accessed 4 April 2019).

<sup>12</sup> See Broward Cty. Sheriff’s Office (Florida) response to Nathan Freed Wessler, ACLU (13 May 2014), <https://www.aclu.org/files/assets/floridastingray/05.20.2014%20-%20Additional%20Information%20re%20Claimed%20Exemptions.pdf> (last accessed 4 April 2019).

they obtained.<sup>13</sup> (Other agencies have released purchase records without such redactions.<sup>14</sup>) Some law enforcement agencies have released lists of every time they have used an IMSI Catcher, but redacted certain details surrounding each incidence of use.<sup>15</sup> (Other agencies have released unredacted lists of IMSI Catcher uses.<sup>16</sup>) Law enforcement agencies typically redact personally identifying information about certain individuals named in responsive documents.<sup>17</sup> When presented with public records requests seeking a variety of different types of information, agencies have also responded by releasing some types of records in whole or in part, and withholding other types of records completely.<sup>18</sup>

17. Law enforcement agencies in the United States have released a wide range of records about IMSI Catchers in response to public records requests. Those records include the following types of information:<sup>19</sup>
  - a. Policy Documents: Law enforcement agencies have released internal rules and guidelines governing their use of IMSI Catchers. For example, the U.S. Department of Justice released relevant portions of its Electronic Surveillance Manual.<sup>20</sup> The Sheriff's Office in Erie County, New York, released an internal memorandum setting

---

<sup>13</sup> See Michigan State Police response to Daniel S. Korobkin, ACLU of Michigan (31 Aug. 2015), [https://www.aclu.org/sites/default/files/field\\_document/msp\\_foia\\_appeal\\_response.pdf](https://www.aclu.org/sites/default/files/field_document/msp_foia_appeal_response.pdf) (last accessed 4 April 2019).

<sup>14</sup> *E.g.*, County of Erie, New York, *Purchase Orders*, <https://www.nyclu.org/sites/default/files/Purchase-Orders.pdf> (last accessed 4 April 2019).

<sup>15</sup> *E.g.*, N.Y.P.D., *Over the Air Intercepts 2008-2015*, [https://www.nyclu.org/sites/default/files/summary\\_overtheairintercept\\_web.pdf](https://www.nyclu.org/sites/default/files/summary_overtheairintercept_web.pdf) (available at *Stingrays*, New York Civil Liberties Union, <https://www.nyclu.org/stingrays>) (last accessed 4 April 2019).

<sup>16</sup> See, *e.g.*, Tallahassee Police Dep't, <https://www.aclu.org/files/assets/floridastingray/03.27.2014%20-%20Master%20CE%20Log.pdf> (discussed in Wessler, *ACLU-Obtained Documents Reveal*, *supra* note 9) (last accessed 4 April 2019).

<sup>17</sup> *E.g.*, Milwaukee Police Dep't response to Mike Katz-Lacabe (21 Sept. 2015), <https://assets.documentcloud.org/documents/2696663/Milwaukee-PD-StingRay-Response-21Sep2015.pdf> (last accessed 4 April 2019).

<sup>18</sup> See, *e.g.*, N.Y.C. Police Dep't response to Mariko Hirose, New York Civil Liberties Union (30 Oct. 2015), [https://www.nyclu.org/sites/default/files/20151030\\_FOIL\\_response\\_NYPD\\_stingrays\\_web.pdf](https://www.nyclu.org/sites/default/files/20151030_FOIL_response_NYPD_stingrays_web.pdf) (last accessed 4 April 2019).

<sup>19</sup> The following provides examples of information released in response to FOIA and public records requests about IMSI Catchers, and is not intended to be comprehensive.

<sup>20</sup> See, *e.g.*, Response from U.S. Dep't of Justice to Linda Lye, ACLU of Northern California (22 Aug. 2013), [https://www.aclunc.org/sites/default/files/USA\\_Book\\_Chapter\\_XIV\\_2013.pdf](https://www.aclunc.org/sites/default/files/USA_Book_Chapter_XIV_2013.pdf) (last accessed 4 April 2019).

out its procedures for the use of IMSI Catchers.<sup>21</sup> See Exhibits NW1/3/57 and NW1/4/59-60.

- b. Internal Communications: Law enforcement agencies have released internal emails and other communications detailing discussions of IMSI Catcher practices, including evidence of misconduct such as the withholding of material information from magistrate judges in applications for court orders.<sup>22</sup> See Exhibits NW1/5/62-63 and NW1/6/65-66.
- c. Purchase Records: Numerous law enforcement agencies have released solicitations, invoices, purchase orders, and similar records reflecting the purchase of IMSI Catcher equipment. These records have generally detailed which equipment was purchased and how much it cost.<sup>23</sup> See Exhibits NW1/7/68 and NW1/8/70.
- d. Marketing and Promotional Materials: Law enforcement agencies have released marketing and promotional materials provided to them by companies selling IMSI Catchers, including documents advertising the capabilities of specific IMSI Catcher models.<sup>24</sup> See Exhibit NW1/9/72-75.
- e. Non-Disclosure Agreements: Until relatively recently, state and local law enforcement agencies were required to sign non-disclosure agreements with the

---

<sup>21</sup> Erie Cty. Sheriff's Office, Memorandum re: Cellular Tracking Procedures (11 June 2014), <https://www.nyclu.org/sites/default/files/20140611-2%28b%29-Cellular-Tracking-Procedures.pdf> (last accessed 4 April 2019).

<sup>22</sup> See, e.g., Linda Lye, *Justice Department Emails Show Feds Were Less Than "Explicit" with Judges on Cell Phone Tracking Tool*, ACLU of Northern California (27 Mar. 2013), <https://www.aclunc.org/blog/justice-department-emails-show-feds-were-less-explicit-judges-cell-phone-tracking-tool>; Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU Free Future (19 June 2014), <https://www.aclu.org/blog/national-security/privacy-and-surveillance/internal-police-emails-show-efforts-hide-use-cell> (both last accessed 4 April 2019).

<sup>23</sup> See, e.g., Erie Cty., New York, <https://www.nyclu.org/sites/default/files/Purchase-Orders.pdf>; Florida Dep't of Law Enf't, <https://www.aclu.org/files/assets/floridastingray/03.18.2014%20-%20FDLE%20Stingray%20Records%20Stingray%20Purchase%20Orders.pdf>; Wilmington, North Carolina, exhibited at NW1/7/68; New York State Police, <https://www.nyclu.org/sites/default/files/20141002-NYSPolice-ResponsetoFOIL.pdf> (all last accessed 4 April 2019).

<sup>24</sup> See, e.g., Harris Corp., *Kingfish: Portable, Cellular Transceiver System*, [https://www.nyclu.org/sites/default/files/Kingfish\\_ProductDescription.pdf](https://www.nyclu.org/sites/default/files/Kingfish_ProductDescription.pdf); Harris Corp., *AmberJack: Phased Array Direction Finding Antenna*, [https://www.nyclu.org/sites/default/files/AmberJack\\_ProductDescription.pdf](https://www.nyclu.org/sites/default/files/AmberJack_ProductDescription.pdf). These documents were released by the Rochester Police Department (New York). See <https://www.nyclu.org/stingrays>. (All last accessed 4 April 2019)



Federal Bureau of Investigation before purchasing IMSI Catchers. Many agencies released their copies of the agreements in response to public records requests.<sup>25</sup> See Exhibit NW1/10/77-82. Agencies have also released copies of non-disclosure agreements provided by companies selling IMSI Catcher equipment.<sup>26</sup> See Exhibit NW1/11/84-86.

- f. IMSI Catcher Usage Data: Many law enforcement agencies have released records reflecting the frequency with which they use IMSI Catchers, as well as information about specific investigations in which they deployed the technology. See Exhibit NW1/12/88-94. In Tallahassee, Florida, for example, the police department used IMSI Catchers to track 277 phones over a six-and-a-half-year period.<sup>27</sup> In Tacoma, Washington, it was more than 170 times in five years,<sup>28</sup> and in New York City more than 1,000 times over seven years.<sup>29</sup> The Michigan State Police used IMSI Catchers 128 times in a recent one-year period,<sup>30</sup> and in Kansas City, Missouri, police had used them 97 times as of 2015.<sup>31</sup> The Milwaukee Police Department used IMSI Catchers in 579 investigations over five years,<sup>32</sup> and the Charlotte-

---

<sup>25</sup> See *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, Ctr. for Human Rights and Privacy, <https://web.archive.org/web/20180416162703/http://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/> (last accessed 4 April 2019).

<sup>26</sup> See, e.g., Harris Corp., *Non-Disclosure Agreement (NDA), Harris Corp., CCSD, Wireless Products Grp. (WPG)/Wireless Solutions*, <https://www.aclu.org/files/assets/floridastingray/03.27.2014%20-%20FDLE%20Stingray%20Records%20Non-Disclosure%20Agreement%20with%20Harris%20Corp.pdf> (last accessed 4 April 2019).

<sup>27</sup> Tallahassee Police Dep't, *Log of Use of Cell Site Simulators*, Released Pursuant to ACLU Public Records Request, <https://www.aclu.org/files/assets/floridastingray/03.27.2014%20-%20Master%20CE%20Log.pdf> (last accessed 4 April 2019).

<sup>28</sup> Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, 15 Nov. 2014, <https://www.thenewstribune.com/news/local/crime/article25894096.html> (last accessed 4 April 2019).

<sup>29</sup> Joseph Goldstein, *New York Police Dept. Has Used Cellphone Tracking Devices Since 2008, Civil Liberties Group Says*, N.Y. Times, 11 Feb. 2016, <https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html> (last accessed 4 April 2019).

<sup>30</sup> Joel Kurth, *Michigan State Police Using Cell Snooping Devices*, Detroit News, 23 Oct. 2015, <https://www.detroitnews.com/story/news/local/michigan/2015/10/22/stingray/74438668/> (last accessed 4 April 2019).

<sup>31</sup> Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, Kansas City Star, 5 Sept. 2015, <https://www.kansascity.com/news/business/technology/article34185690.html> (last accessed 4 April 2019).

<sup>32</sup> Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage From Courts and Defense*, ACLU Free Future (25 Jan. 2016), <https://www.aclu.org/blog/privacy->

Mecklenburg Police Department in North Carolina did so more than 500 times over a similar period.<sup>33</sup> The Sacramento Sheriff's Department initially estimated that it used IMSI Catchers in about 500 criminal cases, but later said it could be up to 10,000.<sup>34</sup> The Baltimore Police Department used the devices in approximately 4,300 investigations since 2007,<sup>35</sup> while the Baltimore County Police Department used IMSI Catchers 622 times over five years.<sup>36</sup>

- g. Investigative Files: Several police departments have released records, such as investigative files, from particular investigations where IMSI Catchers were used.<sup>37</sup>
  - h. Sharing Agreements: In some places, law enforcement agencies that do not have their own IMSI Catchers have entered into agreements with other agencies to make use of their equipment. Some of those agreements have been released.<sup>38</sup> See Exhibit NW1/13/96-101.
18. Agencies that do not have relevant records have responded to public records requests by conducting a search and explaining that they lack such records. For example, in 2014 I sent public records requests to three dozen police departments and sheriff's offices across Florida seeking a variety of records about IMSI Catchers. While a number of agencies provided responsive records, 17 police departments and sheriff's offices responded to the request by either explaining that they have not purchased or used IMSI

---

[technology/surveillance-technologies/new-evidence-shows-milwaukee-police-hide-stingray](#) (last accessed 4 April 2019).

<sup>33</sup> Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, 22 Nov. 2014, <https://www.charlotteobserver.com/news/local/crime/article9235652.html> (last accessed 4 April 2019).

<sup>34</sup> *New Developments in Sacramento "Stingray" Case*, ABC 10 (8 Jan. 2016), <https://www.abc10.com/article/news/local/sacramento/new-developments-in-sacramento-stingray-case/24444110> (last accessed 4 April 2019).

<sup>35</sup> Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Baltimore Sun, 9 Apr. 2015, <https://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html> (last accessed 4 April 2019).

<sup>36</sup> Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, Baltimore Sun, 9 Apr. 2015, <https://www.baltimoresun.com/news/maryland/crime/bs-md-co-county-stingray-20150409-story.html> (last accessed 4 April 2019).

<sup>37</sup> See, e.g., Wessler, *ACLU-Obtained Documents Reveal*, *supra* note 9 (discussing records released by Tallahassee Police Department).

<sup>38</sup> See, e.g., Electronic Surveillance Support Team Multi-Agency Voluntary Cooperation Mutual Aid Agreement (Florida), <https://www.aclu.org/files/assets/floridastingray/04.09.2014%20-%20FDLE%20Mutual%20Aid%20Agreement.pdf> (last accessed 4 April 2019).

Catchers, or that they did not have records responsive to the request.<sup>39</sup> Law enforcement agencies in other states and at the federal level have provided similar responses to public records requests when they lacked responsive records.

## **RESULTS OF DISCLOSURES OF INFORMATION ABOUT IMSI CATCHER USE**

19. Courts in the United States have been highly critical of excessive secrecy by law enforcement agencies around IMSI Catchers. As one court explained, refusal of law enforcement agencies to disclose information about their use of IMSI Catchers “*prevents the court from exercising its fundamental duties under the Constitution*” and is “*inimical to the constitutional principles we revere*”.<sup>40</sup> As a judge on the United States Court of Appeals for the Seventh Circuit put it, “[i]t is time for the Stingray to come out of the shadows, so that its use can be subject to the same kind of scrutiny as other mechanisms, such as thermal imaging devices, GPS trackers, pen registers, beepers, and the like”.<sup>41</sup>
20. This skepticism of excessive secrecy has been made clear in public records cases, where state and federal courts have ordered the Government to release IMSI Catcher records.<sup>42</sup> Those cases have held that certain records, including policy documents, purchase records, non-disclosure agreements, and IMSI Catcher use records, must be released because they do not fall within any exemptions to disclosure. In one case, for example, a federal appeals court held that portions of U.S. Department of Justice IMSI Catcher policy documents were not exempt from disclosure because they did not fall within exemptions covering privileged attorney work product or protectable law enforcement records whose disclosure would present a risk of circumvention of the law

---

<sup>39</sup> Wessler, *ACLU-Obtained Documents Reveal*, *supra* note 9.

<sup>40</sup> *State v. Andrews*, 134 A.3d 324, 338–39 (Md. Ct. Spec. App. 2016).

<sup>41</sup> *United States v. Patrick*, 842 F.3d 540, 552 (7th Cir. 2016) (Wood, C.J., dissenting).

<sup>42</sup> See, e.g., *American Civil Liberties Union of Northern California v. U.S. Dep’t of Justice*, 880 F.3d 473 (9th Cir. 2018) [hereinafter *ACLU-NC v. DOJ*] (requiring disclosure of some information about Department of Justice policies for IMSI Catcher use); *Banks v. City of Tacoma*, No. 16-2-05416-7 (Wash. Super. Ct., Pierce Cty. June 25, 2018) (ordering City of Tacoma, Washington, to pay penalty of \$182,340 for withholding records related to IMSI Catchers in violation of the Washington Public Records Act); *Hodai v. City of Tucson*, 365 P.3d 959 (Ariz. Ct. App. 2016) (requiring Tucson Police Department (Arizona) to release certain records relating to IMSI Catchers and permitting it to withhold others); *New York Civil Liberties Union v. Erie Cty. Sheriff’s Off.*, 47 Misc.3d 1201(A), 15 N.Y.S.3d 713, No. 2014/000206 (N.Y. Sup. Ct. Erie Cty. 2015) (requiring Erie County Sheriff’s Office (New York) to release IMSI Catcher purchase orders, communications with IMSI Catcher vendor, IMSI Catcher procedure manual, and IMSI Catcher use reports and logs).

by criminals.<sup>43</sup> As the court explained, because basic facts about IMSI catchers are already known to the public, releasing IMSI Catcher policy documents will provide “*no relevant information that would assist criminals in conforming their behavior to evade detection or circumvent the law*”.<sup>44</sup>

21. In the United States, the release of records about IMSI Catchers by law enforcement agencies in response to public records requests has had the positive effect of enabling public debate about the propriety of using the technology and how to protect against abuses. This debate has prompted all three branches of Government to begin to impose further restrictions on the use of this surveillance technology. In response to public outcry after release of information about the use of IMSI Catchers by police in their states, lawmakers in California, Illinois, Virginia, and Washington State passed laws regulating law enforcement use of IMSI Catchers, including by requiring search warrants and limiting retention of data collected from the phones of innocent bystanders.<sup>45</sup> State and federal courts across the country have issued rulings requiring search warrants and, in some cases, additional protections against unjustified or overly expansive IMSI Catcher use.<sup>46</sup> In some cases, information released in response to public records requests was critical to demonstrating to the court that IMSI Catchers had been used by police.<sup>47</sup> And following public scrutiny of records released under FOIA and inquiries by lawmakers, the U.S. Departments of Justice and Homeland Security issued new policies requiring warrants for use of IMSI Catchers in most circumstances, a departure from

---

<sup>43</sup> *ACLU-NC v. DOJ*, 880 F.3d at 483–92.

<sup>44</sup> *Id.* at 492.

<sup>45</sup> See Cal. Gov’t Code § 53166; 725 Ill. Comp. Stat. 137/5–137/15; Va. Code Ann. § 19.2-70.3(K); Wash. Rev. Code § 9.73.260.

<sup>46</sup> See, e.g., *State v. Sylvestre*, 254 So.3d 986 (Fla. 4th Dist. Ct. App. 2018); *Jones v. United States*, 168 A.3d 703 (D.C. 2017); *United States v. Ellis*, 270 F. Supp. 3d 1134 (N.D. Cal. 2017); *People v. Gordon*, 68 N.Y.S.3d 306 (N.Y. Sup. Ct. Kings Cty. 2017); *State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016); *United States v. Lambis*, 197 F. Supp. 3d 606 (S.D.N.Y. 2016); *In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015).

<sup>47</sup> See *United States v. Patrick*, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting) (“[I]n this case, the government appears to have purposefully concealed the Stingray’s use from the issuing magistrate, the district court, defense counsel, and even this court. It ultimately admitted its use of the device only in response to an amicus curiae brief filed during this appeal”, which relied on records released in response to a public records request.).

previous policy.<sup>48</sup>

22. In addition to contemplating disclosures pursuant to public records laws, a number of jurisdictions in the United States have passed laws requiring police agencies to proactively disclose information about their purchase, use, or intent to acquire surveillance technologies, including IMSI Catchers.<sup>49</sup> These laws typically require publication of an annual report describing how the surveillance technology was used, how much it costs, and other relevant information.<sup>50</sup> In enacting these laws, these jurisdictions have recognized that “*a publicly transparent and accountable process for the procurement and operation of surveillance technology is fundamental to minimizing the risks posed by such technologies*”, including “*risks to civil liberties related to privacy, freedom of speech or association, or disparate impact on groups through over-surveillance*”.<sup>51</sup>
23. In a number of jurisdictions, release of records detailing particular police departments’ use of IMSI Catchers has been critical in spurring public debate and reform efforts. In Charlotte, North Carolina, for example, police were regularly applying for court orders to use IMSI Catchers without mentioning the technology or explaining to judges that it sweeps in data from the phones of both investigative targets and innocent bystanders. Only after the local newspaper obtained and published court records showing this pattern of omissions did a judge learn of the police department’s use of IMSI Catchers and “*reject[] an application from [the police department] to conduct the cellphone*

---

<sup>48</sup> See U.S. Dep’t of Justice, *Dep’t of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (2015), <https://www.justice.gov/opa/file/767321/download>; U.S. Dep’t of Homeland Sec., Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology* (19 Oct. 2015), <https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf> (both last accessed 4 April 2019).

<sup>49</sup> See, e.g., Oakland, Cal., Code Ch. 9.64; Berkeley, Cal., Municipal Code Ch. 2.99; Seattle, Wash., Municipal Code Ch. 14.18.; Yellow Springs, Ohio, Codified Ordinances Ch. 607; Metro Gov’t of Nashville & Davidson County, Tenn., Code of Ordinances § 13.08.080.

<sup>50</sup> See, e.g., *Master List of Surveillance Technologies*, City of Seattle (1 Oct. 2018), <https://www.seattle.gov/Documents/Departments/Tech/2018-09-28%20Revised%20Master%20List%20of%20Surveillance%20Technologies.pdf> (last accessed 4 April 2019).

<sup>51</sup> Seattle, Wash., Ordinance 125376 (2 Aug. 2017), <https://seattle.legistar.com/View.ashx?M=F&ID=5366954&GUID=8D294BC8-F9B7-4EB0-A86B-BF9F6C487558> (last accessed 4 April 2019).

surveillance. It was a first for police".<sup>52</sup> In Illinois, after the Chicago Police Department acknowledged its use of IMSI Catchers in response to a public records request, calls for regulation led the state legislature to enact a law requiring search warrants and other protections before police are permitted to use the devices.<sup>53</sup> In Baltimore, release of records about use of IMSI Catchers by local police led to the filing of a complaint with the Federal Communications Commission alleging that the police department's use of the technology is illegal and disparately impacts communities of color.<sup>54</sup> In Alameda County, California, after the District Attorney's Office released records showing that it had secured grant funding to purchase an IMSI Catcher, public pressure led the Alameda County Board of Supervisors to enact a privacy policy limiting the technology's use in order to prevent abuses.<sup>55</sup>

24. Across the country, members of the public have been able to learn about use of IMSI Catchers in their communities through numerous news reports in local and national press outlets, and have weighed in on issues raised by IMSI Catcher use at public hearings of legislative and oversight bodies,<sup>56</sup> on the opinion pages of newspapers,<sup>57</sup> by

---

<sup>52</sup> Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, *supra* note 33.

<sup>53</sup> See John Dodge, *After Denials, Chicago Police Department Admits Purchase of Cell-Phone Spying Devices*, CBS Chicago (1 Oct. 2014), <https://chicago.cbslocal.com/2014/10/01/chicago-police-department-admits-purchase-of-cell-phone-spying-devices/>; Khadine Bennett & Edwin C. Yohnka, *Commentary, It's Time to Restrict Police Cellphone (Listening) Privileges*, Chicago Tribune, 16 Feb. 2016, <https://www.chicagotribune.com/news/opinion/commentary/ct-stingray-cellphone-surveillance-police-privacy-perspec-0217-jm-20160216-story.html>; *Rauner OKs Regulating Police Use of Cellphone Data Tracking*, Chicago Tribune, 22 July 2016, <https://www.chicagotribune.com/news/local/politics/ct-bruce-rauner-cellphone-tracking-stingray-20160722-story.html> (all last accessed 4 April 2019).

<sup>54</sup> See Nathan Freed Wessler, *FCC Needs to Impose Strong Protections Around Stingray Use*, ACLU Free Future (1 Sept. 2016), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fcc-needs-impose-strong-protections-around> (last accessed 4 April 2019).

<sup>55</sup> Linda Lye, *Breaking: Documents Reveal Unregulated Use of Stingrays in California*, ACLU of Northern California (14 Mar. 2014), <https://www.aclunc.org/blog/breaking-documents-reveal-unregulated-use-stingrays-california>; *Alameda County Limits Cell Phone Surveillance Tool*, Mercury News, 19 Nov. 2015, <https://www.mercurynews.com/2015/11/19/alameda-county-limits-cell-phone-surveillance-tool/> (both last accessed 4 April 2019).

<sup>56</sup> See, e.g., Darwin BondGraham, *Oakland Privacy Commission Holds Hearing on 'Stingray' Cell Phone Surveillance Devices*, East Bay Express, 12 Aug. 2016, <https://www.eastbayexpress.com/SevenDays/archives/2016/08/12/oakland-privacy-commission-holds-hearing-on-stingray-cell-phone-surveillance-devices>; *Hearing of Judiciary Comm. of Nebraska Legislature Regarding LB738* (21 Jan. 2016), <https://nebraskalegislature.gov/FloorDocs/104/PDF/Transcripts/Judiciary/2016-01-21.pdf> (both last accessed 4 April 2019).

signing petitions,<sup>58</sup> and by engaging policymakers in other ways.

25. In my experience, law enforcement agencies are easily able to respond to public records requests seeking information about IMSI Catchers by acknowledging whether they have relevant records, and by releasing certain records to the public. This level of transparency is completely consistent with the ability of law enforcement agencies to do their jobs. Moreover, it enables public debate and allows lawmakers, courts, and other oversight bodies to obtain the information necessary for crafting reasonable rules governing IMSI Catcher use, thereby protecting against unjustified invasions of privacy and other abuses.

### Statement of Truth

**I believe that the facts stated in this witness statement are true.**

[REDACTED]

Nathan Freed Wessler

Dated this 5<sup>th</sup> day of April 2019

---

<sup>57</sup> See, e.g., Matthew Feeney, Op-Ed, *When It Comes to Surveillance, Watch the Watchmen*, N.Y. Times, 23 Oct. 2017, <https://www.nytimes.com/2017/10/23/opinion/police-surveillance.html> (last accessed 4 April 2019).

<sup>58</sup> See, e.g., *Tell the FCC: No More Police Stingray Surveillance*, colorofchange.org, <https://act.colorofchange.org/sign/end-cell-phone-surveillance/> (last accessed 4 April 2019).

# EXHIBIT NW1/1

Article by Nathan Freed Wessler, *“[We] can neither confirm nor deny the existence or nonexistence of records responsive to your request”: reforming the Glomar response under FOIA*”, New York University School of Law, 2010.



# “[WE] CAN NEITHER CONFIRM NOR DENY THE EXISTENCE OR NONEXISTENCE OF RECORDS RESPONSIVE TO YOUR REQUEST”<sup>1</sup>: REFORMING THE GLOMAR RESPONSE UNDER FOIA

NATHAN FREED WESSLER\*

*Under normal Freedom of Information Act procedures, an individual submits a request for records to a government agency and receives one of three responses: The agency may identify responsive records and release them, determine that there are no responsive records and inform the requestor of this fact, or identify responsive records but determine that they are exempt from disclosure under one of FOIA’s nine statutory exemptions. Since the 1970s, however, a fourth type of response has arisen: Agencies sometimes refuse to confirm or deny whether responsive records do or do not exist on the grounds that acknowledging their very existence itself would reveal secret information. This withholding mechanism, known as the Glomar response, creates special problems for FOIA requestors and receives remarkable deference from federal courts. This Note assesses the justifications for such deference, which are often rooted in separation of powers concerns. Arguing that the level of deference afforded is excessive, this Note posits that both separation of powers and institutional conflict of interest considerations support greater judicial scrutiny of agency invocations of the Glomar response. This Note concludes by offering proposals for judicial, legislative, and administrative reform of the Glomar response.*

## INTRODUCTION

The Freedom of Information Act (FOIA),<sup>2</sup> now in its fifth decade, remains a remarkable, if troubled, tool for government transparency and accountability. FOIA has unquestionably opened government functions and activities to public scrutiny. Federal agencies

---

<sup>1</sup> Letter from Delores M. Nelson, Info. & Privacy Coordinator, Cent. Intelligence Agency, to Melissa Goodman, Staff Attorney, Nat’l Sec. Project, ACLU (May 13, 2009), available at [http://www.aclu.org/pdfs/natsec/CIA\\_05132009.pdf](http://www.aclu.org/pdfs/natsec/CIA_05132009.pdf).

\* Copyright © 2010 by Nathan Freed Wessler. J.D., 2010, New York University School of Law; B.A., 2004, Swarthmore College. Thanks first to Tess Bridgeman, editor extraordinaire, who strengthened this piece immeasurably through her thoughtful comments. Thanks also to Jason Liu, Kristen Richer, Beth George, Kirstin O’Connor, and the editorial staff of the *New York University Law Review*. I am also indebted to Professor Samuel Rascoff for his helpful suggestions and to Melissa Goodman, Ben Wizner, and Amna Akbar for their expert guidance on issues surrounding the Freedom of Information Act.

<sup>2</sup> 5 U.S.C. § 552 (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, further amended by OPEN FOIA Act of 2009, Pub. L. No. 11-83, 123 Stat. 2142, 2184.

process hundreds of thousands of FOIA requests each year, often releasing information about government programs that were previously shrouded in secrecy.<sup>3</sup> Indeed, President Obama used the occasion of his first day in office to issue a memorandum to executive branch officials setting out his interpretation of the scope and import of FOIA, declaring that “[i]n our democracy, the Freedom of Information Act . . . , which encourages accountability through transparency, is the most prominent expression of a profound national commitment to ensuring an open Government.”<sup>4</sup> But despite the trumpeted successes and unmistakable import of FOIA, the law and its enforcement suffer pathologies that undermine the Act’s effectiveness. This Note examines the most vexing of these, the “Glomar response,” and assesses issues raised by extreme judicial deference to agencies’ use of that response in cases involving withholding of national security information.

Under normal FOIA procedures, an individual submits a request for records to a government agency and receives one of three responses: The agency may identify responsive records and release them, determine that there are no responsive records and inform the requestor of this fact, or identify responsive records but determine that they are exempt from disclosure under one of FOIA’s nine statutory exemptions.<sup>5</sup> Since the 1970s, however, a fourth type of response has arisen: Agencies sometimes refuse to confirm or deny whether responsive records do or do not exist on the grounds that acknowledging their very existence would itself reveal secret information. This withholding mechanism, known as the Glomar response,<sup>6</sup> has been recognized by every federal circuit court to consider it but is not a part of the FOIA statute.<sup>7</sup>

The Glomar response creates particularly difficult problems for litigants in FOIA suits because, by both depriving them of information essential to litigation and hobbling judicial review, it severely limits litigants’ ability to contest agencies’ withholding of records. The response also facilitates excessive secrecy. To be effective, the Glomar response must be invoked both when the government has responsive

---

<sup>3</sup> See *Advancing Freedom of Information in the New Era of Responsibility: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 7 (2009) (statement of Miriam Nisbet, Director, Office of Government Information Services) (“[T]he government receives over 600,000 FOIA requests per year . . .”).

<sup>4</sup> Freedom of Information Act: Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4683 (Jan. 21, 2009).

<sup>5</sup> See *infra* notes 17–26 and accompanying text (describing FOIA procedures and exemptions).

<sup>6</sup> See *infra* Part II.A (describing origins of Glomar response and explaining its name).

<sup>7</sup> See *infra* note 62 (citing circuit decisions authorizing Glomar response).

October 2010]

REFORMING THE GLOMAR RESPONSE

1383

records and when it does not.<sup>8</sup> In practice, however, this undermines the government's credibility and the public's trust in legitimate secrecy. The Glomar response may sometimes be necessary to protect the government's deepest national security secrets, and this Note does not argue that it should be totally barred.<sup>9</sup> Nevertheless, overuse hinders FOIA requestors and undermines FOIA itself. Acknowledging that use of the Glomar response is sometimes justified raises difficult questions of accurately delineating legitimate from illegitimate uses. This Note posits that such distinctions can be made and offers suggestions for drawing principled lines.

Judges routinely defer to agency use of the Glomar response. This hesitance to engage in robust scrutiny of Glomar denials has been justified on both constitutional and prudential separation of powers grounds: Courts opine that protection of national security information is entrusted to the executive under Article II of the Constitution and that courts lack the competence to assess executive determinations to withhold national security information.<sup>10</sup> This Note argues that Congress and the courts do in fact have constitutional power to regulate and review use of the Glomar response. Further, they should exercise that power because concerns about comparative competence are overblown and are outweighed by the institutional conflict of interest that arises when the executive branch makes essentially unreviewed decisions to withhold its own records from disclosure.

Although there is an expansive literature on FOIA and government secrecy more broadly, very little has been written about the Glomar response. This Note is the first scholarship since the 1990s devoted to analyzing the Glomar response and the first piece ever to offer a systematic account of the response in the national security realm.<sup>11</sup> Part I describes the structure and function of FOIA. Part II examines the origin of the Glomar response and its current use. Part III analyzes the difficulties posed by judicial deference to the executive's invocation of the Glomar response in cases involving national security-related information. Part IV explores the separation of powers rationales used to support such deference and balances them

---

<sup>8</sup> See *infra* notes 93–95 and accompanying text.

<sup>9</sup> See *infra* note 86 (noting agreement of commentators on this point).

<sup>10</sup> See *infra* notes 137–40 and accompanying text (discussing prudential separation of powers in national security context).

<sup>11</sup> Two articles about the Glomar response were published in the 1990s: Danae J. Aitchison, *Reining in the Glomar Response: Reducing CIA Abuse of the Freedom of Information Act*, 27 U.C. DAVIS L. REV. 219 (1993); John Y. Gotanda, *Glomar Denials Under FOIA: A Problematic Privilege and a Proposed Alternative Procedure of Review*, 56 U. PITT. L. REV. 165 (1994). Several other authors have offered brief discussions about Glomar in articles addressing other problems under FOIA. See sources cited *infra* note 33.

against concerns with institutional conflicts of interest raised when courts allow agencies to decide to withhold their own records under Glomar. It then offers proposals for judicial, administrative, and congressional reform of the response.

## I

### THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act,<sup>12</sup> originally enacted in 1966,<sup>13</sup> marked a watershed change in citizen access to government records. FOIA provided, for the first time, a mandatory and judicially enforceable requirement that government agencies release records to members of the public upon request.<sup>14</sup> The Supreme Court has repeatedly recognized FOIA as a key tool of democratic accountability,<sup>15</sup> and scholarly commentary consistently hails FOIA as a landmark statute and a powerful instrument of open government.<sup>16</sup>

Under FOIA, any person may submit a request to a federal agency for records.<sup>17</sup> The agency is then required to make a prompt search for those records, and to release them to the requestor<sup>18</sup> unless they fall within one of nine statutory exemptions.<sup>19</sup> Where only a portion of a record is exempt from disclosure, the agency must release all

---

<sup>12</sup> 5 U.S.C. § 552 (2006).

<sup>13</sup> See Pub. L. No. 89-487, 80 Stat. 250, 250–51 (1966) (amending Administrative Procedure Act § 3, 60 Stat. 238 (1946), 5 U.S.C. § 1002 (1964)); Pub. L. No. 89-554, § 552, 80 Stat. 378, 383 (1966) (codified as amended at 5 U.S.C. § 552 (2006)).

<sup>14</sup> Martin E. Halstuk, *When Secrecy Trumps Transparency: Why the OPEN Government Act of 2007 Falls Short*, 16 *COMMLAW CONSPICUOUS* 427, 430 (2008).

<sup>15</sup> *Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 171–72 (2004); *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

<sup>16</sup> See, e.g., HERBERT N. FOERSTEL, *FREEDOM OF INFORMATION AND THE RIGHT TO KNOW: THE ORIGINS AND APPLICATIONS OF THE FREEDOM OF INFORMATION ACT* 44 (1999) (“Despite its many inadequacies, America’s FOIA is recognized worldwide as trailblazing legislation.”); Halstuk, *supra* note 14, at 431 (“[P]reserving and fostering democratic principles lays at the heart of [FOIA].”); David E. Pozen, *Deep Secrecy*, 62 *STAN. L. REV.* 257, 314 (2010) (“[FOIA’s] enactment entrenched a dramatic normative shift in Americans’ expectations of government. . . . FOIA [is] the closest thing we have to a constitutional amendment on state secrecy.”).

<sup>17</sup> 5 U.S.C. § 552(a)(3)(A) (2006).

<sup>18</sup> *Id.*; *id.* § 552(a)(6)(A)(i).

<sup>19</sup> *Id.* § 552(b). The exemptions cover classified national security information, *id.* § 552(b)(1), records “specifically exempted from disclosure by [another] statute,” *id.* § 552(b)(3), certain internal agency records, *id.* § 552(b)(2), (5), records whose disclosure would “constitute a clearly unwarranted invasion of personal privacy,” *id.* § 552(b)(6), (7)(C), certain records compiled for law enforcement purposes, *id.* § 552(b)(7), and several other narrow categories of information. Exemptions are typically referred to by the number of their subsection. Thus, for example, the exemption for classified information contained in § 552(b)(1) is known as “Exemption 1.”

October 2010]

REFORMING THE GLOMAR RESPONSE

1385

nonexempt information that is “reasonably segregable” from the exempt material.<sup>20</sup>

If an agency denies a FOIA request (either by determining that records are exempt from disclosure or for another reason such as the nonexistence of responsive records), the requestor may file an administrative appeal within the agency.<sup>21</sup> If the agency upholds the denial on appeal, the requestor has a right to bring suit in federal district court.<sup>22</sup> The court reviews the agency decision *de novo* and may examine withheld records *in camera* to assess whether nondisclosure is justified.<sup>23</sup> In litigation, the defendant agency is typically required to provide the plaintiff/requestor with a detailed affidavit, known as a *Vaughn* index, describing the contents of each withheld document and explaining the statutory justification for its exemption.<sup>24</sup> The *Vaughn* index serves to provide the plaintiff with enough information to contest the agency’s basis for withholding<sup>25</sup> and allows the agency to carry its burden of proof.<sup>26</sup>

The statutory requirement of *de novo* review means that courts are tasked with evaluating, based on their own assessment of the record, whether the agency properly applied the FOIA exemptions.<sup>27</sup> Yet this apparent lack of deference is misleading because, in practice, courts regularly defer to agency determinations under FOIA regardless of the nature of the request or the agency’s justification for rejecting it.<sup>28</sup> Such deference is particularly strong in cases where

---

<sup>20</sup> *Id.* § 552(b).

<sup>21</sup> *Id.* § 552(a)(6)(A).

<sup>22</sup> *Id.* § 552(a)(4)(B).

<sup>23</sup> *Id.* District courts rarely exercise their power to order *in camera* review. Gotanda, *supra* note 11, at 173 & n.55.

<sup>24</sup> *See Vaughn v. Rosen*, 484 F.2d 820, 826–28 (D.C. Cir. 1973) (setting out index procedures).

<sup>25</sup> *Id.* at 823, 826. *Vaughn* indices typically include brief substantive descriptions of the contents of each withheld document. For example, the index provided by the government in response to a recent FOIA suit brought by the ACLU describes one withheld document as “an eighteen-page memo, dated August 1, 2002, discussing the legality of the CIA’s proposed interrogation of Abu Zubaydah, with handwritten attorney markings.” Response to FOIA/PA Request No. F-2004-01456 at 1, *ACLU v. Dep’t of Def.*, No. 4 Civ. 1782 (S.D.N.Y. 2009), available at [http://www.aclu.org/files/assets/20091113\\_OLC-CIA\\_II\\_Vaughn\\_Index\\_Part\\_1.pdf](http://www.aclu.org/files/assets/20091113_OLC-CIA_II_Vaughn_Index_Part_1.pdf). *Vaughn* indices also explain the legal bases for withholding all or part of a document, with references to the specific FOIA exemptions relied on. *E.g.*, *id.* at 1–2.

<sup>26</sup> *Dep’t of State v. Ray*, 502 U.S. 164, 173 (1991).

<sup>27</sup> *Dep’t of the Air Force v. Rose*, 425 U.S. 352, 379 (1976).

<sup>28</sup> Nathan Slegers, Comment, *De Novo Review Under the Freedom of Information Act: The Case Against Judicial Deference to Agency Decisions To Withhold Information*, 43 SAN DIEGO L. REV. 209, 212 (2006); *see also* Paul R. Verkuil, *An Outcomes Analysis of Scope of Review Standards*, 44 WM. & MARY L. REV. 679, 713 (2002) (finding that, over ten-year

agencies have withheld records based on national security concerns.<sup>29</sup> In such cases, courts “must accord substantial weight to the Agency’s determinations.”<sup>30</sup> When reviewing FOIA requests for classified material, courts demand only that the government “articulate a logical basis for classification” in submissions to the court instead of subjecting withheld documents to actual scrutiny.<sup>31</sup>

## II

### THE GLOMAR RESPONSE

#### A. *The Origin of the Glomar Response*

Normally, an agency will respond to a FOIA request by acknowledging whether responsive records do or do not exist and then either releasing those records or explaining that they are exempt from disclosure. Since the 1970s, however, agencies have sometimes offered a fourth, nonstatutory response: Under certain circumstances, agencies refuse to confirm or deny whether or not responsive records exist.<sup>32</sup> This evasive reply, known as the Glomar response, creates special problems for FOIA requestors but has received surprisingly little attention in the FOIA literature.<sup>33</sup>

The Glomar response was first judicially recognized in two parallel FOIA cases in the D.C. Circuit, *Phillippi v. CIA*,<sup>34</sup> and *Military Audit Project v. Casey*,<sup>35</sup> both involving requests for information about a secret Central Intelligence Agency (CIA) program to raise a

---

period, district courts reversed just ten percent of FOIA cases and concluding that this reversal rate is lower than should be expected under de novo review standard).

<sup>29</sup> Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation over National Security Information Under the Freedom of Information Act*, 37 VILL. L. REV. 67, 67, 90 (1992); Adam M. Samaha, *Government Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. REV. 909, 973 (2006).

<sup>30</sup> *Gardels v. CIA*, 689 F.2d 1100, 1104 (D.C. Cir. 1982) (internal quotation marks omitted) (citing *Ray v. Turner*, 587 F.2d 1187, 1194 (D.C. Cir. 1978)); see also *CIA v. Sims*, 471 U.S. 159, 176 (1985) (exhibiting such deference).

<sup>31</sup> Samaha, *supra* note 29, at 939.

<sup>32</sup> See *Phillippi v. CIA (Phillippi I)*, 546 F.2d 1009, 1012 (D.C. Cir. 1976) (providing first judicial recognition of Glomar response).

<sup>33</sup> Only two articles out of the voluminous literature on FOIA have been devoted to discussing the Glomar response. See generally Aitchison, *supra* note 11 (discussing use of Glomar response by CIA under national security exemptions); Gotanda, *supra* note 11 (discussing use of Glomar response under privacy exemptions). Several other pieces provide brief discussions of Glomar. See, e.g., Karen A. Winchester & James W. Zirkle, *Freedom of Information and the CIA Information Act*, 21 U. RICH. L. REV. 231, 248–50 (1987) (describing Glomar response as used by CIA); Gregory G. Brooker, Note, *FOIA Exemption 3 and the CIA: An Approach To End the Confusion and Controversy*, 68 MINN. L. REV. 1231, 1252–61 (1984) (discussing use of Glomar response by CIA in Exemption 3 cases).

<sup>34</sup> *Phillippi I*, 546 F.2d at 1009.

<sup>35</sup> 656 F.2d 724 (D.C. Cir. 1981).

October 2010]

REFORMING THE GLOMAR RESPONSE

1387

sunken Soviet submarine using a privately registered salvage ship named the Hughes Glomar Explorer. The Los Angeles Times partially broke the story about the program in February 1975,<sup>36</sup> prompting the CIA to attempt to suppress further reports.<sup>37</sup> CIA officials convinced news outlets to refrain from further reporting on the subject for more than a month, but eventually the major news organizations ran stories both about the details of the Glomar Explorer project and about the CIA's efforts to bury the story.<sup>38</sup>

After news broke about the government's attempts to suppress the Glomar Explorer story, Harriet Ann Phillippi, a journalist, filed a FOIA request with the CIA seeking "all records relating to the [CIA's] attempts to persuade any media personnel not to . . . make public the events relating to the activities of the *Glomar Explorer*."<sup>39</sup> Instead of responding to Phillippi's request with the usual acknowledgement that responsive records existed but were exempt from release, the Agency issued a novel response: It stated that "the fact of the existence or nonexistence of the records you request" was itself exempt from disclosure as a classified matter of national security.<sup>40</sup>

Around the same time as Phillippi, plaintiffs in *Military Audit Project* submitted FOIA requests to the CIA and Department of Defense seeking records describing the U.S. government's role in the "planning, design, construction, leasing, use and disposition of the Glomar Explorer."<sup>41</sup> Both agencies responded by refusing to confirm or deny the existence of such records.<sup>42</sup> The requestors in *Phillippi* and *Military Audit Project* independently filed suit to compel the government to reveal whether or not it possessed responsive records and, if so, to release them.

Phillippi's request was the first to reach decision on appeal. The CIA claimed that the very fact of whether or not it had records responsive to Phillippi's request was exempt from disclosure under Exemptions 1 and 3.<sup>43</sup> The court held that the agency's refusal to confirm or deny the existence of requested documents was permissible under FOIA but reversed and remanded because the district court

---

<sup>36</sup> See William Farr & Jerry Cohen, *CIA Reportedly Contracted with Hughes in Effort To Raise Sunken Soviet A-Sub*, L.A. TIMES, Feb. 8, 1975, at 18.

<sup>37</sup> *Military Audit Project*, 656 F.2d at 729; see also Seymour Hersh, *C.I.A. Salvage Ship Brought Up Part of Soviet Sub Lost in 1968, Failed To Raise Atom Missiles*, N.Y. TIMES, Mar. 19, 1975, at 52.

<sup>38</sup> *Military Audit Project*, 656 F.2d at 729.

<sup>39</sup> *Phillippi I*, 546 F.2d at 1011 n.1.

<sup>40</sup> *Id.* at 1011–12.

<sup>41</sup> *Military Audit Project*, 656 F.2d at 729.

<sup>42</sup> *Id.* at 729–30.

<sup>43</sup> *Phillippi I*, 546 F.2d at 1012.

had based its ruling solely on in camera affidavits submitted by the CIA without attempting to compile a public record.<sup>44</sup> In approving the Glomar response, the court explained its reasoning as follows: “In effect, the situation is as if appellant had requested and been refused permission to see a document which says either ‘Yes, we have records related to contacts with the media concerning the *Glomar Explorer*’ or ‘No, we do not have any such records.’”<sup>45</sup> In such cases, where disclosure of that hypothetical document would itself compromise national security, the government could “claim that national security considerations require it to refuse to disclose whether or not requested documents exist.”<sup>46</sup>

*Phillippi I* thus opened the doors to a new government response to FOIA requests, one neither described in the statute nor contemplated by Congress when it passed the Act. Ironically, soon after the decision in *Phillippi I*, the government abandoned its Glomar response and acknowledged that it possessed records relating to the Glomar Explorer.<sup>47</sup> Still, it was not until nearly thirty-five years later that the CIA would actually begin releasing records about the Glomar Explorer project, and even then significant details continued to be withheld.<sup>48</sup>

---

<sup>44</sup> *Id.* at 1012–15 & n.14. The court noted that in some cases the subject matter of a FOIA request could be so sensitive as to require “examin[ation of] classified affidavits *in camera* and without participation by plaintiff’s counsel.” *Id.* at 1013. Before resorting to that procedure, however, trial courts must “attempt to create as complete a public record as possible” by requiring an agency “to provide a public affidavit.” *Id.*

<sup>45</sup> *Id.* at 1012.

<sup>46</sup> *Id.* This point was uncontested by *Phillippi I*. *Id.*

<sup>47</sup> *Phillippi v. CIA (Phillippi II)*, 655 F.2d 1325, 1328 (D.C. Cir. 1976). Even before this decision, the government’s argument in *Phillippi I* was complicated by the fact that it had disclosed its connection with the Glomar Explorer in a tax case in Los Angeles. *Phillippi I*, 546 F.2d at 1014 n.9. Although the Glomar response is widely accepted by courts today, its initial use was controversial. Indeed, the CIA’s use of the Glomar response in *Military Audit Project* raised the ire of the district court judge, who removed himself from further proceedings in the case in protest. After the CIA finally admitted to involvement with the Glomar Explorer in mid-1977, the judge called the CIA’s initial use of the Glomar response “just a game that was played over a period of a year in front of me” and decried the Agency’s refusals to confirm to the court that it held responsive records—later revealed to include more than 128,000 documents—as “irresponsible” and “outrageous.” Timothy S. Robinson, ‘Compromised,’ *Judge Gesell Quits CIA Case*, WASH. POST, July 1, 1977, at A13.

<sup>48</sup> Calvin Woodward, *Gone Fishing: Secret Hunt for a Sunken Soviet Sub*, ASSOCIATED PRESS, Feb. 13, 2010, available at <http://abcnews.go.com/Politics/wireStory?id=9827998>. Although the official government account of the Glomar Explorer project was recently partially declassified in PROJECT AZORIAN: THE STORY OF THE HUGHES GLOMAR EXPLORER (2010), available at <http://www.gwu.edu/~nsarchiv/nukevault/ebb305/doc01.pdf>, significant portions of the account remain redacted. See, e.g., *id.* at 6–9.



October 2010]

REFORMING THE GLOMAR RESPONSE

1389

### B. How the Glomar Response Works

The principle behind the Glomar response is that revealing the very fact of whether or not the government possesses records about a topic can sometimes reveal protected information, even if the underlying records would themselves be safe from disclosure under FOIA's exemptions. The Glomar response does not function independently of the FOIA statute, however: "[I]n order to invoke the *Glomar* response . . . , an agency must tether its refusal to one of the nine FOIA exemptions."<sup>49</sup> Since *Phillippi I*, the Glomar response has been accepted by courts in connection with three distinct types of disclosure concerns: those relating to national security (justified by Exemptions 1 and 3), those that would result in an "unwarranted invasion of personal privacy" (pursuant to Exemptions 6 and 7(C)),<sup>50</sup> and those entailing the protection of the identities of confidential informants to federal law enforcement agencies (under § 552(c)(2)).<sup>51</sup> Although important in their own right, this Note does not analyze the latter two uses of the Glomar response.

In national security FOIA cases, the government's claim is that revealing whether or not responsive records exist would itself damage national security. Take, for example, a FOIA request submitted to the CIA seeking information about covert and unacknowledged CIA actions in a Latin American country, including interference with political and military leadership there.<sup>52</sup> The government might issue a Glomar response on the grounds that acknowledging whether such records exist would necessarily disclose classified national security

---

<sup>49</sup> *Wilner v. NSA*, 592 F.3d 60, 71 (2d Cir. 2009) (internal quotation marks and citation omitted); *accord Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007).

<sup>50</sup> Gotanda, *supra* note 11, at 176. In the privacy context, the concern is that the government would infringe upon an individual's privacy interest by acknowledging that the government has records about him or her, as when a request is made to the FBI for investigative records about an individual. Because it is presumed that an agency like the FBI would hold certain types of records about an individual only if he or she had been under investigation, acknowledging whether records exist would compromise the individual's privacy interest by "carry[ing] a stigmatizing connotation." Office of Info. Policy, U.S. Dep't of Justice, *OIP Guidance: The Bifurcation Requirement for Privacy "Glomarization,"* 17 FOIA UPDATE 3, 3 (1996) [hereinafter *Bifurcation Requirement*], available at [http://www.usdoj.gov/oip/foia\\_updates/Vol\\_XVII\\_2/page3.html](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_2/page3.html) (quoting Office of Info Policy, U.S. Dep't of Justice, *OIP Guidance: Privacy "Glomarization,"* 7 FOIA UPDATE 3, 3 (1986)).

<sup>51</sup> Subsection (c)(2) of FOIA provides that requests for certain records that would reveal the identity of confidential informants to federal law enforcement agencies may be treated as not subject to disclosure. 5 U.S.C. § 552(c)(2) (2006). This provision has been interpreted as "provid[ing] express legislative authorization for a Glomar response" in a narrow set of circumstances. *Benavides v. DEA*, 968 F.2d 1243, 1246 (D.C. Cir. 1992).

<sup>52</sup> See *Riquelme v. CIA*, 453 F. Supp. 2d 103, 105–06 (D.D.C. 2006) (turning on these facts).

information by indicating whether the CIA had in fact engaged in the alleged covert activities, since the agency would only possess records if it had a role in the activities in question.<sup>53</sup>

Two FOIA exemptions are used to protect national security information—Exemptions 1 and 3. Exemption 1 shields from disclosure records that are properly classified under the executive order governing classification of national security information.<sup>54</sup> The executive order specifically allows the Glomar response, stating that in response to a FOIA request “[a]n agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified . . . .”<sup>55</sup> Courts consistently allow invocation of the Glomar response under Exemption 1.<sup>56</sup>

Exemption 3 provides that an agency may withhold records that are “specifically exempted from disclosure by [another] statute.”<sup>57</sup> Dozens of federal statutes have been recognized by courts as providing grounds for exempting records from disclosure under this provision.<sup>58</sup> In the national security context, most intelligence agencies

---

<sup>53</sup> *Id.* at 109.

<sup>54</sup> 5 U.S.C. § 552(b)(1) (2006). Under the executive order currently in effect, classification of information is called for when “unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security . . . , and [the information] pertains to” military matters; intelligence activities, sources, or methods; foreign relations; and other described categories of information. Exec. Order No. 13,526 § 1.4, 75 Fed. Reg. 707, 709 (Dec. 29, 2009), *reprinted in* 50 U.S.C.A. § 435 note (West 2010).

<sup>55</sup> Exec. Order No. 13,526 § 3.6(a), 75 Fed. Reg. at 719. President Carter issued the first executive order on classification of national security information to recognize the Glomar response. *See* Exec. Order No. 12,065 § 3-505, 3 C.F.R. 190, 199 (1979) (“No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act . . . refuse to confirm the existence or non-existence of a document unless the fact of its existence or non-existence would itself be classifiable under this Order.”). Each subsequent president to issue a classification order has included similar language in his order. *See* Exec. Order No. 12,356 § 3.4(f)(1), 3 C.F.R. 166, 174 (1983) (President Reagan); Exec. Order No. 12,958 § 3.7(a), 3 C.F.R. 333, 347 (1996), *reprinted as amended in* 50 U.S.C. § 435 note (Supp. III 2003) (President Clinton); Exec. Order No. 13,292 § 3.6(a), 3 C.F.R. 196, 207 (2004) (President George W. Bush) (amending Exec. Order No. 12,958).

<sup>56</sup> *See, e.g.,* Wilner v. NSA, 592 F.3d 60, 71 (2d Cir. 2009); Miller v. Casey, 730 F.2d 773, 777 (D.C. Cir. 1984).

<sup>57</sup> 5 U.S.C. § 552(b)(3) (2006). Exemption 3 is triggered by statutes that either “(A) require[ ] that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establish[ ] particular criteria for withholding or refer[ ] to particular types of matters to be withheld.” *Id.* § 552(b)(3). Any withholding statute enacted “after the date of enactment of the OPEN FOIA Act of 2009” must “specifically cite[ ] to this paragraph” to trigger Exemption 3. *Id.* § 552(b)(3)(B) (Supp. III 2009).

<sup>58</sup> *See* OFFICE OF INFO. POLICY, U.S. DEP’T OF JUSTICE, STATUTES FOUND TO QUALIFY UNDER EXEMPTION 3 OF THE FOIA (2010), *available at* <http://www.justice.gov/oip/exemption3-april-2010.pdf> (listing statutes that courts have found to satisfy requirements of Exemption 3).

October 2010]

REFORMING THE GLOMAR RESPONSE

1391

are covered by nondisclosure statutes. Records held by the CIA relating to “intelligence sources and methods,” for example, are exempt from disclosure under § 102(d)(3) of the National Security Act of 1947.<sup>59</sup> Information regarding the functions or activities of the National Security Agency is similarly exempt from disclosure under § 6 of the National Security Act of 1959.<sup>60</sup> In Glomar cases, courts ask whether “acknowledging the existence or nonexistence of the information entailed in [the] FOIA [r]equest would reveal” information protected by the relevant withholding statute, such as intelligence sources and methods in the case of the CIA or the organization, functions, and activities of the National Security Agency (NSA).<sup>61</sup> If the fact of existence or nonexistence of records can be construed as within the ambit of the withholding statute, the agency’s Glomar response is deemed valid.

The Glomar response for national security information has been approved by every circuit to consider the issue (in cases involving either or both of the national security exemptions).<sup>62</sup> Congress has never amended FOIA to include express authorization for Glomar.<sup>63</sup>

### C. *Glomar Procedures in Practice*

FOIA cases are marked by asymmetrical access to information between the requesting party and the responding agency.<sup>64</sup> When the agency claims that records are exempt from disclosure under § 552(b),

---

<sup>59</sup> Pub. L. No. 108-458, 118 Stat. 3643 (2004) (codified at 50 U.S.C. § 403-1(i) (2006)); see also *CIA v. Sims*, 471 U.S. 159, 167 (1985) (holding that section 102(d)(3) of National Security Act “qualifies as a withholding statute under Exemption 3”). The CIA’s “operational files” are also exempt from disclosure pursuant to Pub. L. No. 98-477, 98 Stat. 2209 (1984) (codified at 50 U.S.C. § 431(a) (2006)).

<sup>60</sup> Pub. L. No. 86-36, § 6, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 (2006)); see also *Founding Church of Scientology v. NSA*, 610 F.2d 824, 827–28 (D.C. Cir. 1979) (holding that section 6 of National Security Act qualifies as withholding statute under FOIA Exemption 3).

<sup>61</sup> *Wilner*, 592 F.3d at 72.

<sup>62</sup> See *Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004) (“Every appellate court to address the issue has held that the FOIA permits the CIA to make a ‘Glomar response’ . . .”). For illustrative decisions, see *Wilner*, 592 F.3d at 68, *Larson v. Dep’t of State*, 565 F.3d 857, 861–62, 870 (D.C. Cir. 2009), *Bassiouni*, 392 F.3d at 246, *Pullara v. CIA*, 248 F.3d 1140, 1140 (5th Cir. 2001) (per curiam), and *Minier v. CIA*, 88 F.3d 796, 801 (9th Cir. 1996). For analogous cases, compare *Adejumobi v. NSA*, 287 F. App’x 770 (11th Cir. 2008) (per curiam) (noting NSA’s Glomar response but not deciding its validity), and *Carpenter v. U.S. Dep’t of Justice*, 470 F.3d 434, 436–37 & nn.3, 6 (1st Cir. 2006) (recognizing but not applying Glomar response).

<sup>63</sup> See generally 5 U.S.C. § 552 (2006). At least one congressional committee has (briefly) indicated approval of the response. See H.R. REP. NO. 98-726, pt. 1, at 27 (1984), reprinted in 1984 U.S.C.C.A.N. 3741, 3765.

<sup>64</sup> See, e.g., *Campaign for Responsible Transplantation v. FDA*, 511 F.3d 187, 196 (D.C. Cir. 2007) (“[This court has] expressed concern over the ‘distort[ing]’ effects of . . . infor-

requestors face special difficulties because they lack information about the actual content of withheld records that would allow them to contest vigorously the withholding in court.<sup>65</sup> In non-Glomar FOIA cases, *Vaughn* indices<sup>66</sup> and in camera review of records<sup>67</sup> alleviate the burden on plaintiffs and facilitate accurate resolution of the case.

Although these procedures certainly have their faults,<sup>68</sup> they have substantially enabled an adversarial process that ensures robust disclosure of records. With Glomar, however, these procedures are unavailable. Because the existence of underlying documents is shielded in the Glomar context and creating a *Vaughn* index necessarily requires acknowledging the existence of underlying records, a *Vaughn* index would be of no assistance.<sup>69</sup> Similarly, in camera review of withheld records is seen as inapposite, since there are no records to review as long as an agency maintains a Glomar response. As a substitute procedure, courts require the government to prepare public affidavits describing, in as much detail as possible, the logical justifications for refusing to confirm or deny the existence of responsive records.<sup>70</sup> But although courts call for agencies to “create as complete a public record as possible,”<sup>71</sup> the sensitive nature of issues at stake in Glomar cases generally prompts the agency to limit its public affidavits and supplement them with submission of classified declarations to the court. These declarations can be considered in camera and ex parte.<sup>72</sup> When reviewing such submissions, courts are required to afford “substantial weight”<sup>73</sup> to agency affidavits as long as they contain “reasonably specific detail, demonstrate that the information

---

mation asymmetry [in FOIA litigation] on ‘the traditional adversary nature of our legal system’s form of dispute resolution.’” (citation omitted) (second alteration in original)).

<sup>65</sup> Agencies’ Glomar responses are typically terse, providing requestors with virtually no information. *See, e.g.*, Letter from Delores M. Nelson to Melissa Goodman, *supra* note 1 (“The fact of the existence or nonexistence of requested records is currently and properly classified and is intelligence sources and methods information that is protected from disclosure . . . . Therefore, your request has been denied . . . .”).

<sup>66</sup> *See supra* notes 24–26 and accompanying text (describing *Vaughn* index requirement and procedure).

<sup>67</sup> *See generally* 5 U.S.C. § 552(a)(4)(B) (2006).

<sup>68</sup> *See, e.g.*, Brooker, *supra* note 33, at 1249–51 (criticizing courts’ hesitancy to use in camera review in Exemption 3 cases); Deyling, *supra* note 29, at 82–86 (arguing that in camera review has not been effectively used by judges); *id.* at 98–102 (criticizing *Vaughn* indices as often insufficiently descriptive and of little aid to adversarial process).

<sup>69</sup> *See* *Phillippi v. CIA (Phillippi I)*, 546 F.2d 1009, 1013 n.7 (D.C. Cir. 1976) (“Since the ‘document’ the Agency is currently asserting the right to withhold is confirmation or denial of the existence of the requested records, we stress that we are not requiring, at this stage, the *Vaughn* index requested by appellant.”).

<sup>70</sup> *Wilner v. NSA*, 592 F.3d 60, 68 (2d Cir. 2009); *Phillippi I*, 546 F.2d at 1013.

<sup>71</sup> *Phillippi I*, 546 F.2d at 1013.

<sup>72</sup> *Wilner*, 592 F.3d at 68; *Phillippi I*, 546 F.2d at 1012.

<sup>73</sup> *Wilner*, 592 F.3d at 68.

October 2010]

REFORMING THE GLOMAR RESPONSE

1393

withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.”<sup>74</sup> Courts give tremendous deference to agency arguments, accepting them if they are “logical or plausible.”<sup>75</sup> Although courts occasionally reject agency Glomar responses,<sup>76</sup> most assertions of the Glomar response are accepted.<sup>77</sup>

Once an agency has carried its burden of justifying use of the Glomar response, a requestor can force disclosure of the existence or nonexistence of requested records only by one of two showings: Either that the government has already “officially acknowledged” the existence of the sought-after records,<sup>78</sup> or that the government is acting in bad faith or concealing violations of law.<sup>79</sup> Both are extremely hard to prove in court.

To invalidate a Glomar response on the grounds that the government has already acknowledged the existence of the requested records, the information previously disclosed must exactly match the information requested, both in specificity and content, and the previous disclosure must have been both official and documented.<sup>80</sup> Information in the public domain indicating that the government holds requested records is not sufficient unless it came from an acknowledgement by a government official in the same agency subject

---

<sup>74</sup> *Larson v. Dep’t of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (quoting *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984)).

<sup>75</sup> *Id.* (internal quotations omitted) (citing *Wolf v. CIA*, 473 F.3d 370, 374–75 (D.C. Cir. 2007)); see also *Aitchison*, *supra* note 11, at 237–38 (“[C]ourts have extreme difficulty determining the propriety of the Glomar response . . . [in part because they have] no method for checking the agency’s accuracy other than examining public and *in camera* affidavits.”).

<sup>76</sup> See, e.g., *Morley v. CIA*, 508 F.3d 1108, 1126 (D.C. Cir. 2007) (remanding for agency to “substantiate its *Glomar* response”); *Judicial Watch, Inc. v. U.S. Secret Serv.*, 579 F. Supp. 2d 182, 185–86 (D.D.C. 2008) (invalidating agency’s Glomar response on basis that agency’s proffered harms justifying refusal were not credible); *ACLU v. Dep’t of Def.*, 389 F. Supp. 2d 547, 561, 565–66 (S.D.N.Y. 2005) (rejecting government’s Glomar response as to one part of plaintiffs’ FOIA request); *Nat’l Sec. Archive v. CIA*, No. 99-1160, slip op. at 15–16, 19 (D.D.C. July 31, 2000) (holding that CIA had waived Glomar response by previous official disclosures of information).

<sup>77</sup> See *ACLU*, 389 F. Supp. 2d at 562 (“[T]he courts generally respect the CIA’s right to make a Glomar response.”).

<sup>78</sup> *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990); see also *Wilner*, 592 F.3d at 70 (quoting *Fitzgibbon*).

<sup>79</sup> E.g., *Wilner*, 592 F.3d at 75.

<sup>80</sup> *Fitzgibbon*, 911 F.2d at 765; see also *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007) (“Prior disclosure of similar information does not suffice; instead, the *specific* information sought by the plaintiff must already be in the public domain by official disclosure.”).

to the request.<sup>81</sup> This exacting standard is difficult to meet, although some requestors have prevailed on this ground.<sup>82</sup>

Proving bad faith on the part of the agency is similarly difficult. Agencies may not, as a rule, invoke the Glomar response out of bad faith or to conceal violations of law.<sup>83</sup> Courts place the burden of proof for showing bad faith on the requestor, and will uphold the agency's action as long as its explanation is "logical or plausible."<sup>84</sup> Given the information asymmetry inherent in Glomar cases, plaintiffs have a difficult time meeting this standard. Even where the subject of a FOIA request is a program that is arguably operating in violation of the law, such as the NSA's warrantless wiretapping program, courts will not presume that the agency used the Glomar response *in order to* conceal such violations of the law and thus let the agency's response stand.<sup>85</sup>

### III

#### DIFFICULTIES POSED BY THE GLOMAR RESPONSE

Few, if any, commentators (or litigants for that matter) contest that the government may in some cases legitimately invoke the Glomar response.<sup>86</sup> Rather, most criticism directed at the practice is that the response is used too often or that courts treat it too deferentially, and that it allows the government to withhold information

---

<sup>81</sup> *Hunt v. CIA*, 981 F.2d 1116, 1120 (9th Cir. 1992); *Afshar v. Dep't of State*, 702 F.2d 1125, 1129–30 (D.C. Cir. 1983).

<sup>82</sup> *See, e.g., Wolf*, 473 F.3d at 379 (invalidating CIA Glomar response on basis that former CIA director had testified before Congress that agency possessed information relating to subject of FOIA request); *Nat'l Sec. Archive v. CIA*, No. 99-1160, slip op. at 15–16, 19 (D.D.C. July 31, 2000) (holding that CIA waived Glomar response as to request for CIA biographies of former leaders of Eastern European countries through previous admissions that agency compiles "biographies on *all* heads of state").

<sup>83</sup> A similar rule applies to claims that information is classified, as the executive order governing classification of national security information prohibits classification to "conceal violations of law, inefficiency, or administrative error [or to] prevent embarrassment to a person, organization, or agency." Exec. Order No. 13,526 § 1.7(a)(1)–(2), 75 Fed. Reg. 707, 710 (Dec. 29, 2009), *reprinted in* 50 U.S.C.A. § 435 note (West 2010).

<sup>84</sup> *Wilner*, 592 F.3d at 75.

<sup>85</sup> *E.g., People for the Am. Way Found. v. NSA*, 462 F. Supp. 2d 21, 29–31 (D.D.C. 2006); *see also Arabian Shield Dev. Co. v. CIA*, No. 3-98-CV-0624-BD, 1999 WL 118796, at \*4 (N.D. Tex. Feb. 26, 1999) (prohibiting agency "from classifying documents as a ruse when they could not otherwise be withheld from public disclosure [but not preventing] the classification of national security information merely because it might reveal criminal or tortious acts").

<sup>86</sup> *See, e.g., Aitchison, supra* note 11, at 237 ("Arguably, legitimate uses for the Glomar response do exist."); *Pozen, supra* note 16, at 313–14 n.203 ("Glomar responses may be necessary in some extreme cases."). Even the requestor in *Phillippi I* conceded that the Glomar response was sometimes appropriate. *Phillippi v. CIA (Phillippi I)*, 546 F.2d 1009, 1012 (D.C. Cir. 1976).

October 2010]

REFORMING THE GLOMAR RESPONSE

1395

excessively.<sup>87</sup> It is difficult to determine the frequency of invocation of the Glomar response, as government agencies are not required to keep statistics on its use.<sup>88</sup> The only publicly accessible indication of the frequency of Glomar responses is in reported court cases, from which it appears that use of the response has increased sharply in recent years.<sup>89</sup> This is only moderately illuminating, however, as most agency denials of FOIA requests do not result in litigation.<sup>90</sup> It is clear that numerous agencies have taken advantage of the Glomar response since its first use by the CIA,<sup>91</sup> but the frequency of use by each agency is unreported.

Curtailing use of the response is difficult, as agencies have a strong incentive, in addition to the general dynamics contributing to

---

<sup>87</sup> See, e.g., Aitchison, *supra* note 11, at 237 (“[T]he CIA extended the Glomar response beyond its logical limits . . . .”); Gotanda, *supra* note 11, at 177 (“The expanded use of Glomar denials has made it significantly more difficult for FOIA requestors to effectively challenge an agency’s withholding.”).

<sup>88</sup> FOIA requires all agencies to submit annual public reports detailing “the number of determinations made by the agency not to comply with requests for records . . . and the reasons for each such determination.” 5 U.S.C. § 552(e)(1)(A) (2006). This is interpreted as requiring agencies to specify how often they invoked each of FOIA’s disclosure exemptions and to account for other reasons for denying requests, but not how often the Glomar response has been used. See, e.g., CIA, FREEDOM OF INFORMATION ACT ANNUAL REPORT, FISCAL YEAR 2008, at 8–9 (2008), available at [http://www.foia.ucia.gov/txt/Annual\\_Report\\_2008.pdf](http://www.foia.ucia.gov/txt/Annual_Report_2008.pdf) (reporting number of FOIA exemptions claimed but not Glomar responses). Because the Glomar response is never invoked independently of the nine FOIA exemptions, it is not considered an independent reason for denying a request. Telephone Interview with Office of the Info. & Privacy Coordinator, CIA (Feb. 5, 2010) (relating that CIA’s FOIA tracking database does not differentiate Glomar responses from other denials).

<sup>89</sup> Amicus Curiae Brief of National Security Archive in Support of Appellants to Vacate and Remand at 9, *Wilner*, 592 F.3d 60 (No. 08-4762-cv) (“The Glomar Response has arisen in roughly 80 federal court opinions since 1976. Roughly 60 of those cases have been decided since September 11, 2001 . . . .”). This statistic covers invocation of the Glomar response in both national security and privacy cases.

<sup>90</sup> In a recent two-year period, only approximately 0.2% of FOIA denials resulted in litigation against the withholding agency. Compare Edward B. Gerard, Note, *Bush Administration Secrecy: An Empirical Study of Freedom of Information Act Disclosure*, 15 MEDIA L. & POL’Y 84, 121 tbl.5 (2005) (reporting that 88,966 and 108,919 FOIA requests were fully or partially denied by federal agencies in 2002 and 2003, respectively (excluding requests made to Social Security Administration and Veterans Administration)), with DEP’T OF JUSTICE, 2002 LITIGATION AND COMPLIANCE REPORT: 2002 CALENDAR YEAR REPORT ON FREEDOM OF INFORMATION ACT LITIGATION ACTIVITIES (2003), available at <http://www.justice.gov/oip/02introduction.htm> (listing 184 FOIA cases received by DOJ for litigation in 2002), and DEP’T OF JUSTICE, 2003 LITIGATION AND COMPLIANCE REPORT: 2003 CALENDAR YEAR REPORT ON FREEDOM OF INFORMATION ACT LITIGATION ACTIVITIES (2004), available at <http://www.justice.gov/oip/03introduction.htm> (listing 265 FOIA cases received by DOJ in 2003).

<sup>91</sup> See, e.g., ROBERT M. PALLITTO & WILLIAM G. WEAVER, PRESIDENTIAL SECRECY AND THE LAW 82 (2007) (noting that Glomar response has been “seized on by other government departments” and listing some agencies that have invoked it since mid-1990s).

excessive classification,<sup>92</sup> to overuse it. The most basic difficulty posed by the Glomar response is that, to be effective, it must be used consistently.<sup>93</sup> For any particular refusal to confirm or deny the existence of records to be credible, the requestor must believe that the government agency issues identical refusals both when it has responsive records and when it does not.<sup>94</sup> Were the government to invoke the Glomar response only when it had responsive records that it wished to conceal, while giving a traditional “no records” response when it had no such responsive records, then requestors would come to see the Glomar response as nothing more than a functional government admission that records existed but were being covered up.<sup>95</sup> As a result, the government is overprotective of information in two distinct ways.

First, agencies tend to use the Glomar response in reply to FOIA requests that seek information about implausible government activities or operations which could easily be denied on their merits without harming national security. For example, the National Reconnaissance Office and the CIA issued Glomar denials in response to a FOIA request seeking information about an alleged secret spy satellite program “able ‘to read the pulses and patterns of the human brain.’”<sup>96</sup> It seems rather implausible that such a program exists. Refusing to confirm or deny the existence of responsive records appears more likely to stoke paranoid conspiracy theories than to conceal classified information about the nation’s intelligence activities. But because the request seeks the *type* of information that could reveal sensitive national security information if acknowledged—namely, the capabilities of the government’s spy satellite technology—the desire to make consistent use of Glomar likely prompted the agency to issue the response.

Second, agencies issue Glomar responses even when broad details of a program are publicly known and when requestors have a

---

<sup>92</sup> There is widespread agreement that the government overclassifies information. *See, e.g.,* THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 417 (“Current security requirements nurture overclassification and excessive compartmentation of information among agencies.”); Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL’Y REV. 399, 401 (2009) (“In recent years, in fact, classification—specifically overclassification—has increased . . .”).

<sup>93</sup> Winchester & Zirkle, *supra* note 33, at 249–50.

<sup>94</sup> *Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004); Winchester & Zirkle, *supra* note 33, at 249–50.

<sup>95</sup> DOD Freedom of Information Act Program Regulation, 32 C.F.R. § 286.12(a)(1) (2009).

<sup>96</sup> *Roman v. Dailey*, No. 97-1164, 1998 U.S. Dist. LEXIS 6708, at \*2, \*6–12 (D.D.C. May 8, 1998) (upholding Glomar responses).



October 2010]

REFORMING THE GLOMAR RESPONSE

1397

significant basis for believing that the requested records exist. This was the case in *Phillippi* and *Military Audit Project*, where the government issued Glomar responses amid widespread press reports about both the substance of the Glomar Explorer project and about the CIA's efforts to suppress press coverage of it.<sup>97</sup>

This expansive application of the Glomar response can be viewed as either necessary or destructive. Per the former view, consistent and widespread use of the Glomar response is necessary to protect sensitive information from damaging disclosure<sup>98</sup> and is a vital mechanism for preventing release of the government's deepest secrets.<sup>99</sup> In the national security realm, this view is sharpened by the mosaic theory, which posits that “[e]ven disclosure of what appears to be the most innocuous information . . . poses a threat to national security . . . because it might permit our adversaries to piece together sensitive information.”<sup>100</sup>

On the alternative view, the Glomar response is dangerous because, in the words of one district court judge, it “encourage[s] an unfortunate tendency of government officials to over-classify information, frequently keeping secret that which the public already knows, or that which is more embarrassing than revelatory of intelligence sources or methods.”<sup>101</sup> That tendency to overclassify is revealed in the story of the Glomar Explorer itself: In *Phillippi*, the CIA refused to confirm or deny whether it had records related to its own efforts to persuade news outlets to withhold publication of articles about the Glomar Explorer,<sup>102</sup> even though those very same news organizations necessarily had firsthand knowledge of those efforts.<sup>103</sup> Even after the CIA acknowledged that it held records, problems with excessive secrecy persisted. In the late 1980s, a private citizen filed a FOIA request with the NSA seeking, among other documents, records about

---

<sup>97</sup> See *supra* notes 36–38 and accompanying text (discussing press reports about CIA's involvement with Glomar Explorer).

<sup>98</sup> H.R. REP. NO. 98-726, at 26–27 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3741, 3764–65.

<sup>99</sup> Pozen, *supra* note 16, at 313 n.203.

<sup>100</sup> *Wilner v. NSA*, 592 F.3d 60, 74 (2d Cir. 2009) (internal quotation marks omitted). See generally David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (discussing evolution of mosaic theory and problems of judicial deference to mosaic theory claims). For discussions of mosaic theory in Glomar cases, see, for example, *Wolf v. CIA*, 473 F.3d 370, 377 (D.C. Cir. 2007), and *Hunt v. CIA*, 981 F.2d 1116, 1119 (9th Cir. 1992).

<sup>101</sup> *ACLU v. Dep't of Def.*, 389 F. Supp. 2d 547, 561 (S.D.N.Y. 2005).

<sup>102</sup> *Phillippi v. CIA (Phillippi I)*, 546 F.2d 1009, 1011 (D.C. Cir. 1976).

<sup>103</sup> See, e.g., Hersh, *supra* note 37, at 52 (“The New York Times was informed by the C.I.A. . . . that publication [of details about the Glomar Explorer project] would endanger the national security [and therefore] decided at that time to withhold publication.”).

the Glomar Explorer.<sup>104</sup> Despite the CIA's decision to acknowledge the existence of such records more than a decade earlier, the NSA initially refused to confirm or deny whether it possessed responsive records.<sup>105</sup> Such secrecy seems excessive, as it closes the barn doors far too late: The horse is out of the government's stable, and everybody knows where it came from.

#### IV

##### SEPARATION OF POWERS AND PROPOSALS FOR REFORM

Deference by courts to agency use of the Glomar response is pervasive, but traditional explanations of that deference are faulty. In the national security arena, the two recurring justifications for such deference stand on separation of powers grounds: first, that the judiciary should not interfere with the executive's constitutional authority to protect national security information;<sup>106</sup> and second, that courts are comparatively less well equipped to make determinations about the protection of national security records.<sup>107</sup> These concerns are important to address, as they are the major obstacles preventing courts from subjecting Glomar responses to more searching review.

This Part addresses these separation of powers issues by first considering whether courts have constitutional authority to more vigorously scrutinize national security-related Glomar responses. Concluding that Congress has given courts this authority, this Part then assesses whether courts *should* engage in such permitted scrutiny by balancing prudential separation of powers concerns against the problem of institutional conflict of interest that arises when executive agencies make essentially unreviewed decisions to withhold their own records from disclosure.<sup>108</sup> This Part concludes by offering proposals for reform.

---

<sup>104</sup> See *Lindsey v. NSA*, No. 90-2408, 1990 WL 148422, at \*1 (4th Cir. Oct. 9, 1990).

<sup>105</sup> *Id.* at \*2. More than two years after issuing this initial Glomar response, the NSA changed course, conducting a search for records and informing the requestor that the agency could find no responsive files. *Id.*

<sup>106</sup> See *infra* Part IV.A.1.

<sup>107</sup> See *infra* Part IV.A.2.

<sup>108</sup> For a similar analysis in the state secrets context, see D.A. Jeremy Telman, *Our Very Privileged Executive: Why the Judiciary Can (and Should) Fix the State Secrets Privilege*, 80 TEMP. L. REV. 499, 505–10 (2007). The constitutional and prudential separation-of-powers dimensions roughly track the formalist and functionalist interpretations of separation of powers. This Note does not seek to enter the debate between proponents of these modes of interpretation. See generally M. Elizabeth Magill, *The Real Separation in Separation of Powers Law*, 86 VA. L. REV. 1127, 1136–45 (2000) (describing and analyzing this debate).

## A. Separation of Powers Concerns in Glomar Oversight

### 1. Constitutional Separation of Powers Concerns

Judicial deference to the Glomar response raises the question of whether constitutional separation of powers concerns prohibit, or conversely, require, more probing review. The federal judiciary often takes a “deferential view of the Executive’s classification power [based on] the notion that . . . the President is constitutionally vested with broad, substantive responsibility for the conduct of foreign affairs” and national defense.<sup>109</sup> On this view, the executive branch “must have the largely unshared duty to determine and preserve the degree of internal security necessary . . . . [I]t is the constitutional duty of the Executive to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense.”<sup>110</sup> Such a view locates executive authority in the President’s Article II national security powers as commander in chief of the military<sup>111</sup> and in his or her foreign affairs powers suggested by the treaty and ambassador clauses,<sup>112</sup> as bolstered by judicial discussions of executive power in these contexts.<sup>113</sup> Under this reading of executive power, courts are constitutionally obligated to defer to executive actions intended to protect national security information under FOIA, including the use of the Glomar response.

Of course, the separation of powers in our constitutional system is not absolute, and the role of interbranch checks and balances is crucial to cabinining the power of each branch.<sup>114</sup> Courts have never held that the executive’s classification decisions are beyond the reach of

---

<sup>109</sup> Note, *Keeping Secrets: Congress, the Courts, and National Security Information*, 103 HARV. L. REV. 906, 917–18 (1990).

<sup>110</sup> N.Y. Times Co. v. United States, 403 U.S. 713, 728–30 (1971) (Stewart, J., concurring); see also Note, *supra* note 109, at 906 (“Driven by separation of powers considerations, both Congress and the judiciary have recognized the legitimacy of th[e] executive’s role in protecting national security, and generally have declined to challenge either the breadth or the scope of executive classification decisions.”).

<sup>111</sup> U.S. CONST. art. II, § 2, cl. 1.

<sup>112</sup> U.S. CONST. art. II, § 2, cl. 2; *Id.* §§ 2, 3.

<sup>113</sup> See, e.g., Dep’t of the Navy v. Egan, 484 U.S. 518, 527 (1988) (“[The President’s] authority to classify and control access to information bearing on national security . . . flows primarily from th[e] constitutional investment of power in the President and exists quite apart from any explicit congressional grant.”); United States v. Nixon, 418 U.S. 683, 706 (1974) (suggesting that separation of powers doctrine provides heightened protection to presidential communications when they involve “military, diplomatic, or sensitive national security secrets”). Fuller engagement with the varied literature on theories of the unitary executive and the national security constitution is beyond the scope of this Note.

<sup>114</sup> THE FEDERALIST NO. 48, at 300 (James Madison) (Gary Wills ed., 1982) (“[U]nless [the legislative, executive, and judiciary] departments be so far connected and blended, as to give to each a constitutional controul over the others, the degree of separation which the maxim requires as essential to a free government, can never in practice, be duly main-

judicial review in FOIA cases, and proper judicial review of Exemption 1 FOIA claims leaves ample space to place checks on executive authority. Indeed, Congress, which itself has deep and wide-ranging national security powers enumerated in the Constitution,<sup>115</sup> has specifically given the courts a role in overseeing executive withholding of records under FOIA's Exemption 1, both in the command that courts review agency determinations *de novo*<sup>116</sup> and in the requirement that courts determine whether withheld records are "in fact properly classified."<sup>117</sup> In Exemption 3 cases, somewhat less scrutiny may be envisioned, as the judicial role is simply to determine whether an effective withholding statute exists and whether that statute applies in the given case.<sup>118</sup> Still, the *de novo* review provision requires courts to make a serious inquiry into the proper application of the withholding statute, again demonstrating congressional intent to give courts a role in balancing executive power.

The most useful means of determining the degree of deference due to executive invocation of the Glomar response is provided by the framework proposed by Justice Jackson in his concurrence to *Youngstown Sheet & Tube Co. v. Sawyer*.<sup>119</sup> In Justice Jackson's tripartite scheme, the extent of executive power to perform a given action is dependent on whether Congress has spoken on the issue and the degree of authority the Constitution grants to the executive in that

---

tained."); Magill, *supra* note 108, at 1157–59 (discussing mixture of separation of powers and balance of powers in constitutional system).

<sup>115</sup> U.S. CONST. art. I, § 8, cl. 1 ("The Congress shall have Power To . . . provide for the common Defence . . ."); *id.* cl. 3 (granting foreign commerce power to Congress); *id.* cl. 10 ("[Congress shall have power] To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations . . ."); *id.* cls. 11–16 (granting Congress power to declare war and to create and regulate military); *id.* art. II, § 2, cl. 2 (granting Senate significant role in Treaty and Ambassador clauses). Congress was thus by far the dominant branch in national security and foreign affairs at the time of the country's founding. Moreover, courts have often reaffirmed Congress's national security powers. *See, e.g., Hamdan v. Rumsfeld*, 548 U.S. 557, 591–95 (2006) (discussing necessity of congressional power to authorize use of military commissions); *Greene v. McElroy*, 360 U.S. 474, 496, 495–500 (1959) (noting Congress's power to authorize government agencies' security clearance programs); *Ex parte Quirin*, 317 U.S. 1, 26–28 (1942) (listing constitutional sources of Congress's national security powers and finding that Congress had authorized military commissions in World War II); *Little v. Barreme*, 6 U.S. (2 Cranch) 170, 177–79 (1804) (approving only those executive actions taken on high seas which Congress had explicitly authorized through legislation).

<sup>116</sup> 5 U.S.C. § 552(a)(4)(B) (2006).

<sup>117</sup> *Id.* § 552(b)(1)(A).

<sup>118</sup> *See Wolf v. CIA*, 473 F.3d 370, 377 (D.C. Cir. 2007) ("The Supreme Court gives even greater deference to CIA assertions of harm to intelligence sources and methods under [Exemption 3 withholdings pursuant to] the National Security Act [than under Exemption 1]."); *supra* notes 57–60 and accompanying text (describing Exemption 3 and providing examples of judicial decisions involving Exemption 3 statutes).

<sup>119</sup> 343 U.S. 579, 634 (1952) (Jackson, J., concurring).

sphere.<sup>120</sup> Presidential authority is at its greatest when Congress has approved the action taken (category one), occupies a murky middle ground when Congress is silent on the issue (category two), and is at its lowest when Congress has expressly disapproved the President's action (category three). In FOIA cases, Congress has expressly granted power to the judiciary to evaluate the executive's national security-justified FOIA withholdings. The executive's power is thus pushed toward its "lowest ebb," Jackson's third category.<sup>121</sup> In the presence of such congressional action, the President can claim plenary authority over classification and withholding decisions only if the President's own constitutional powers are sufficient to encompass them.<sup>122</sup> In the FOIA context, because Congress has occupied the field and created a role for the courts, the executive must act consistently with the will of Congress, unless the President has independent powers in this area that trump Congress's.<sup>123</sup> As Justice Jackson cautioned, recognizing executive power in such circumstances is dangerous, as it means that the President's power is exclusive in the field and that Congress may never effectively regulate the area, threatening the very "equilibrium established by our constitutional system."<sup>124</sup>

While Congress has vested courts with authority to review national security-related FOIA withholdings in general, it has been almost completely silent regarding the Glomar response. Congress has failed to limit or prohibit Glomar, despite Congress's (arguable) knowledge of Glomar's use.<sup>125</sup> This congressional inaction may push

---

<sup>120</sup> Justice Jackson proposed a three-part framework for evaluating presidential power. First, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum." *Id.* at 635. Second, "[w]hen the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority." *Id.* at 637. Third, "[w]hen the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." *Id.* The Court has recently reaffirmed the utility of this framework. *Medellin v. Texas*, 127 S. Ct. 1346, 1368 (2008).

<sup>121</sup> 343 U.S. at 637 (Jackson, J., concurring).

<sup>122</sup> *Id.*

<sup>123</sup> FOIA is a creation of Congress, as are its disclosure exemptions. The issue here is not whether Congress could force executive disclosure of classified or otherwise sensitive national security information under FOIA by repealing Exemptions 1 and 3. Rather, the issue is simply whether Congress and the courts have the power to *regulate* executive applications of those exemptions.

<sup>124</sup> *Youngstown*, 343 U.S. at 638 (Jackson, J., concurring).

<sup>125</sup> For limited evidence of congressional cognizance of the Glomar response, see *supra* note 63 (noting brief favorable discussion of Glomar response in 1984 committee report). Passing reference to the Glomar response was later made in testimony at a 1996 House subcommittee hearing. *War Crimes Disclosure Act, Health Information, Privacy Protection Act: Hearing on H.R. 1281 and S. 1090 Before the Subcomm. on Government Management,*

executive authority over Glomar toward Justice Jackson's second category, the "zone of twilight."<sup>126</sup> Judicial decisions in category two cases are split. Congressional silence has sometimes been read by courts as evidencing congressional acquiescence, vesting the executive with authority to act.<sup>127</sup> Conversely, congressional silence has also been interpreted as *divesting* the executive of authority to act in cases where the President lacks clear inherent authority over the matter at hand, and Congress's silence is interpreted as lack of approval.<sup>128</sup>

In the case of the Glomar response, congressional silence should not be interpreted as vesting the executive with exclusive authority so as to oust the courts from the ability to provide meaningful review. First, congressional silence does not always (or even often) constitute congressional assent.<sup>129</sup> Although Congress gave fleeting mention to the Glomar response in a 1984 committee hearing, it has apparently not considered the issue since.<sup>130</sup> Congress has amended FOIA nine times<sup>131</sup> but has never spoken on use of the Glomar response. In *Dames & Moore v. Regan*, the Supreme Court held congressional silence to be tantamount to consent to presidential power where Congress *had* considered proposals to limit executive power on an issue but had explicitly rejected them.<sup>132</sup> Such knowing acquiescence is not present here, as the history of congressional nonengagement with the Glomar response does not fairly suggest that the practice is "known to and acquiesced in by Congress."<sup>133</sup>

Second, although Congress has not spoken to the Glomar response, it has spoken clearly on the judicial role in FOIA cases. Congress's mandates that courts engage in *de novo* review and that

---

*Information and Technology of the H. Comm. on Government Reform and Oversight*, 104th Cong. 48 (1996) (statement of Professor Robert E. Herzstein).

<sup>126</sup> *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

<sup>127</sup> *Dames & Moore v. Regan*, 453 U.S. 654, 686 (1981); *Haig v. Agee*, 453 U.S. 280, 300–01 (1981).

<sup>128</sup> See *Youngstown*, 343 U.S. at 585, 587–89 (majority opinion) (holding that Congress had power over areas in question and that because it had passed no statutes expressly or impliedly authorizing President's actions, President was without power to act).

<sup>129</sup> See Burt Neuborne, *In Praise of Seventh-Grade Civics: A Plea for Stricter Adherence to Separation of Powers*, 26 LAND & WATER L. REV. 385, 400 (1991); cf. *Rapanos v. United States*, 547 U.S. 715, 750 (2006) (Scalia, J.) (plurality opinion) (arguing that congressional inaction should not be interpreted as acquiescence with executive activity absent "overwhelming evidence" of congressional intent).

<sup>130</sup> See *supra* note 125 (setting forth references to Glomar response by Congress).

<sup>131</sup> See OPEN FOIA Act of 2009, Pub. L. No. 111-83, § 564, 123 Stat. 2142, 2184 (2009) (codified at 5 U.S.C. § 552(b)(3) (Supp. III 2009)) (amending Exemption 3); DEPARTMENT OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT 5–7 (2009), available at [http://www.justice.gov/oip/foia\\_guide09.htm](http://www.justice.gov/oip/foia_guide09.htm) (listing eight amendments through 2007).

<sup>132</sup> 453 U.S. at 685–86.

<sup>133</sup> *Id.* at 686 (internal quotations omitted).

October 2010]

REFORMING THE GLOMAR RESPONSE

1403

Exemption 1 withholdings be “properly classified”<sup>134</sup> evinces a background principle of judicial review and congressional retention of power when the executive withholds national security information. Further, Congress recently amended Exemption 3 to require that for any new statute to trigger withholding under that section, the new law must explicitly reference Exemption 3.<sup>135</sup> This reaffirms congressional control over withholding under that exemption, and gives an additional role to courts in scrutinizing agency withholding claims. Congress’s default norm of judicial review of agency withholding decisions applies equally to Glomar and non-Glomer cases and undermines claims that congressional silence on the Glomar response is of constitutional import.<sup>136</sup>

Assuming that Congress could regulate (whether or not it could prohibit) use of the Glomar response through legislation—just as it regulates national security–related agency withholdings under Exemptions 1 and 3—then the corollary question is whether the courts currently possess power to review and restrict use of the Glomar response. Congressional silence on the propriety of Glomar should not be interpreted as acquiescing to current uses of the response and extreme judicial deference to those uses. Rather, such silence should be understood as continuing Congress’s policy of retaining limitations on executive power and investing the judiciary with authority over national security FOIA withholdings in general. Thus, the courts are in fact required to scrutinize and restrain uses of the Glomar response. Given that they have such power as a matter of law, the next question is whether they should, as a matter of policy, exercise it.

## 2. Prudential Separation of Powers

The question of whether courts *should* scrutinize the Glomar response, as opposed to the question of whether they *may* do so, requires engagement with prudential separation of powers issues, namely, the judiciary’s supposed relative lack of institutional competence in protecting sensitive national security information.<sup>137</sup> This con-

---

<sup>134</sup> 5 U.S.C. § 552 (b)(1)(B) (2006).

<sup>135</sup> OPEN FOIA Act of 2009 § 564.

<sup>136</sup> See *Wilner v. NSA*, 592 F.3d 60, 68 (2d Cir. 2009) (noting that “[a]n agency ‘resisting disclosure’ of the requested records [via the Glomar response] ‘has the burden of proving the applicability of an exemption,’” just as in non-Glomer cases).

<sup>137</sup> See *Telman*, *supra* note 108, at 507–10 (discussing prudential separation of powers justifications for allowing executive to invoke state secrets privilege in civil suits); *cf.* *Neuborne*, *supra* note 129, at 391 (discussing “functional” separation of powers).

cern is manifest in ordinary FOIA cases,<sup>138</sup> but it is especially strong in cases upholding the Glomar response. In a recent Glomar case, the Second Circuit “affirm[ed its] ‘deferential posture in FOIA cases regarding the uniquely executive purview of national security.’”<sup>139</sup> It did so on the basis that, given “the relative competencies of the executive and judiciary, we believe that it is bad law and bad policy to ‘second-guess the predictive judgments made by the government’s intelligence agencies’ regarding questions [about] whether disclosure of . . . records would pose a threat to national security.”<sup>140</sup> This species of deference stems partly from a concern about the severity of harms that could result from incorrect disclosure decisions by courts—if the fact of existence or nonexistence of records would reveal truly sensitive national security information, then forcing an agency to confirm whether it has records could cause harm.<sup>141</sup> Mosaic theory exacerbates this concern, since judges fear that second-guessing agency justifications for refusing to confirm or deny the existence of records about seemingly innocent or minor matters would allow enemy analysts to place the last tile into an accumulating mosaic of information.<sup>142</sup>

Additionally, the Glomar response in particular lends itself to abdication of judicial oversight as a result of the nature of evidence received in Glomar cases. Unlike the *Vaughn* affidavits and in camera review of withheld documents available to judges in normal FOIA cases, the evidence put forward by the government in Glomar response cases consists solely of affidavits—public or classified—that describe the logical bases for agencies’ refusal to confirm or deny the existence of records.<sup>143</sup> Thus, the judge must proceed on the basis of the agency’s logical arguments alone, without the benefit of examining records or other evidence. As one commentator has noted, the evidence typically considered by judges in Glomar cases “threaten[s] to undermine the text and purpose of [FOIA because courts rely] solely on the agenc[ies’] representations and do[ ] not determine for [them-

---

<sup>138</sup> See, e.g., *CIA v. Sims*, 471 U.S. 159, 176 (1985) (allowing CIA to withhold records under Exemption 3 based partly on concern that “judges, who have little or no background in the delicate business of intelligence gathering,” are ill-equipped to make accurate determinations in protecting national security information).

<sup>139</sup> *Wilner*, 592 F.3d at 76 (quoting *Larson v. Dep’t of State*, 565 F.3d 857, 865 (D.C. Cir. 2009)).

<sup>140</sup> *Id.* (citation omitted) (quoting *Larson*, 565 F.3d at 865); accord *Gardels v. CIA*, 689 F.2d 1100, 1105 (D.C. Cir. 1982).

<sup>141</sup> See *Wheeler v. CIA*, 271 F. Supp. 2d 132, 140 (D.D.C. 2003) (“[T]he decisions of the [agency], who must, of course, be familiar with the whole picture, as judges are not, are worthy of great deference given the magnitude of the national security interests and the potential risks at stake.” (quoting *Knight v. CIA*, 872 F.2d 660, 664 (5th Cir. 1989))).

<sup>142</sup> See *supra* note 100 and accompanying text (describing mosaic theory).

<sup>143</sup> *Wilner*, 592 F.3d at 68; *Larson*, 565 F.3d at 862.



October 2010]

REFORMING THE GLOMAR RESPONSE

1405

selves] whether the underlying documents are properly classified or whether any portion can be reasonably segregated and disclosed.”<sup>144</sup> In the case of classified affidavits examined in camera and ex parte, judges also lose the benefit of receiving informed adverse arguments from the requesting party. Because agencies will likely argue the danger of disclosure in the strongest possible terms, judges’ fears about mistakenly forcing disclosures will be at their peak while the resources available to allay those fears will be particularly limited when the Glomar response is in play.

Institutional competence concerns can become paralyzing if played out to their logical end. It is certainly true that agencies tasked with regularly handling national security information possess expertise that allows them to assess the risks of disclosing records. But it is also widely recognized that the government radically overclassifies information.<sup>145</sup> This tendency to overclassify—and the attendant deference courts confer—may be even greater with the Glomar response, which allows agencies to argue that they are protecting their greatest, most sensitive secrets. Whether agencies’ true rationale for invoking Glomar is legitimately to protect information that would damage the national security if released, or instead to conceal wrongdoing or avoid embarrassment, is unknown and unexamined in most Glomar cases. Ceding all questions of competence to the executive results in a level of deference inconsistent with the judicial function and, particularly, with de novo review.

Moreover, there is no reason to think that courts are unable to handle national security information—the comparative competency concern is overblown.<sup>146</sup> The provision for in camera, ex parte review of withheld records under FOIA clearly contemplates a role for judges in assessing government withholding decisions, thus evidencing

---

<sup>144</sup> Pozen, *supra* note 16, at 313 n.203.

<sup>145</sup> See *supra* note 92 (discussing general agreement that government overclassifies information).

<sup>146</sup> See *Hamdi v. Rumsfeld*, 542 U.S. 507, 535 (2004) (“[W]e necessarily reject the Government’s assertion that separation of powers principles mandate a heavily circumscribed role for the courts in [evaluating enemy combatant designation procedures].”); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 320 (1972) (“We cannot accept the Government’s argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to . . . the issues involved in domestic security cases.”); *Arar v. Ashcroft*, 585 F.3d 559, 613 (2d Cir. 2009) (en banc) (Parker, J., dissenting) (“The Supreme Court has repeatedly made clear that the separation of powers does not prevent the judiciary from ruling on matters affecting national security, and that the courts are competent to undertake this task.”); *Zweibon v. Mitchell*, 516 F.2d 594, 643 (D.C. Cir. 1975) (“[J]udges do, in fact, have the capabilities needed to consider and weigh data pertaining to the foreign affairs and national defense of this nation.”).

congressional confidence in the ability of courts to make determinations in all areas covered by FOIA, including the national security exemptions.<sup>147</sup> Courts frequently deal with sensitive national security information in contexts outside of FOIA,<sup>148</sup> and there is no reason they cannot apply their expertise in evaluating factual and legal arguments to examinations of the Glomar response.

Overblown concerns about judicial competence must be balanced against another serious concern: institutional conflicts of interest inherent in agencies making largely unreviewed decisions to withhold information that those agencies have a (potentially illegitimate) interest in keeping secret.<sup>149</sup> When it comes to the Glomar response, these conflict concerns militate against judicial deference to agency decisionmaking. Indeed, agencies' inability effectively to police themselves *requires* a structural separation of powers check in the form of meaningful judicial review. Given agency incentives to over-invoke the Glomar response, more restrained use of the response will depend on courts exercising their constitutional power to examine Glomar claims. Arguments made in the context of the state secrets privilege, which raises issues parallel to those at stake with the Glomar response—and has spawned a more developed literature—help explain the point.

The state secrets privilege is a common law evidentiary doctrine recognized by the Supreme Court more than fifty years ago.<sup>150</sup> The

---

<sup>147</sup> See *Ray v. Turner*, 587 F.2d 1187, 1210 (D.C. Cir. 1978) (“The major argument [for judicial deference is] that judges lack the knowledge and expertise necessary to make decisions about disclosure in [national security] cases. Congress soundly rejected this contention, however, and refused to create a presumption in favor of agency classifications or to retreat from full *de novo* review.”).

<sup>148</sup> See Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1806(f), 1825(g) (2006) (empowering district courts to review applications and orders from Foreign Intelligence Surveillance Court in camera and ex parte); Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 §§ 1–16 (setting procedures for federal courts to review, evaluate, and protect classified information in criminal trials); *United States v. Reynolds*, 345 U.S. 1, 9–11 (1953) (affirming power of courts to review executive claims of state secrets privilege and to examine documents in camera if necessary); *Parhat v. Gates*, 532 F.3d 834, 844–48 (D.C. Cir. 2008) (evaluating classified intelligence documents and concluding that assertions in those documents were not reliable for purposes of making enemy combatant designation). Courts also issue classified or redacted opinions in order to protect classified national security information at issue in suits before them. See, e.g., *Parhat v. Gates*, No. 06-1397, 2008 WL 2588713, at \*1 (D.C. Cir. June 30, 2008) (ordering public release of sealed opinion regarding challenge to detention at Guantánamo, and noting that classified material is to be redacted in public opinion).

<sup>149</sup> Cf. Ben Wizner, Staff Attorney, ACLU, Remarks at the American Constitution Society Panel Discussion: The State Secrets Privilege: Time for Reform? (Apr. 4, 2008) (transcript available at [http://www.acslaw.org/files/2008-04-07\\_ACS\\_State\\_Secrets\\_Privilege.doc](http://www.acslaw.org/files/2008-04-07_ACS_State_Secrets_Privilege.doc)) (making this argument in state secrets context).

<sup>150</sup> *Reynolds*, 345 U.S. at 1.

October 2010]

REFORMING THE GLOMAR RESPONSE

1407

privilege, which can be invoked by the government in any civil case, serves as a means of protecting secret government documents from forced disclosure in discovery.<sup>151</sup> Under the state secrets privilege, “[t]he executive branch that is making the determinations [to invoke the state secrets privilege is,] in most of these cases[,] the same executive branch that’s being charged with wrongdoing in these cases.”<sup>152</sup> Thus, just as with the Glomar response, the executive branch has “an interest . . . in avoiding embarrassment” which distorts its ability to properly invoke the state secrets privilege in some cases.<sup>153</sup> The judiciary’s fixation on its own lack of expertise with protecting national security information in state secrets cases—the prudential separation of powers concern discussed above—leads to excessive deference to state secrets claims and an insufficient check on excessive withholding of information.<sup>154</sup> Analogous concerns inhere in the Glomar context.

Agencies undoubtedly have expertise that allows them to evaluate whether acknowledging the existence of records would cause harm to national security or other government interests. But they also have incentives to withhold records for other, less legitimate reasons. One dangerous, though not necessarily invidious, reason stems from institutional culture and individual incentives to overclassify information. No individual FOIA officer or agency classification authority wants to be responsible for acknowledging the existence of agency records (or releasing those records) if doing so would cause harm to national security or other interests. Thus, they are likely to err on the side of nondisclosure when faced with a FOIA request implicating national security issues.<sup>155</sup> Institutional incentives also run toward

---

<sup>151</sup> *Id.* at 7–8, 10 (holding that privilege prevents disclosure when “there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged”).

<sup>152</sup> Wizner, *supra* note 149.

<sup>153</sup> *Id.*; see also Beth George, Note, *An Administrative Law Approach to Reforming the State Secrets Privilege*, 84 N.Y.U. L. REV. 1691, 1706–07 (2009) (discussing incentives for government to “over-invoke the [state secrets] privilege,” including “the desire to cover up embarrassing or illegal acts within the administration,” “to prevent the prosecution of government officials,” and “to prevent paying money damages as a result of alleged government misconduct”).

<sup>154</sup> See Telman, *supra* note 108, at 505 (“Courts have been inexplicably obtuse in ignoring the conflict of interest inherent in the government’s invocation of the Privilege and inexcusably callous in dismissing the rights of individual litigants who cannot vindicate their rights due to the Privilege.”).

<sup>155</sup> See *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on National Security, Emerging Threats and International Relations of the H. Comm. on Government Reform*, 108th Cong. 82 (2004) [hereinafter *Too Many Secrets*] (statement of Carol A. Haave, Undersecretary of Defense for Intelligence) (“[P]eople have a tendency to err on the side of caution and so therefore may in fact

excessive secrecy by sanctioning underclassification and overdisclosure but taking a permissive stance toward excessive withholding of records.<sup>156</sup> Thus, in a setting where excessive classification is the norm, FOIA officers and agency classification authorities tend to withhold information when it is unnecessary to do so.<sup>157</sup>

A more troubling reason for overuse of the Glomar response lies in agencies' desire to conceal embarrassing information or cover up illegal conduct. This tendency is especially problematic in cases where publicly available information about government programs raises questions about the legality or propriety of government conduct.<sup>158</sup> For example, the government has maintained Glomar responses in the face of requests for information about the NSA's warrantless wiretapping program,<sup>159</sup> details of which were revealed by the *New York Times* in 2005.<sup>160</sup> Prior to congressional authorization of that program in 2008,<sup>161</sup> serious challenges to its legality were raised in courts and the press, with one federal court holding that the program violated "the [Administrative Procedure Act]; the Separation of Powers doctrine; the First and Fourth Amendments of the United States Constitution; and the statutory law."<sup>162</sup> Given that the program is already public, issuing a Glomar response raises an inference that the government is seeking to suppress incriminating evidence of illegal spying on Americans, or, perhaps, to protect itself from embarrassment and additional public scrutiny. Most of the harms that would flow from acknowledging the existence of records about a truly secret

---

[over]classify things . . ."); Christina E. Wells, "National Security" Information and the Freedom of Information Act, 56 ADMIN. L. REV. 1195, 1202 (2004) ("[E]xecutive officials have every incentive to read a classification charge expansively. In fact, psychological studies suggest that executives will err on the side of safety when something as important as national security is at stake.").

<sup>156</sup> Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 148–49 (2006).

<sup>157</sup> Cf. *Too Many Secrets*, *supra* note 155, at 81–82 (statement of Carol A. Haave, Undersecretary of Defense for Intelligence) (estimating that up to fifty percent of classifications are excessive).

<sup>158</sup> See *ACLU v. Dep't of Def.*, 389 F. Supp. 2d 547, 561 (S.D.N.Y. 2005) ("The danger of Glomar responses is that they encourage an unfortunate tendency of government officials to over-classify information, frequently keeping secret that which the public already knows, or that which is more embarrassing than revelatory of intelligence sources or methods.").

<sup>159</sup> See generally *Wilner v. NSA*, 592 F.3d 60 (2d. Cir. 2009); *People for the Am. Way v. NSA/Cent. Sec. Serv.*, 462 F. Supp. 2d 21 (D.D.C. 2006).

<sup>160</sup> James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

<sup>161</sup> FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified at 50 U.S.C. § 1881 (2010)).

<sup>162</sup> *ACLU v. NSA/Cent. Sec. Serv.*, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006), *rev'd on standing grounds*, 493 F.3d 644 (6th Cir. 2007).

October 2010]

REFORMING THE GLOMAR RESPONSE

1409

program dissipate once that program becomes public, leaving a smaller scope of legitimate potential harm that can be invoked to support the Glomar response.<sup>163</sup>

In sum, courts are competent to handle national security information and routinely do so in FOIA and other contexts, so there is no reason to doubt their competence to review invocations of the Glomar response. Further, the judiciary has a crucial structural separation-of-powers role to play in checking the executive: Given the dangers of institutional conflict of interest, courts should exercise their oversight power with increased vigor in Glomar cases.

### 3. *Judicial Reform of the Glomar Response*

The most obvious remedy for excessive judicial deference is for courts to apply greater scrutiny. However, this is not to argue that courts should uniformly reject use of the Glomar response. The response surely has a role in a small subset of cases where the government is legitimately shielding highly sensitive information and where no other response would adequately protect national security. Several modest reforms would help restrict the Glomar response to only such appropriate uses. First, courts could more aggressively apply the existing bad faith standard.<sup>164</sup> By probing more deeply into agency justifications for the Glomar response, courts can help smoke out illegitimate attempts to use the response to avoid embarrassment or conceal violations of law. Further, courts could use the bad faith standard to look behind agency rationales and ensure that agencies invoke the Glomar response only when it is absolutely necessary—that is, only when traditional withholding of records under the FOIA exemptions would not suffice to protect against harmful disclosures.

Courts could also take advantage of their *in camera* review power to demand that agencies produce more evidence to justify their invocation of the Glomar response, including any underlying records (if they exist) or an admission that records do not exist if that is the case. This would help judges more accurately evaluate the propriety of Glomar claims, including by allowing them to take a hard look at justi-

---

<sup>163</sup> When what was once a secret becomes public, an agency's remaining rationale for invoking a Glomar response is that unique harms flow from that agency *itself* confirming or disproving its role in a particular activity. *Phillippi v. CIA (Phillippi I)*, 546 F.2d 1009, 1014 n.11 (D.C. Cir. 1976). Thus, in the context of the NSA's warrantless wiretapping program, the Agency asserts that acknowledging the existence of certain records would confirm operational details, such as exactly who has been surveilled, which are as yet not public. *Wilner*, 592 F.3d at 69–70.

<sup>164</sup> See *supra* notes 83–85 and accompanying text (describing bad faith standard); *cf.* Deyling, *supra* note 29, at 102–04 (proposing that courts apply strengthened bad faith standard in non-Glomar national security cases).

fications based on mosaic theory.<sup>165</sup> In order to protect against accidental disclosure of the existence or nonexistence of records, courts could take advantage of protective procedures already used in cases involving classified records.<sup>166</sup> This approach has been criticized on the grounds that it would “draw[ ] [courts] into a sham review if documents do not exist.”<sup>167</sup> To the contrary, such review would help provide a check on executive power by providing judges with a fuller picture of agencies’ decisionmaking. Increased judicial scrutiny is an important first step toward reform of the Glomar response, especially given the existing statutory mandate of de novo judicial review.

### B. *Alternative Proposals for Reform*

Alongside increased judicial scrutiny, Congress or the executive itself could pursue other potentially effective means of reform. Further, because relatively few FOIA requestors seek judicial review of agency denials, the courts are a realistic option only for sophisticated and well-funded parties with the time and patience to litigate.<sup>168</sup> While such litigation can result in significant disclosures of information,<sup>169</sup> even if courts more vigorously oversaw use of the Glomar response in cases that reached them, the infrequency of FOIA suits

---

<sup>165</sup> See *supra* notes 100, 142 and accompanying text (discussing mosaic theory).

<sup>166</sup> Existing procedures include ex parte and in camera document review, employing law clerks with security clearances, use of Department of Justice court security officers who are trained to “assist the courts in protecting the secrecy of classified information,” and measures to secure secret records physically, including use of “Sensitive Compartmented Information Facilit[ies]” in or near courthouses. ROBERT TIMOTHY REAGAN, KEEPING GOVERNMENT SECRETS: A POCKET GUIDE FOR JUDGES ON THE STATE-SECRETS PRIVILEGE, THE CLASSIFIED INFORMATION PROCEDURES ACT, AND COURT SECURITY OFFICERS 3, 17–19 (2007), available at [http://www.fjc.gov/public/pdf.nsf/lookup/Secrets1.pdf/\\$file/Secrets1.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/Secrets1.pdf/$file/Secrets1.pdf); see also Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information, 18 U.S.C. app. 3 § 9 note (2006), reprinted in REAGAN, *supra*, at 31–37. Such procedures would respond to concerns that “any *in camera* review of requested materials would necessarily confirm their existence, thus eviscerating defendant’s Glomar Response.” Roman v. NSA, No. 07-CV-4502, 2009 WL 303686, at \*6 n.5 (E.D.N.Y. Feb. 9, 2009).

<sup>167</sup> Gotanda, *supra* note 11, at 179 (proposing reforms in privacy “Glomarization” context).

<sup>168</sup> See *supra* note 90 (calculating that approximately only 0.2% of agency denials of FOIA requests result in litigation).

<sup>169</sup> Recent FOIA lawsuits by civil liberties and human rights organizations have resulted in the release of thousands of pages of government documents. See, e.g., JAMEEL JAFFER & AMRIT SINGH, ADMINISTRATION OF TORTURE 2 (2007) (“In October 2003, the ACLU . . . filed a [FOIA] request . . . for government records concerning the treatment of prisoners apprehended by the United States in connection with the ‘war on terror.’ A lawsuit filed . . . to enforce the FOIA request has since resulted in the release of thousands of government documents.”); Ctr. for Constitutional Rights, Freedom of Information Act: Ghost Detention and Extraordinary Rendition Case, <http://ccrjustice.org/ghostfoia> (last visited Mar. 21, 2010) (making available thousands of pages of government documents regarding

October 2010]

REFORMING THE GLOMAR RESPONSE

1411

would still dilute the effectiveness of judicial review because agencies would expect few of their actions to be challenged in court. Congressional and executive reforms are no substitute for proper judicial review, but they can play a role in ensuring that limitations are placed on use of the Glomar response and that FOIA's goal of government transparency and citizen oversight is adequately served.

### 1. Administrative Reform

Reforms instituted wholly within the executive branch provide one possible solution.<sup>170</sup> Regulation of agency use of the Glomar response can occur both at the level of individual agencies and across the entire executive branch. Within agencies, FOIA procedures are governed by published regulations,<sup>171</sup> some of which include provisions authorizing the Glomar response and regulating its use.<sup>172</sup> Agencies whose regulations do not provide rules for invocation of the Glomar response, such as the Departments of Justice and Homeland Security, should promulgate regulations setting out clear rules for when it is appropriate to use Glomar.<sup>173</sup> Agencies such as the CIA and Department of Defense that already have Glomar regulations should amend them to clarify the limited circumstances under which Glomar may be invoked. Such rules should make clear that under existing law Glomar is never appropriate to conceal agency wrongdoing or to avoid embarrassment and that it should be used only when no other response will protect legitimately classified information. The benefit of including rules on the proper use of the Glomar response in the Code of Federal Regulations is that doing so makes the rules public, predictable, and more readily enforceable.<sup>174</sup> It also avoids ad

---

CIA's secret rendition and black site-prison programs that were released in response to FOIA lawsuit).

<sup>170</sup> A similar path has been proposed in the state secrets context as a way of bolstering "internal self-policing" and curbing abuse in light of barriers to meaningful judicial oversight. George, *supra* note 153, at 1716-17. As compared to the state secrets privilege, administrative reforms to the Glomar response are even more apt to produce results because FOIA is implemented and administered in the first instance by agency officials granting or denying requests.

<sup>171</sup> See generally 28 C.F.R. § 16.1-.12 (2009) (DOJ FOIA regulations); 32 C.F.R. § 286.1-.36 (2009) (DOD FOIA regulations); 32 C.F.R. § 1900.01-.45 (2009) (CIA FOIA regulations).

<sup>172</sup> E.g., 32 C.F.R. § 286.12(a)(1) (2009) (DOD Glomar regulation); 32 C.F.R. § 1900.21(c) (2009) (CIA Glomar regulation).

<sup>173</sup> In the absence of formal rules governing use of the Glomar response, agencies are bound by only the general limitations established by courts. However, court cases provide limited guidance for agency officials to determine whether the Glomar response is proper in connection with any given FOIA request.

<sup>174</sup> See George, *supra* note 153, at 1721-23, 1722 n.156 (arguing for publicly published rules governing use of state secrets privilege). Creating agency rules on Glomar also allows

hoc application of Glomar, thus helping ensure that the response is not used inappropriately to conceal records when they would be embarrassing to agency officials but not damaging to national security on the whole.<sup>175</sup>

Reform at the agency level may prove difficult, as institutional pressures on FOIA officers and other staff to err on the side of excessive concealment are likely to be significant. Thus, a more powerful catalyst for reform may come from top-level executive action. The Attorney General sets broad priorities for FOIA implementation through memoranda to the heads of executive departments and agencies announcing the standards that the DOJ will use in deciding whether to defend agency withholding decisions in court.<sup>176</sup> The Attorney General could draft and circulate such standards regarding the Glomar response.<sup>177</sup> These standards should state that the DOJ will defend an agency's Glomar response only if the response is required to avoid foreseeable and serious harm to national security and if using normal FOIA procedures would be highly likely to reveal classified or otherwise protected national security information. Additionally, the standards should make clear that the Glomar response is never to be used to shield agencies from embarrassment, or otherwise used in bad faith.

Congress recently created another oversight mechanism: the Office of Government Information Services (OGIS).<sup>178</sup> OGIS is tasked with "reviewing [agency] compliance with [FOIA]," and "recommending policy changes to Congress and the President."<sup>179</sup> As OGIS develops its purview, it should make oversight of the Glomar response a priority. Because OGIS is located in the National Archives and Records Administration, and not in the DOJ, it may have suffi-

---

for notice-and-comment rulemaking, which provides an opportunity for public input and the potential for more transparency-oriented rules in response to commenters' concerns.

<sup>175</sup> Short of promulgating new Glomar regulations, the Chief FOIA Officers in each federal agency could play a role in ensuring greater compliance with FOIA and more moderate use of the Glomar response. *See generally* OPEN Government Act of 2007, Pub. L. No. 110-175, § 10(a), 121 Stat. 2524, 2529 (2007) (codified at 5 U.S.C. § 552(j)-(k) (Supp. I 2009) (creating position of Chief FOIA Officer in each agency)).

<sup>176</sup> *See, e.g.*, Memorandum from Eric H. Holder, Jr., U.S. Att'y Gen., to Heads of Executive Dep'ts and Agencies (Mar. 19, 2009), *available at* <http://www.justice.gov/ag/foia-memo-march2009.pdf> (describing policy under President Obama).

<sup>177</sup> *Cf. Bifurcation Requirement, supra* note 50, at 2 ("[I]n employing privacy 'Glomarization,' agencies must be careful not to use it to an extent that is not warranted . . . . [T]his means making sure that the *only possible* response that the agency can give to the request is to neither confirm nor deny that any responsive record exists.").

<sup>178</sup> OPEN Government Act of 2007 § 10(a). OGIS began operating in September 2009. Office of Government and Information Services, <http://www.archives.gov/ogis/> (last visited May 25, 2010).

<sup>179</sup> 5 U.S.C. § 552(h)(2) (Supp. I 2007).



October 2010]

REFORMING THE GLOMAR RESPONSE

1413

cient independence to play a forceful oversight role.<sup>180</sup> OGIS should track agency use of Glomar and should draft best practices guidelines for Glomar use.

## 2. *Legislative Reform*

Congress also has a role to play in limiting agency use of the Glomar response. Because FOIA is wholly a statutory creation (unlike, for example, the state secrets privilege<sup>181</sup>), it makes sense for Congress to regulate use of the Glomar response under the Act. Congress has recently demonstrated a willingness to strengthen FOIA by passing pro-transparency amendments in the last two legislative sessions,<sup>182</sup> and there is no reason it could not weigh in on the appropriate uses of the Glomar response.<sup>183</sup>

Danae Aitchison has proposed amending FOIA to regulate use of the Glomar response by expanding the review power of courts.<sup>184</sup> He proposes that “Congress . . . explicitly grant[ ] courts in Glomar response cases the power to order live testimony [from agency officials] about a request,” and that Congress “should direct courts to use *in camera* affidavits only as a last resort.”<sup>185</sup> These amendments would be steps in the right direction, in part because they, along with similar mechanisms, would demonstrate to courts that Congress intends there to be robust judicial review of Glomar claims. This, in turn, would undermine courts’ reliance on comparative competence concerns.<sup>186</sup>

An alternative approach would be for Congress to regulate the primary conduct of agencies, rather than judicial review of that conduct, by specifying when the Glomar response may properly be

---

<sup>180</sup> See 155 CONG. REC. S2818 (2009) (statement of Sen. Leahy) (“Establishing [the OGIS] within the National Archives is essential to reversing the troubling trend of lax FOIA compliance and excessive government secrecy during the past 8 years.”).

<sup>181</sup> See Telman, *supra* note 108, at 514 (“The . . . problem with a statutory solution [to state secrets privilege problems] is that it is hard to imagine . . . how legislators . . . could fashion a solution that would anticipate all the contexts in which the Privilege might be invoked.”).

<sup>182</sup> See OPEN Government Act of 2007; OPEN FOIA Act of 2009, Pub. L. No. 111-83, § 564, 123 Stat. 2142, 2184 (2009) (codified at 5 U.S.C. § 552(b)(3) (Supp. III 2009)).

<sup>183</sup> Indeed, some other countries’ freedom of information laws specifically discuss—and regulate—responses analogous to the Glomar response. See, e.g., Freedom of Information Act, 2000, c. 36, § 24(2) (Eng.) (“The duty to confirm or deny does not arise if, or to the extent that, exemption from [that duty] is required for the purpose of safeguarding national security.”); Freedom of Information Act, 1982, § 25 (Austl.) (describing when agency is not required to “give information as to the existence or non-existence of a document”).

<sup>184</sup> See Aitchison, *supra* note 11, at 249–51.

<sup>185</sup> *Id.*

<sup>186</sup> See generally *supra* Part IV.A.2 (discussing institutional competence concerns and prudential separation of powers).

used.<sup>187</sup> Congress should clarify that the Glomar response is to be used only as a last resort, when traditional responses would reveal properly protected national security information. Congress should also modify the official acknowledgement standard<sup>188</sup> to prohibit an agency from maintaining a Glomar response once *any* government official has officially acknowledged that records about a topic or program exist. This would end overuse of the Glomar response in cases where one agency continues to refuse to confirm or deny the existence of records after another agency has acknowledged government involvement in a formerly secret program.<sup>189</sup>

Reporting requirements provide a further means of regulation because they reveal agency practices and can act as catalysts for future reform. FOIA requires that each federal agency prepare annual reports detailing their activity under the Act.<sup>190</sup> Congress should add a subsection to FOIA requiring these reports to include information about the number of times the Glomar response is used and the exemptions under which it is invoked. Additionally, the Government Accountability Office is now tasked with “conduct[ing] audits of administrative agencies on the implementation of [FOIA].”<sup>191</sup> The GAO should examine and evaluate use of the Glomar response during such audits.

Finally, the relevant congressional committees should hold hearings to investigate use and abuse of the Glomar response. Congressional oversight would help push agency officials to self-regulate and could trigger constructive reform. Hearings would also allow courts to better evaluate the executive’s constitutional authority under Justice Jackson’s *Youngstown* framework by ending congressional silence about Glomar.

## CONCLUSION

FOIA is a powerful instrument of government transparency, but its effectiveness is frustrated by overuse of the Glomar response in

---

<sup>187</sup> See Aitchison, *supra* note 11, at 246 (“Congress should state that agencies may use the Glomar response only in very limited circumstances.”).

<sup>188</sup> See *supra* notes 78–82 and accompanying text (discussing official acknowledgements standard applied by courts).

<sup>189</sup> See, e.g., *Hunt v. CIA*, 981 F.2d 1116, 1120 (9th Cir. 1992) (“According to CIA affidavits, it is . . . irrelevant that some of the information sought by [the requestor] had already been made public by other governmental and law enforcement agencies.”).

<sup>190</sup> 5 U.S.C. § 552(e) (2010); see also *supra* note 88 (describing reporting requirements). Similar reporting schemes are required in other areas involving national security concerns, such as with FISA warrants and National Security Letters. George, *supra* note 153, at 1721.

<sup>191</sup> OPEN Government Act of 2007, Pub. L. No. 110-175, § 10(a), 121 Stat. 2524 (2007) (codified at 5 U.S.C. § 552(i) (Supp. I 2007)).

October 2010]

REFORMING THE GLOMAR RESPONSE

1415

connection with national security–related requests. Reviewing judges seldom invalidate Glomar responses and often invoke separation of powers concerns to justify their deference to agency Glomar claims. Although such concerns are not wholly without basis, they are exaggerated. This Note argues that the judiciary should give greater weight to conflict-of-interest problems raised when agencies use the Glomar response to withhold their own records with little judicial oversight. Greater scrutiny of agency uses of the Glomar response is needed.

Congressional and judicial reforms aimed at decreasing deference to Glomar claims deserve serious consideration, but reforms implemented by the executive may be the most effective short-term strategy for limiting use of the Glomar response. Executive branch reforms have the virtue of addressing problems with the Glomar response at their root, before judicial review becomes necessary. Ultimately, however, it is most important that action is taken, not that any particular actor makes the first move. There is clearly a role for limited secrecy in our democracy, but the government must take seriously the spirit of transparency underlying FOIA in its responses to requests made under the Act.<sup>192</sup> Vigorous regulation and oversight can prevent the Glomar response from continuing to be an exception that swallows the rule.

---

<sup>192</sup> Cf. DANIEL PATRICK MOYNIHAN, *SECRECY* (1998) (discussing dangers of government secrecy); Fuchs, *supra* note 156, at 136–39 (arguing that excessive government secrecy undermines national security).

# EXHIBIT NW1/2

Publication by ACLU, *“Stingray Tracking Devices: Who’s Got Them?”*, November 2018.



Published on *American Civil Liberties Union* (<https://www.aclu.org>)

## Stingray Tracking Devices: Who's Got Them? <sup>[1]</sup>

[Updated November 2018]

The map below tracks what we know, based on press reports and publicly available documents, about the use of stingray tracking devices by state and local police departments. Following the map is a list of the federal agencies known to have the technology. The ACLU has identified 75 agencies in 27 states and the District of Columbia that own stingrays, but because many agencies continue to shroud their purchase and use of stingrays in secrecy, this map dramatically underrepresents the actual use of stingrays by law enforcement agencies nationwide.

Stingrays, also known as "cell site simulators" or "IMSI catchers," are invasive cell phone surveillance devices that mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect's cell phone, they also gather information about the phones of countless bystanders who happen to be nearby.

[More on Stingray tracking devices](#) <sup>[2]</sup>

### Federal Agencies Known to Use Cell Site Simulators:



[3]

[Federal Bureau of Investigation](#) <sup>[3]</sup>



[4]

[Drug Enforcement Administration](#) <sup>[4]</sup>



[5]

[U.S. Secret Service](#) <sup>[5]</sup>



[6]

[Immigration and Customs Enforcement](#) <sup>[6]</sup>

©

Source URL: <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>



[7]

[U.S. Marshals Service](#) [7]



[7]

[Bureau of Alcohol, Tobacco, Firearms, and Explosives](#) [7]



[8]

[Internal Revenue Service](#) [8]



[9]

[U.S. Army](#) [9]



[10]

[U.S. Navy](#) [10]



[11]

[U.S. Marine Corps](#) [11]

**Links**

- [1] <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>
- [2] <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices>
- [3] <http://online.wsj.com/news/articles/SB10001424053111904194604576583112723197574>
- [4] <https://epic.org/foia/fbi/stingray/In-re-US-Application-06022012.pdf>
- [5] [https://www.fbo.gov/index?s=opportunity&mode=form&id=5bdo813d2a6cc76117eca48451bed9c3&tab=core&\\_cview=0](https://www.fbo.gov/index?s=opportunity&mode=form&id=5bdo813d2a6cc76117eca48451bed9c3&tab=core&_cview=0)
- [6] [https://www.fbo.gov/?s=opportunity&mode=form&id=d40f66df9ef1cf54bcc98f45195507f2&tab=core&tabmode=list&print\\_preview=1](https://www.fbo.gov/?s=opportunity&mode=form&id=d40f66df9ef1cf54bcc98f45195507f2&tab=core&tabmode=list&print_preview=1)
- [7] <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/2/>



[12]

[U.S. National Guard](#) [12]



[13]

[U.S. Special Operations Command](#) [13]



[14]

[National Security Agency](#) [14]



[15]

[Customs and Border Protection](#) [15]

[8]

surveillance-technology-irs-cellphone-tower

[9] [https://www.fbo.gov/index?s=opportunity&mode=form&id=fdo3ebae781f3a3fdb7633699bc1e351&tab=core&\\_cview=1](https://www.fbo.gov/index?s=opportunity&mode=form&id=fdo3ebae781f3a3fdb7633699bc1e351&tab=core&_cview=1)

[10] <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f34fc14f76e8744bfe75d41e6d0242db>

[11] [https://www.fbo.gov/index?s=opportunity&mode=form&id=6a5efbce2b7bdf2f37448ad68d48e7e&tab=core&\\_cview=0](https://www.fbo.gov/index?s=opportunity&mode=form&id=6a5efbce2b7bdf2f37448ad68d48e7e&tab=core&_cview=0)

[12] <https://www.fbo.gov/>

[https://www.fbo.gov/?s=opportunity&mode=form&id=407f9f124a17646ad4e866f628cc7591&tab=core&tabmode=list&print\\_preview=1](https://www.fbo.gov/?s=opportunity&mode=form&id=407f9f124a17646ad4e866f628cc7591&tab=core&tabmode=list&print_preview=1)

[13] <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=3176fb4a66f92793ac34e7670205e2c5>

[14] <https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/>

[15] <https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf>

# EXHIBIT NW1/3

Excerpt from Electronic Surveillance Manual, Executive Office for United States Attorneys, U.S. Department of Justice, released in response to FOIA request by Linda Lye, ACLU of Northern California (Aug. 22, 2013).



USABook > Criminal Procedure > Electronic Surveillance > Electronic Surveillance Manual > **XIV**,  
prev | next | help

## **XIV. Cell Site Simulators/Digital Analyzers/Triggerfish**

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," *i.e.*, telephone number) and electronic serial number ("ESN," *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/ triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).

Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.

Because section 3127 of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider. See discussion below in Chapter XV.

# **EXHIBIT NW1/4**

Memorandum from Chief Scott R. Patronik, Erie County Sheriff's Office, to All Cellular Phone Tracking Team Members, re: Cellular Tracking Procedures (June 11, 2014), released in response to public records request by the New York Civil Liberties Union.

# ERIE COUNTY SHERIFF'S OFFICE

## MEMORANDUM

---

**TO:** All Cellular Phone Tracking Team Members

**FROM:** Chief Scott R. Patronik

**DATE:** June 11, 2014

**SUBJECT: CELLULAR TRACKING PROCEDURES**

1. Cellular tracking equipment is to be used for official law enforcement purposes only.
2. Notify the Chief of Special Services, or designee, of any cellular tracking requests/missions.
3. A CL will be taken "Asst Other Police – Cellular Tracking" (4519) (even if assisting ECSO Personnel). Include in the CL (at a minimum):
  - Reference original CL# or other agency name / case number;
  - Name and contact information of requestor;
  - Brief summary as to the purpose of the cellular tracking request. (Lost person, suicidal person, arrest warrant, etc);
  - Describe the legal authority for tracking the cellular phone (exigent circumstances, arrest warrant, court order, etc). Exigent circumstances exist when there is an immediate danger of death or serious physical injury to a person;
  - The phone number being tracked and the cellular provider for the number;
  - Name of the person being tracked (if known); and
  - If any data collected will be saved as evidence after the tracking session.

**LAW ENFORCEMENT SENSITIVE (LES) // FOR OFFICIAL USE ONLY (FOUO)**

4. Unless there is a specific reason to do so, do not save any data collected by the cellular tracking equipment after the completion of the tracking session.
5. If data collected by the cellular tracking equipment is saved after the completion of a tracking session, the data must be handled as evidence (burned to non-rewritable media such as DVD-R, chain of custody, proper storage, etc). Before analyzing this collected evidence, you must discuss the collection with the appropriate prosecutor's office to ensure there is proper legal authority to analyze the collected data.
6. The following procedures are considered Law Enforcement Sensitive (LES) information, the disclosure of which would reveal non-routine criminal investigative techniques and procedures. At a minimum, these procedures will be disseminated only on a "need-to-know" basis and when unattended will be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

# **EXHIBIT NW1/5**

Email exchange among attorneys in the United States Attorney's Office for the Northern District of California (May 23, 2011), released in response to FOIA request by the ACLU of Northern California and the San Francisco Bay Guardian newspaper.

**Kenney, Patricia (USACAN)**

---

**From:** Waldinger, Kyle (USACAN)  
**Sent:** Monday, May 23, 2011 12:48 PM  
**To:** Beausey, Karen (USAMA); USACAN-Attorneys-Narcotics  
**Subject:** RE: IMPORTANT INFORMATION RE: PEN REGISTERS

And just to be super clear, the agents may not use the term "WIT" (or "WITT") but rather may be using the term "Triggerfish" or the term "Stingray," so please make sure that the agents know what you are referring to.

---

**From:** Beausey, Karen (USACAN)  
**Sent:** Monday, May 23, 2011 12:17 PM  
**To:** USACAN-Attorneys-Narcotics  
**Subject:** FW: IMPORTANT INFORMATION RE: PEN REGISTERS  
**Importance:** High

Hi everyone. Miranda asks 4 questions, but I think we need an answer to a 5<sup>th</sup> one as well: whether or not the initial intended purpose of the pen register was to use the WIT technology to locate someone, did the agents eventually use the pen in that way? In other words, a pen might have started out as just a pen, and later the agents decided to use the order to also attempt to locate the target. They may or may not have told you about this decision. So, check in with your agents and find out whether they have been using pen register orders to locate targets with the WIT boxes, whether or not they started out intending to do so.

Thanks.

Karen

---

**From:** Kane, Miranda (USACAN)  
**Sent:** Monday, May 23, 2011 11:55 AM  
**To:** USACAN-Attorneys-Criminal  
**Subject:** IMPORTANT INFORMATION RE: PEN REGISTERS  
**Importance:** High

**Effective immediately all pen register applications and proposed orders must be reviewed by your line supervisor before they are submitted to a magistrate judge.**

As some of you may be aware, our office has been working closely with the magistrate judges in an effort to address their collective concerns regarding whether a pen register is sufficient to authorize the use of law enforcement's WIT technology ( a box that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with some specificity) to locate an individual. It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit.

While we continue work on a long term fix for this problem it is important that we are consistent and forthright in our pen register requests to the magistrates which is why I am

adding this additional review. I anticipate that I will be able to eliminate the line supervisor approval requirement once we have an opportunity to discuss the issue with the bench and revise the language in our common application. In the meantime, I appreciate your cooperation in this matter.

In addition, if you have requested a pen register in the last six months – since January 2011 - please provide the following information to your supervisor as soon as possible: 1) Was the pen register approved by a magistrate? 2) Which magistrate reviewed it? 3) Was the purpose of the pen register to locate a person? 4) Did the agency requesting the pen register use WIT technology? This information will be extremely valuable to me in my discussions with the magistrate judges.

Again, thank you in advance for your assistance. I will update everyone about the status of this issue at our Criminal Division Meeting on June 7, 2011.

Miranda

# EXHIBIT NW1/6

Email exchange among officers with the police departments in Sarasota and North Port, Florida (Apr. 15–20, 2009), released in response to public records request by the ACLU of Florida.



**From:** [Kenneth Castro](#)  
**To:** [Robert Estrada](#)  
**Cc:** [Paul Sutton](#); [Tom Laughlin](#); [Curt Holmes](#)  
**Bcc:**  
**Subject:** RE: Trap and Trace Confidentiality  
**Date:** Monday, April 20, 2009 10:29:57 AM

---

Thank you. Your attentiveness to this issue is greatly appreciated. Have a great week!!

---

**From:** Robert Estrada [restrada@northportpd.com]  
**Sent:** Monday, April 20, 2009 9:15 AM  
**To:** Kenneth Castro  
**Cc:** Terry Lewis; Kevin Vespia  
**Subject:** FW: Trap and Trace Confidentiality

Sgt. Castro, we have changed the PCA within the agency after consulting with the SAO. The PCA that was already within the court system according to the SAO will have to remain since it has already been submitted. At some point and time the SAO will submit the changed document as an addendum. We have implemented within our detective bureau to not use this investigative tool on our documents in the future.

---

**From:** Kevin Vespia  
**Sent:** Thursday, April 16, 2009 7:54 AM  
**To:** Robert Estrada  
**Subject:** FW: Trap and Trace Confidentiality

Bob,

If we did this, can you please look into this and come up with a plan on how we correct it? We need to address this ASAP. Thanks



**Capt. Kevin Vespia #110**  
**North Port Police Department**  
**4980 City Hall Blvd.**  
**North Port, FL 34286**  
**Office: 941-429-7306**  
**Fax: 941-429-7389**

Note: Florida Public Records Law Provides that most written communications to or from Municipal employees regarding city business are public records, available to the public and media upon request. Therefore, this e-mail message may be subject to public disclosure.

---

**From:** Terry Lewis  
**Sent:** Thursday, April 16, 2009 7:26 AM  
**To:** Kevin Vespia  
**Subject:** FW: Trap and Trace Confidentiality

let me know what u find

---

**From:** Kenneth Castro [mailto:Kenneth.Castro@sarasotagov.com]  
**Sent:** Wed 4/15/2009 11:25 AM  
**To:** Terry Lewis  
**Cc:** Tom Laughlin; Curt Holmes; Paul Sutton  
**Subject:** Trap and Trace Confidentiality

Good Morning Chief,

I just received a phone call from one of our detectives (Tom Laughlin) who is assigned to the U.S. Marshalls Task Force out of Tampa. He received a call from the ASA Craig Schaefer regarding some concerns. Schaefer advised him that they received a PCA regarding a **North Port PD Case 09-031066** in where the detective specifically outlined the investigative means used to locate the suspect. As you are aware for some time now, the US Marshalls and I believe FDLE have had equipment which enables law enforcement to ping a suspects cell phone and pin point his/her exact location in an effort to apprehend suspects involved in serious crimes. In the past, and at the request of the U.S. Marshalls, the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions we simply refer to the assistance as " received information from a confidential source regarding the location of the suspect." To date this has not been challenged, since it is not an integral part of the actual crime that occurred.

The ASA was not sure what agency your Detective Sinehth used that had the equipment that enabled him/her to locate his suspect. They were concerned as we all are, that by providing these specifics on a pca, could jeopardize future investigations attempting to locate fugitives. The Tampa Office of the US Marshalls was not involved in the case, and they are not aware of who was. If this is in fact one of your cases, could you please entertain either having the Detective submit a new PCA and seal the old one, or at minimum instruct the detectives for future cases, regarding the fact that it is unnecessary to provide investigative means to anyone outside of law enforcement , especially in a public document. Please note that I am passing information on to you, and I have not been able to confirm that the case or detective are affiliated with NPPD.

Thank You

Sgt. Ken Castro  
941-954-7093 Office  
941-915-3095 Cell

---

Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing. E-mail messages sent or received by City of Sarasota officials and employees in connection with official City business are public records subject to disclosure under the Florida Public Records Act.

# EXHIBIT NW1/7

Invoice from Harris Corporation to Wilmington, North Carolina, Police Department for purchase of \$93,625 of IMSI Catcher equipment (Jan. 15, 2014), released in response to public records request by the ACLU of North Carolina.



Harris Proprietary

Invoice	INV6779-04018
Date	1/15/2014
Page:	1

HARRIS CORP - WIRELESS PRODUCTS GROUP  
 P.O. BOX 9800, M/S R5-11A  
 MELBOURNE, FL 32902-9800  
 PH: 800-358-6297, FAX: 321-309-7437, wpg@harris.com

# Invoice

**Bill To:**  
 Wilmington Police Department  
 City of Wilmington  
 Accounts Payable  
 PO Box 1810  
 Wilmington NC 28402

FINANCED  
 1/15/14  
 JAN 27 2014

**Ship To:**  
 Wilmington Police Department  
 City of Wilmington  
 615 Bess Street  
 Wilmington NC 28401

DISCLOSURE OF THIS DOCUMENT AND THE INFORMATION IT CONTAINS ARE STRICTLY PROHIBITED BY FEDERAL LAW (18 U.S.C.) THIS DOCUMENT CONTAINS HARRIS TRADE SECRET AND CONFIDENTIAL BUSINESS OR FINANCIAL INFORMATION EXEMPT FROM DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT. THIS DOCUMENT MAY CONTAIN TECHNICAL DATA ACCORDING TO THE DEPARTMENT OF STATE, INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR), 22 CFR CHAPTER 1, SUBCHAPTER M, PARTS 123-130) AND THE DEPARTMENT OF COMMERCE, EXPORT ADMINISTRATION REGULATIONS (EAR), 15 CFR PARTS 730-774. THIS DOCUMENT AND THE INFORMATION IT CONTAINS MAY NOT BE EXPORTED OR SHARED WITH A FOREIGN NATIONAL WITHOUT VALID EXPORT AUTHORIZATION. BEFORE MAKING OR PERMITTING ANY DISCLOSURE OF THIS DOCUMENT OR THE INFORMATION IT CONTAINS, WHETHER IN FULL OR IN PART, HARRIS SHALL BE GIVEN TIMELY NOTICE AND THE OPPORTUNITY TO CHALLENGE SUCH DISCLOSURE UNDER APPLICABLE LAW.

Purchase Order No.		Customer ID	Salesperson	Shipping Method	Pmt Terms	Req Shlp Date	Harris Ord No.
316869		WSO-001	WPG3	BEST WAY	Net 30	7/14/2013	ORD6779-02349
Ordered	Shipped	B/O	Item Number	Description	Discount	Unit Price	Ext. Price
1	1		SRAY-II-HLS-UP 40269	StingRay II to HailStorm Upgrade Serial Number		\$72,000.00	\$72,000.00
1	1		2009523-101	Laptop PC "This \$3,500 valued Laptop PC is included in the cost of the StingRay II Upgrade"			\$0.00
1	1		HARPOON-DB-700-800 35175	Harpoon PA Kit - Dual Band 700/800 Upgr Serial Number		\$15,500.00	\$15,500.00

**Remit Payment To:**

<b>Electronic Funds Transfer (EFT):</b>	<b>GCSD Mail Deposits:</b>	<b>GCSD Overnight Deliveries:</b>
Harris Corporation, GCSD Citibank Delaware Philadelphia, PA Account No: 30523187 ABA Rtg No: 021000089	Harris GCSD P.O. Box 7247 - LB 6759 Philadelphia, PA 19170-6769	Harris GCSD - LB 6759 C/O Citibank Delaware Lockbox Operations 1815 Brett Road New Castle, DE 19720 Phone number: 302-323-3800

Please reference the invoice number with your payment. Harris Tax ID# 34-0276860

Subtotal	\$87,600.00
Deposit	\$0.00
Misc	\$0.00
Tax	\$8,125.00
Freight	\$0.00
Trade Discount	\$0.00
Purchase Price	\$93,825.00

# EXHIBIT NW1/8

State of New York Purchase Order for purchase of \$197,100 of IMSI Catcher equipment by New York State Police (Mar. 11, 2005), released in response to public records request by the New York Civil Liberties Union.

~~DONE~~ Raeve  
4/7/05

AG-130

## STATE OF NEW YORK PURCHASE ORDER

Orig. Agency Code	Date	RN:	Troop Number	Vendor: Show on all Bills and Correspondence		
01060	3/11/2005		HQ 8878	Contract No.	Com Group No	Document No
						05402

<b>Originating Agency:</b> New York State Police Finance - Bldg 22 1220 Washington Ave Albany, NY 12226-2252 Tax ID:	<b>Vendor TAX ID:</b> <div style="background-color: black; width: 100px; height: 40px; margin: 5px 0;"></div>	<b>Ship to:</b> <div style="background-color: black; width: 100px; height: 20px; margin: 5px 0;"></div> NY State Police, UNYRIC 630 Columbia Ave. Ext. Latham NY 12110
---	--	---

Item Number	Description	Qty	Unit	Price	Amount
	Cellular telephone tracking equipment per	0		\$0.0000	\$0.00
	Quote #QTE6779-00634 dated 2/3/05	1	lot	\$197,100.0000	\$197,100.00

**APPROVED**  
 DEPT. OF AUDIT & CONTROL  
 MAR 21 2005  
 FOR THE STATE COMPTROLLER

**Total:** \$197,100.00

Funding Source - Auto Theft Funds

Internal Use

P0 Number	Line	Act	Amount	Dept	Cost Center	Var	Yr	Object
05402	1	A	\$79,833.68	01	223721		04	57900
05402	2	A	\$117,266.32	01	227092		04	57900
05402	3		\$0.00	01				

The contract established by this purchase order is governed by Appendix A, Standard Clauses For All New York State Contracts, which is incorporated herein and made a part hereof, a copy of which is available on request. Vendor signifies acceptance of terms and conditions of Appendix A by delivery of the goods or services and/or by acceptance of payment.

All prices are FOB destination unless otherwise indicated.

**PLEASE FURNISH THE ABOVE ARTICLES**

CB: [REDACTED] Change Notice Attached  
 PA: [REDACTED] Troop Number  
 FA: [REDACTED] HQ 8878

\_\_\_\_\_  
 Authorized Signature

# EXHIBIT NW1/9

Harris Corporation, Wireless Products Group, KingFish®: Portable, Cellular Transceiver System and AmberJack®: Phased Array Direction Finding Antenna, released by Rochester, New York, Police Department in response to public records request by the New York Civil Liberties Union.

## **KingFish®** **Portable, Cellular Transceiver System**

### **Product Description**

KingFish® is a multiprotocol, cellular communications system from Harris' long line of advanced wireless products. The KingFish is a man-portable, single receiver, single transmitter platform capable of supporting multiple, cellular communication technologies. KingFish is based on a Software Defined Radio (SDR) architecture, which enables upgrades to future cellular standards, while preserving the initial investment in hardware. The KingFish currently supports GSM, CDMA2000® and iDEN™ protocols.

### **Features**

- SDR technology enables convenient field upgrades of software for future standards and capabilities.
- Intuitive Graphical User Interface (GUI)
- Collected data can be viewed or exported for post-processing data analysis.
- Low-power system designed for vehicular operation.
- Battery power designed for portable operation.



### **DISTRIBUTION WARNING**

This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).



# KingFish®

## Portable, Cellular Transceiver System



### Available Software Applications

- RayFish® GSM Controller
- RayFish CDMA2000 Controller
- RayFish iDEN Controller

### Operating Bands

- Cellular: 824–849 MHz, 869–894 MHz
- iDEN: 806–821 MHz, 855–866 MHz
- E-GSM 900: 880–915 MHz, 925–960 MHz
- DCS 1800: 1710–1785 MHz, 1805–1880 MHz
- PCS 1900: 1850–1910 MHz, 1930–1990 MHz
- AWS 2100: 1710–1755 MHz, 2110–2155 MHz (requires AWS converter accessory)

### Compatible Accessories

- PC Controllers
  - Ultra Mobile PC
  - Dell® Laptop
  - Panasonic Toughbook®
- AmberJack® Direction-Finding Antennas
- Harpoon® Power Amplifier (PA)
- 25-watt filtered PA
- AWS converter
- GPS kit
- Backpack

### Hardware Features

- External PA output
- DF antenna input
- DF Control/Status (interface with AmberJack DF antenna)
- Swappable Li-ion Battery
- Bluetooth® Connectivity

### Power Source

- DC power: 10–16 Vdc, <10 amps
- AC power: 90–132/180–264 Vac, 47 to 63 Hz

### Physical Characteristics

- Radio housing: Aluminum case
- Size: L = 11.5", W = 10", H = 3.5"
- Weight: 8 lbs.
- Wheeled transit carrying case



Specifications are subject to change without notice. Harris is a registered trademark of Harris Corporation. AmberJack, BlackFin II, FireFish, FishHawk, LoggerHead, Gossamer, Harpoon, KingFish, LoggerHead, Moray, Porpoise, RayFish, StingRay, and StingRay II are registered trademarks of Harris Corporation. DriftNet, FishFinder, LongShip, Octopus, and Scorpion are trademarks of Harris Corporation. CDMA2000 is a registered trademark of the Telecommunications Industry Association in the United States (TIA-USA). iDEN is a trademark of Motorola, Inc. Bluetooth is a trademark of Bluetooth SIG, Inc. Windows XP Professional is a trademark of Microsoft Corporation. Panasonic Toughbook is a registered trademark of Panasonic Corporation. Dell is a registered trademark of Dell Inc.

## DISTRIBUTION WARNING

**This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).**



Government Communications Systems Division | P.O. Box 9800 | Melbourne, FL USA 32902-9800  
1-800-358-5297 or [wpg@harris.com](mailto:wpg@harris.com) | [www.wpg.harris.com](http://www.wpg.harris.com) | [www.harris.com](http://www.harris.com)

## **AmberJack<sup>®</sup>** **Phased Array Direction Finding Antenna**

### **Product Description**

AmberJack<sup>®</sup> is a phased array direction-finding (DF) antenna accessory capable of providing lines of bearing to mobile phone users and base stations. The DF antenna array is designed to operate with Harris' StingRay II<sup>®</sup>, StingRay<sup>®</sup>, KingFish<sup>®</sup>, and Gossamer<sup>®</sup> products.

AmberJack combines Harris' expertise in phased array antenna technology and location based services to offer a state-of-the-art direction-finding system. Phased array technology offers a universal DF antenna for existing, as well as future cellular standards.

The DF antenna array incorporates magnetic mounts for easy installation on the roof of a vehicle and offers a low profile for reduced visibility.

### **Features**

- Interfaces with StingRay II, StingRay, and KingFish cellular support products.
- Enables graphical representation of mobile phone or base station location through line of bearing display.
- Weather resistant, rugged enclosure. Mountable inside or outside the vehicle.



### **DISTRIBUTION WARNING**

This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).

# AmberJack®

## Phased Array Direction Finding Antenna



### Frequency Coverage

- AmberJack-X (U.S. Cellular/PCS 1900)
  - Cellular reverse: 824–849 MHz
  - Cellular forward: 869–894 MHz
  - PCS reverse: 1850–1910 MHz
  - PCS forward: 1930–1990 MHz
- AmberJack-G (EGSM 900/DCS 1800)
  - EGSM reverse: 880–915 MHz
  - EGSM forward: 925–960 MHz
  - DCS reverse: 1710–1785 MHz
  - DCS forward: 1805–1880 MHz
- AmberJack-W (Wideband)
  - iDEN™ reverse: 806–825 MHz
  - iDEN forward: 851–870 MHz
  - Cellular reverse: 824–849 MHz
  - Cellular forward: 869–894 MHz
  - PCS reverse: 1850–1910 MHz
  - PCS forward: 1930–1990 MHz
  - EGSM reverse: 880–915 MHz
  - EGSM forward: 925–960 MHz
  - AWS reverse: 1710–1755 MHz
  - AWS forward: 2110–2155 MHz

### Compatible Software Applications

- RayFish® GSM Controller
- RayFish CDMA2000® Controller
- RayFish iDEN Controller

### Physical Characteristics

- Size: D = 17", H = 4.2"
- Weight: <14 lbs



Specifications are subject to change without notice. Harris is a registered trademark of Harris Corporation. AmberJack, FireFish, FishHawk, Gossamer, Harpoon, KingFish, LoggerHead, Moray, Porpoise, StingRay, and StingRay II are registered trademarks of Harris Corporation. BlackFin, DriftNet, FishFinder, LongShip, Octopus, RayFish, SideWinder, and Scorpion are trademarks of Harris Corporation. CDMA2000 is a registered trademark of the Telecommunications Industry Association in the United States (TIA-USA). iDEN is a trademark of Motorola, Inc. Bluetooth is a trademark of Bluetooth SIG, Inc. Windows XP Professional is a trademark of Microsoft Corporation.

## DISTRIBUTION WARNING

**This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).**



Government Communications Systems Division | P.O. Box 9800 | Melbourne, FL USA 32902-9800  
1-800-358-5297 or wpg@harris.com | www.wpg.harris.com | [www.harris.com](http://www.harris.com)

# **EXHIBIT NW1/10**

Agreement re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations, executed by Federal Bureau of Investigation and Milwaukee Police Department (Aug. 13, 2013), released in response to public records request by Mike Katz-Lacabe

COPY



COPY

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

August 13, 2013

David Salazar  
Captain  
Milwaukee Police Department  
P. O. Box 531  
Milwaukee, WI 53201

Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations

*LAW ENFORCEMENT SENSITIVE (LES): The information in this document is the property of the Federal Bureau of Investigation (FBI) and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI Operational Technology Division authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network.*

Dear Captain Salazar:

We have been advised by Harris Corporation of the Milwaukee Police Department's request for acquisition of certain wireless collection equipment/technology manufactured by Harris Corporation. Consistent with the conditions on the equipment authorization granted to Harris Corporation by the Federal Communications Commission (FCC), state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.

As you are aware, law enforcement agencies increasingly rely on wireless collection equipment/technology to conduct lawfully-authorized electronic surveillance. Disclosing the existence of and the capabilities provided by such equipment/technology to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings. Accordingly, the Milwaukee Police Department agrees to the following conditions in connection with its acquisition and use of the Harris Corporation equipment/technology:

1. By entering into this agreement, the Milwaukee Police Department affirms that it has statutory authority to lawfully employ this technology and will do so only in support of public safety operations or criminal investigations.
2. The Milwaukee Police Department assumes responsibility for operating the equipment/technology in accordance with Federal law and regulation and accepts sole liability for any violations thereof, irrespective of the Federal Bureau of Investigation approval, if any, for the sale of the equipment/technology.
3. The Milwaukee Police Department will ensure that operators of the equipment have met the operator training standards identified by the FBI and are certified to conduct operations.
4. The Milwaukee Police Department will coordinate with the FBI in advance of its use of the wireless collection equipment/technology to ensure de-confliction of respective missions.
5. The Milwaukee Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies.
6. The Milwaukee Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) provided to it to any other law enforcement or government agency without the prior written approval of the FBI. Prior to any approved distribution, dissemination, or comparable disclosure of any information concerning the wireless collection equipment/technology or any software, manuals, or related technical documentation related to such equipment/technology, all materials shall be marked "Law Enforcement Sensitive, For Official Use Only - Not to be Disclosed Outside of the Milwaukee Police Department."

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

7. The Milwaukee Police Department shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI. If the Milwaukee Police Department learns that a District Attorney, prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology in a manner that will cause law enforcement sensitive information relating to the technology to be made known to the public, the Milwaukee Police Department will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.

Notification shall be directed to the attention of:

Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

8. In addition, the Milwaukee Police Department will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology. This point supposes that the agency has some control or influence over the prosecutorial process. Where such is not the case, or is limited so as to be inconsequential, it is the FBI's expectation that the law enforcement

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

agency identify the applicable prosecuting agency, or agencies, for inclusion in this agreement.

9. A copy of any court order in any proceeding in which the Milwaukee Police Department is a party directing disclosure of information concerning the Harris Corporation equipment/technology and any associated software, operating manuals, or related documentation (including its technical/engineering description(s) and capabilities) will immediately be provided to the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise. Any such court orders shall be directed to the attention of:

Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

10. The Milwaukee Police Department will not publicize its acquisition or use of the Harris Corporation equipment/technology or any of the capabilities afforded by such equipment/technology to the public, other law enforcement agencies, or other government agencies, including, but not limited to, in any news or press releases, interviews, or direct or indirect statements to the media.
11. In the event that the Milwaukee Police Department receives a request pursuant to the Freedom of Information Act (5 U.S.C. § 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities), the Milwaukee Police Department will immediately notify the FBI of any such request telephonically and in writing in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels. Notification shall be directed to the attention of:

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE


The Milwaukee Police Department's acceptance of the above conditions shall be evidenced by the signatures below of an authorized representative and wireless collection equipment operators of the Milwaukee Police Department.


Sincerely,


  
Amy S. Hess  
Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation

Acknowledged and agreed to this 8-29- day of 2013.


  
David Salazar  
Captain  
Milwaukee Police Department  
Milwaukee, WI


  
William S. LaFleur  
Lieutenant of Police


  
Brian P. Brosseau  
Police Officer

  
Eric Draeger  
Police Officer

  
Christopher Heidemann  
Police Officer

  
William Schroeder  
Police Officer

  
Eric Donaldson  
Detective

  
Brett Huston  
Detective

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

# **EXHIBIT NW1/11**

Harris Corporation, Non-Disclosure Agreement with City of Tucson, Arizona (June 7, 2010), released by Tucson Police Department in response to public records request by journalist.

**Non-Disclosure Agreement (NDA)  
Harris Corporation, GCSD  
Wireless Products Group (WPG)/Wireless Solutions**

[Effective Date: 6/7/10]

In order to protect certain Harris Corporation developed "Title 18" Protected Products, (hereinafter called "Products,") both HARRIS CORPORATION, a Delaware Corporation, through its GCSD Division ("HARRIS") and the City of Tucson mutually agree as follows:

1. The Products protected under this NDA include, but are not limited to the following:

WPG Title 18 USC Restricted Products	
RayFish® Core Hardware Platform	
KingFish®	X
SlingRay®	X
SlingRay IR®	X
RayFish® Core Software	
GSM Transceiver	X
GSM SlingRay II® Transceiver	X
CDMA Transceiver	X
iDEN Transceiver	X
RayFish® Accessory Hardware	
Map Router	X
RayFish® Core	
Band IV Converter - AWS (2100/1700)	X
RayFish®	
RayFish® Power Kit	X
AmberJack® DP Antenna	X
RayFish® Amplifier	
Broadband Amplifiers	X
Harpoon™ Amplifiers	X
Harpoon™	
Gossamer®	X
Gossamer® DP Kit	X
Harpoon™	
Lanterneye	X
Tarpon®	X
Wireless Antenna	
Moray®	X

2. Harris Corporation's Government Communications Systems Division, Wireless Products Group (hereinafter, "Harris") provides a number of tools, equipment and capabilities, both hardware and software (hereinafter "Products"), that provide users a capability to locate targets of interest. These Products are restricted and other wise controlled under United States Code, Title 18, and by other governing policies, regulations and laws.

Missions utilizing in whole or in part the Harris Products are covered in their entirety by this NDA.

The City of Tucson is subject to this NDA and except for Court ordered or other judicially mandated disclosures, will not disseminate, publish or release any information about the operations, missions, equipment, CONOPS, mission or investigation results, methods or any other information related to or arising out of the use, deployment or application of the Products that would be deemed a release of technical data as is described and agreed to under this NDA. In the event of a court ordered or judicially mandated disclosure, the City of Tucson shall use its best efforts to make such disclosure in a manner that provides maximum protection of the information to be disclosed. Agency shall promptly notify Harris upon receipt of such order or mandate and provide a copy of any such written order or mandate.

Further, City of Tucson personnel may be exposed to additional Harris WPG equipment to which it may not have direct access, such as might be used by a federal partner to assist the City of Tucson and its personnel in performance of their duties. The City of Tucson understands that such exposure is also covered by this NDA and that it shall neither disclose its knowledge of such missions, equipment, CONOPS, mission or investigation results, methods or any other information that would be deemed a release of technical data as is described and agreed to under this NDA, nor will the City of Tucson or its personnel demand direct access to such Products through direct or indirect pursuits or inquiries to gain access to such restricted equipment.

Further, the City of Tucson will ensure the operation of Harris Products will be restricted to only those personnel permanently assigned to department sections tasked with completing electronic surveillance missions. Authorized personnel should be sworn members who possess arrest authority, but may include full-time civilian employees permanently assigned to the same department sections tasked with supporting electronic surveillance missions.

3. The City of Tucson shall not discuss, publish, release or disclose any information pertaining to the Products covered under this NDA to any third party individual, corporation, or other entity, including any affiliated or unaffiliated State, County, City, Town or Village, or other governmental agency or entity without the prior written consent of Harris and shall further limit the circulation and disclosure of information regarding the Products within its own organization to its employees or agents having a "need to know" about the Products and shall ensure that they are informed of the sensitive nature thereof and agree to and are required to observe the provisions of confidentiality set forth herein and under Title 18 of the U.S. Code.

The City of Tucson is subject to the Arizona Public Records Law, A.R.S. sec. 39-121, et seq. While the City will not voluntarily disclose any Protected Product, in the event that the City receives a Public Records request from a third party relating to any Protected Product, or other information Harris deems confidential, the City will notify Harris of such a request and allow Harris to challenge any such request in court. The City will not take a position with respect to the release of such material, beyond its contractual duties, but will assist Harris in any such challenge.

4. This Agreement shall be binding upon the parties, their successors, and assignees. Neither party shall assign this Agreement nor any Product received from Harris pursuant to this Agreement without Harris' prior written consent.
5. This Agreement shall be governed by, subject to, and construed in accordance with the laws of the State of Arizona. Jurisdiction and venue shall lie in the State of Arizona, Pima County, for all causes of actions arising under this Agreement.
6. Removal of any Product listed herein from the restrictions under Title 18 of the U.S. Code in no way affects, voids or invalidates this Agreement, it being the intent of the Parties to treat this Agreement as enforceable notwithstanding such removal. Protection of all other Products herein remain in full force and effect.

Agency Representative (Department or Division Head):

End User:

City of Tucson

Agency Organization

Laura Gesting

Name

Contract Administrator

Title

6-9-10

Date

End User Organization

Name

Title

Date

Harris Corporation, Government Communications Systems Division:



Name QJ

Sr. Contract Admin.

Title

6/10/10

Date

# **EXHIBIT NW1/12**

Log of Tallahassee, Florida, Police Department's uses of IMSI Catchers, 2007- 2014, released in response to public records request by the ACLU.

Date	Track	Exigent	Incident Type	Agency	Location	Agency Case Number	Court Case Number	Target #	Order Status	Sealed
9-6-07 (?)	X		Wanted Person	USMS	400 Blk Macomb St.	N/A		UNKNOWN	Exigent/Consent	
9/14/2007	X		Wanted Person	TPD/USMS	Chatahoochee, FL	07-27677	08-CF-684	(850) 544-████	Court Order	X
10/9/2007	X	X	Homicide	TPD/LCSOWCSO	Wakulla, FL	07-32767		(850) 766-████	Exigent/Consent	
10/26/2007	X		Drug Trafficking	TPD	679 W. Tennessee St.	07-34842	07-CF-3988	(850) 264-████	Court Order	X
11/2/2007	X	X	Abduction	LCSO	See LCSO report	LCSO 07251052		UNKNOWN	Exigent/Consent	
1/10/2008	X	X	Robbery Just Occurred	TPD	1410 CCNE Majestic Dr.	08-001032	13-CF3120 OPEN	(850) 591-████	Exigent/Consent	X
1/18/2008	X		Grand Theft	TPD	2408 Surrey Street JacksonBluff	08-001872		(850) 727-████	Court Order	
2/13/2008	X		Wanted Person	TPD	Gaines St. Area	07-021774		(850) 728-████	Unable to Locate	
2/15/2008	X		Wanted Person	TPD	S. Leon County			(850) 727-████	Unable to Locate	
3/7/2008	X	X	Sex Battery/Grand Theft	TPD	Fleetwood Dr.	08-007662		(850) 241-████	Exigent/Consent	
4/25/2008	X	X	Robbery Just Occurred	TPD	3535 Apalachee Pkwy	08-013406		(561) 843-████	Exigent/Consent	
4/25/2008	X	X	Robbery Just Occurred	TPD	7535 W. Tennessee St.	08-013421		(239) 293-████	Exigent/Consent	
4/25/2008	X	X	Robbery Just Occurred	TPD	Majestic Dr.	08-013508		(850) 510-████	Exigent/Consent	
4/25/2008	X	X	Robbery Just Occurred	TPD	Wilson Green	08-013276/013508	08-CJ-494	(850) 980-████	Court Order	X
4/29/2008	X	X	Armed Robbery/Purstui	TPD	Brighton Rd.	08-014038		(786) 426-████	Exigent/Consent	
5/7/2008	X	X	Homicide	TPD/FDLE	Various	08-015078		(727) 403-████	Exigent/Consent	
5/7/2008	X	X		TPD/FDLE		08-015078	08-CF--1081; 08- CF-1682	(850) 241-████	Exigent/Consent	
5/7/2008	X			TPD/FDLE		08-015078		(720) 934-████	Court Order	X
5/21/2008	X		Wanted Person	Marshall's	North Monroe St.	WCOS# 04ARR003071		(850) 509-████	Court Order	X
5/28/2008	X	X	911 Hangup	Wakulla SO	Wakulla Station			(904) 235-████	Exigent/Consent	
5/29/2008	X		Wanted Person	TPD/TFD	Lakeshore Dr.	08-016481	08-CF-1920	(850) 443-████	Court Order	X
6/12/2008	X	X	911 Hangup	TPD	Pecan Rd.			(561) 449-████	Exigent/Consent	
7/20/2008	X	X	ATM Burglary	FDLE	Thomessville Rd.	FDLE		(850) 510-████	Exigent/Consent	
7/22/2008	X	X	Missing Juvenile	LCSO	Mahan Drive	LCSO # 08- 167562			Exigent/Consent	
7/23/2008	X	X	Abducted Person	LCSO	Great Value Inn - N. Monroe St.				Exigent/Consent	
8/12/2008	X	X	Homicide	TPD	South City	08-026075	08-CF-2902	(850) 274-████	Court Order	X
	X		Robbery/Kidnapping				08-CF-3895; 08- CF-3890	(850) 727-████	Court Order	X
8/13/2008						08-025267	08-CF-3102	(850) 728-████	Court Order	X
							09-CF-129	(954) 243-████	Court Order	X
							09-CF-128	(850) 264-████	Court Order	X
8/27/2008	X		Robbery/Kidnapping			08-025267	08-CF-3102 OPEN	(954) 558-████	Court Order	X
9/4/2008	X		Bank Robbery	LCSO	Pryor Rd. / Old Bainbridge	LCSO #08-205743	08-CF-3191	(850) 727-████	Court Order	X
9/13/2008	X	X	Sexual Battery	TPD	Pensacola/White	08-029677		(941) 400-████	Exigent/Consent	
9/16/2008	X		Homicide	TPD	Floral St.	08-029997	09-CF-52	(850) 294-████	Court Order	X
9/23/2008	X	X	Commercial Robbery w/Firearm	TPD	1701 W. Tennessee St.	08-031048		(850) 294-████	Exigent/Consent	
10/1/2008	X		Serial Bank Robbery	TPD	2402 Quazar Circle	09-004241	09-CR-30-RH	(850) 459-████	Court Order	X
10/28/2008	X	X	Commercial Robbery	TPD	N. Monroe St.	08-035137	USDC	(850) 241-████	Exigent/Consent	
11/6/2008	X	X	Burglary, Sex Battery, Kidnapping	Coral Springs PD	Paul Russell/S. Monroe			(954) 461-████	Exigent/Consent	
11/14/2008	X	X	Home Invasion Robbery	TPD	2616 Mission Rd. #12	08-037256		(850) 459-████	Exigent/Consent	
11/20/2008	X	X	Home Invasion Robbery	TPD	2125 Jackson Bluff Rd.	08-038009		(813) 508-████	Exigent/Consent	
12/4/2008	X		Robbery	TPD	2424 W. Tharpe St.	08-038361 08-039527	08-CF-4169	(850) 212-████	Court Order	X



1/10/2009	X	X	Home Invasion Robbery	TPD	568 Beverly Ct	09-001006		(850) 524-████	Exigent/Consent	
1/17/2009	X	X	Robbery	TPD	313 Arden Rd.	09-001705		(850) 524-████	Exigent/Consent	
1/21/2009	X		Burglary	FDLE	Pensacola, Florida	FDLE			No Copy on File w/TPD	
2/6/2009	X		Fraud	TPD	2011 N Monroe Street	09-003461	09-CF-400	(850) 264-████	Court Order	
2/9/2009	X	X	Armed Sex Batt Fugitive	TPD	153 Belmont Dr.	09-003611		(850) 264-████	Exigent/Consent	
2/11/2009	X		Poss W/T/S, Poss Firearm by CF	TPD	2855 Apalachee Pkwy	08-042029	09-CF-563	(904) 537-████	Court Order	
2/13/2009	X		Sale of Controlled Sub.	TPD	446 Mercury Drive	09-004906		(850) 210-████	Court Order	
2/18/2009	X		USMS -Wanted Person	TPD	2405 Jackson Bluff Road	09-005628	09-CF-756	(850) 284-████	Court Order	
2/26/2009	X		USMS-Wanted Person	TPD/USMS	8010 Blacklack Rd	USMS #09-44456	07-CF-2031	(850) 241-████	Court Order	
3/6/2009			Serial Burglary	TPD	1838 E Wagon Wheel Circle	USDC	09-CR-7-RH	(850) 284-████	Court Order	
3/6/2009	X					09-006935	09-CF-801	(904) 536-████	Court Order	
3/6/2009	X						09-CF-802	(904) 887-████	Court Order	
3/6/2009	X							(904) 487-████	Number listed on multi-number order	
3/6/2009	X	X	Abduction	TPD	1210 Francisco Drive	09-006949	NONE	(850) 443-████	Court Order	
3/13/2009	X		Sexual Battery	TPD	3100 Apalachee Pkwy 21	09-006909	09-CF-859	(850) 508-████	Court Order	X
4/1/2009	X	X	Home Invasion Robbery	TPD	1554 Lake Ave #107	09-009756		(850) 251-████	Exigent/Consent	
4/1/2009	X	X	Murder	LCSSO		LCSSO- Rabon		(850) 728-████	Exigent/Consent	
4/16/2009	X	X	Missing Endangered Infant	GCSSO	Cairo, GA			(850) 210-████	Exigent/Consent	
5/1/2009	X	X	Stalking	TPD	1089 Sutor Rd.	09-009900		(850) 274-████	Exigent/Consent	X
5/14/2009	X		Shooting	TPD	1805 North Monroe Street	09-014987	09-CF-1630	(850) 692-████	Court Order	X
6/1/2009	X		Homicide		FL Gaines, GA			(850) 508-████	No Copy on File w/TPD	X
6/12/2009	X	X	Attempted Homicide	TPD	275 John Knox Rd	09-017699		(850) 591-████	Exigent/Consent	
6/12/2009	X	X	Suicide/Sexual Battery	TPD	3818 Leane drive	09-017761		(850) 524-████	Exigent/Consent	
6/18/2009	X		Home Invasion Robbery	TPD	1112 South Magnolia Dr	09-018345	08-CF-2032; 08-CF-2216; 08-CF-2026	(850) 524-████	Court Order	
6/25/2009	X		Bank Robbery	TPD	1700 North Monroe Street	09-019059	09-CF-2200	(850) 322-████	Court Order	X
7/9/2009	X		Bank Robbery	TPD	3000 S. Adams St.	09-019059	09-CF-2251	(863) 513-████	Court Order	
7/20/2009	X		Bank Robbery	TPD	Sawtooth Dr.	09-019059	09-CF-2466	(305) 890-████	Court Order	
8/3/2009	X	X	Armed Robbery	TPD	1619 Lake Ave.	09-023267		(850) 228-████	Exigent/Consent	
8/9/2009	X	X	Strong Arm Robbery	TPD	2020 West Pensacola Street	09-2387/1-09-023866		(850) 459-████	Exigent/Consent	
8/13/2009	X	X	Armed Robbery	TPD	218 Bragg Dr	09-024260		(850) 508-████	Exigent/Consent	
8/25/2009	X		Wanted Person	USMS	Wakulla County	WCSSO # 090FF001960		(352) 317-████	Court Order	
8/31/2009	X	X	Home Invasion Robbery	TPD	2614 West Tennessee Street	09-026361		(850) 879-████	Exigent/Consent	
12/15/2009	X		Murder - Witness Track	USMS-TPD	1609 Rawhide Ct	09-038546	07-CF-1809; 08-CF-3906	(850) 710-████	Court Order	X
1/5/2010	X		Wanted Person	TPD/USMS	223 Ayers Court	09-21533	09-CF-4234	(561) 207-████	Court Order	X
1/20/2010	X		Sexual Battery	TPD	1325 W. Tharpe St/ Magnolia & Parkway	10-1773 (TPD)	NONE	(850) 545-████	Court Order	X
2/19/2010	X	X	Home Invasion Robbery	TPD	5423 Appledore Dr.	10-005029		(850) 694-████	Exigent/Consent	
2/24/2010	X		Homicide	TPD	Shallow Brk Dr.	10-1469		(954) 330-████	Missing	
4/14/2010	X	X	Burglary/Robbery/Agg Assault	TPD	2001 Old St. Augustine Rd.	TPD # 10-009687		(850) 321-████	Exigent/Consent	
5/19/2010	X	X	Serial Sexual Battery	TPD/FDLE/LCSSO	Killearn/TLH	10-014734		(850) 524-████	Exigent/Consent	
6/7/2010	X		Attempted Murder	TPD	1425 Nashville Drive	10-12590	10-CF-1348	(850) 408-████	Court Order	X
8/14/2010	X		Wanted Person	TPD/USMS	2521 Saxon St.	10-025221	10-CF-2668	(850) 272-████	Court Order	X
8/24/2010	X		Homicide	USMS/TPD/FDLE	Decatur Co. GA	USMS		(478) 278-████	Court Order	X
8/27/2010	X		Burglary/Theft/Agg Ass LEO	LCSSO/TPD/FDLE	Various- ATM Thefts	USMS		(850) 228-████	Court Order	X
8/27/2010						LCSSO #09-231282		(850) 210-████	Number listed on multi-number order	X
8/27/2010								(850) 251-████	Number listed on multi-number order	X



1/21/2012	X	X	Robbery/Kidnapping	TPD	700 Paul Russel Dr.	12-1857			(850) 339	Exigent/Consent	
	X	X							(850) 294	Exigent/Consent	
1/23/2012	X		Grant Theft Auto	TPD	Holton St.	12-1089	12-CF-196		(850) 570	Court Order	X
2/9/2012	X		Wanted Person / Armed Robbery	FDLE		N/A			N/A	No Copy on File w/TPD	
2/13/2012	X		Wanted Person	TPD/USMS	2626 Hastings Dr.	12-4210	12-CF-904		(850) 363	Court Order	X
2/15/2012	X		Wanted Person	TPD/USMS	103 Elm Ave. Havana, FL	11-28120	12-CF-407		(850) 345	Court Order	X
2/29/2012	X	X	Stabbing/Sex Batt	LCSO	Hannava, FL	LCSO				Exigent/Consent	
3/13/2012	X		Wanted Person - VOP Armed Burg	TPD	808 Annawood Dr. TLH	12-11744	09-CF-2559		(850) 727	Court Order	X
	X								(850) 322	Court Order	
5/1/2012	X								(850) 339	Court Order	
3/13/2012	X		Drug Investigation	TPD	Stone Rd.	12_3490	12-MM-1078		(850) 241	Court Order	X
3/14/2012	X		Wanted Person - Poss Firearm by CF, Felony Battery	TPD	2855 Apalachee Pkwy	12-5477	12-CF-770		(850) 284	Court Order	X
3/21/2012	X	X	Suicidal/Homicidal Threats	TPD	234 E. 7th Ave.	TPD IB 12-28			(850) 345	Exigent/Consent	
3/22/2012	X	X	Home Invasion Robbery	TPD	2421 Jackson Bluff Rd.	12-7687			(386) 679	Exigent/Consent	
3/24/2012	X	X	Missing/Endangered Adult	TPD	1472 Mitchell Ave.	12-7978			(210) 563	Exigent/Consent	
4/2/2012	X	X	911 Call / Domestic Battery	TPD					(850) 556	Exigent/Consent	
4/9/2012	X	X	Suicidal Person	TPD					(352) 870	Exigent/Consent	
4/10/2012	X	X	Armed Robbery	TPD					(803) 445	Exigent/Consent	
4/10/2012	X		Suicidal Person	TPD					(850) 212	Court Order	X
4/16/2012	X		Att. Homicide	TPD					(850) 274	Court Order	X
4/16/2012	X		Sexual Battery/Wanted Person	TPD	1533 N. Monroe St.	12-8813	12-CF-189		(850) 212	Court Order	X
4/16/2012	X		Attempt Murder/Wanted Person	USMS/TPD/GA	1847 Rodrigue Rd.	12-10311	12-CF-1239		(850) 274	Court Order	X
4/20/2012	X		Bank Robbery	LCSO/USMS					(850) 322	Court Order	X
4/27/2012	X		Wanted Person -	LCSO/USMS					(850) 284	Court Order	X
4/30/2012	X	X	Suicidal Person	TPD	2609 Texas St.		12-CF-110; 12-CF-849; 12-CF-1352		(850) 322	Exigent/Consent	
5/3/2012	X	X	Abduction/Car Jacking	TPD						Exigent/Consent	
	X	X								Exigent/Consent	
5/7/2012			Wanted Person Agg Batt/Burg/Ghett	TPD/USMS/LCSO	1700 Joe Louis St.	LCSO 120149754	12-CF-1234; 12-CF-1673		(850) 226	Court Order	X
5/31/2012	X		Home Invasion Robbery	TPD	1560 High Rd.	12-14480	12-CF-1439; 12-CF-1440		(850) 284	Court Order	X
6/19/2012	X		Homicide	TPD	1610 Lake Ave.	12-16287	12-CF-1956		(561) 654	Exigent/consent	X
6/21/2012	X		Agg Stalking/Burg Occ Dwelling/Crim Misch	TPD	2421 Jackson Bluff Rd.	12-16321	12-CF-1966		(407) 770	Court Order	X
7/5/2012	X		Internet solicitation/traveling to meet minor	TPD	234 E. 7th Ave.	12-017696	12-CF-2186		850-384	Court Order	X
7/5/2012	X		Failure to Register as a Sexual Predator	TPD			12-CF-1184		(850) 591	Court Order	X
7/26/2012	X		Burg/Person Assaulted / Agg Batt / Depr 911	TPD	2702 N. Monroe St.	12-19799	12-CF-2403		(850) 212	Court Order	X
8/5/2012	X		Attempted Homicide/Armed Robbery	TPD	2415 N. Moore St.	12-20684	12-CF-2513		(850) 345	Court Order	X
8/20/2012	X		Wanted Person - Fel Batt/VOP Agg Ass	LCSO/TPD/USMS	644 Ridge Rd.	LCSO 120169592	12-CF-2668; 12-CF-863		(850) 408	Court Order	X
8/29/2012	X		Wanted Person -	TPD/USMS	604 Laura Lee Ave.	12-23260	12-CF-2640		(850) 345	Court Order	X
8/29/2012	X		Wanted Person	LCSO/USMS	3300 Crump Rd.	LCSO 120169673	12-CF-3230		(850) 570	Court Order	X
10/2/2012	X		Wanted Person	USMS/TPD/LCSO			12-CF-3275		(229) 977	Court Order	X
10/8/2012	X		Wanted Person	SAO/TPD/LCSO	2740 W. Tharpe	11-84816	12-CF-1348		(850) 544	Court Order	X
10/11/2012	X	X	Homicide	TPD		12-27521	12-CF-3405		(850) 619	Court Order	X
10/22/2012	X		Wanted Person	LCSO/USMS	Cobblestone Ln.	LCSO 120203927	12-MM-5404		(850) 320	Court Order	X
							WARRANT				

10/19/2012	X		Robbery - Forgery	TPD	2421 Jackson Bluff Rd.	12-27833	TPD OPEN	(772) 940-████	Court Order	X
10/29/2012	X		USMS Wanted Person	TPD	2501 S. Meridian Rd.	12-26838	INACTIVE	(850) 459-████	Court Order	X
10/29/2012	X		USMS Wanted Person	TPD	2849 Apalachee Parkway	12-28495	12-CF-3524	(850) 694-████	Court Order	X
11/1/2012	X		Homicide	TPD	4495 Shelter Rd.	12-29501	12-CF-3813	(850) 509-████	Court Order	X
11/7/2012	X		USMS Wanted Person	TPD	1293 C Rumba Lane	12-19760	OPEN	(850) 544-████	Court Order	X
11/9/2012	X		USMS Wanted Person	LCSCO/TPD/USMS		LCSCO 12-213895	12-CF-3864	(850) 590-████	Court Order	X
11/10/2012	X	X	Suicidal Person	TPD	830 E. Park Ave			(850) 544-████	Exigent/Consent	
11/13/2012	X		USMS Wanted Person	TPD	Marianna, FL	12-16681	12-CF-2048	(850) 557-████	Court Order	X
11/13/2012	X		USMS Wanted Person	TPD	1107 Basin St.	12-30101	12-CF-3681	(850) 345-████	Court Order	X
11/13/2012	X		USMS Wanted Person	TPD	3535 Roberts Ave.	12-27156	OPEN	(850) 274-████	Court Order	X
11/13/2012	X		USMS Wanted Person	TPD	2074 Midyette	12-29738	12-CF-3682	(305) 502-████	Court Order	X
11/20/2012	X		Armed Robbery	TPD	1327 Volusia St.	12-31242	TPD OPEN	(850) 524-████	Court Order	X
11/29/2012	X		Wanted Person	TPD	2305 Amelia Cir.	12-32067	INACTIVE	850-212-████	Court Order	X
11/29/2012	X	X	Robbery	TPD		12-30971	11-CF-3869	(850) 284-████	Exigent/Consent	
12/1/2012	X		Domestic Battery	Gretna, PD	Gretna, FL				No Copy on File w/TPD	
12/4/2012	X		Wanted Person	USMS/TPD		12-33158	120CF04010	(850) 264-████	Court Order	X
Dec-12	X		Burglary	TPD	2309 Old Bainbridge Rd.	12-33321		(305) 761-████	Exigent/Consent	
1/4/2013	X		USMS Wanted Person	LCSCO/USMS	3535 Roberts Ave.	LCSCO 12-220020	12-CF-3974; 12-CF-3893	(470) 244-████	Court Order	X
1/9/2013	X		Robbery Spree	TPD	Multiple Locations	13-1362	13-CF-462	(850) 284-████	Court Order	X
1/13/2013	X		Home Invasion / Shooting Incident	LCSCO/TPD	Misty Garden	LCSCO #13-7498	13-CF-618	(786) 479-████	Court Order	X
1/29/2013	X		Wanted Person	TPD/USMS	10416 Rase Rd	LCSCO # 13-0018190	10-CF-3236	(850) 519-████	Court Order	X
1/30/2013	X		Wanted Person	WCSCO/USMS	1525 W. Tennessee St	FDLE # 130018946		(850) 694-████	Court Order	X
1/31/2013	X		Home Invasion Robbery	GCSCO/FDLE					No Copy on File w/TPD	
2/5/2013	X		Wanted Person	TPD/USMS	Motel 6- 2738 N Monroe St	13-2635	07-CF-2875	(850) 321-████	Court Order	X
2/13/2013	X	X	Missing/Endangered Juvenile	TPD	1380 Ocala Rd.	13-3971	13-CF-414	(850) 303-████	Exigent/Consent	
2/13/2013	X		Home Invasion Robbery	TPD	222 S. Ocala Rd.	13-2635	OPEN	(850) 345-████	Court Order	X
2/16/2013	X		Robbery	TPD	1706 W. Tennessee St	13-4269	13-CF-765	(850) 321-████	Court Order	X
2/20/2013	X		Armed Robbery	FAMU/TPD	FAMU Campus	FAMU		(850) 345-████	Court Order	X
2/28/2013	X		USMS wanted person	LCSCO/USMS	Nekoma Ct.	LCSCO #13-20596	13-CF-637	(850) 597-████	Court Order	X
3/5/2013	X		Armed Robbery	TPD	4200 W. Tennessee St.	13-5766	13-CF-750	(850) 933-████	Court Order	X
3/14/2013	X		Drug Investigation linked to Shooting	TPD	2020 W. Pensacola St	13-5641	OPEN	(850) 363-████	Court Order	X
3/14/2013	X		USMS Wanted Person	WCSCO/USMS	3905 Cates Ave.	WCSCO 13OFF00342	13-MM-1019	(786) 691-████	Court Order	X
3/20/2013	X		Homicide	TPD	Magnolia/Parkway		13-CF-905	(850) 509-████	Court Order	X
3/20/2013	X						OPEN	(954) 729-████	Court Order	X
3/20/2013	X							(850) 241-████	Court Order	X
3/20/2013	X							(321) 246-████	Court Order	X
3/20/2013	X							(850) 321-████	Court Order	X
3/20/2013	X							(850) 510-████	Court Order	X
3/20/2013	X							(850) 567-████	Court Order	X
3/20/2013	X		Armed Robbery	TPD	4100 Blk. Bradford Rd.			(850) 661-████	Exigent/Consent	
3/22/2012	X		Sexual Battery	TPD	770 Appleyard Dr	13-7341	13-CF-907	(850) 228-████	Court Order	X
4/11/2013	X		Financial Crimes	TPD	234 East 7th Ave	13-8442	OPEN	(305) 684-████	Court Order	X

4/17/2013	X		Solicitation of Minor	TPD/CAC	234 East 7th Ave	13-9979	13-CF-1255	(850) 509	Court Order	X
4/17/2013	X		Solicitation of Minor	TPD/CAC	234 East 7th Ave	13-9789	13-CF-1257 OPEN	(850) 345	Court Order	X
4/19/2013	X		Wanted Person - Sex Batt 11yo vic	USMS		USMS			No Copy on File w/TPD	
4/23/2013	X		Missing/Endangered Child	TPD	2708 Rockbrook Dr.	13-10567	NONE	(850) 459	Court Order	X
4/25/2013	X		Armed Robbery/Attempt Homicide	TPD	600 Dixie Dr.	13-10718	13-CF-1373 OPEN	(850) 702	Court Order	X
4/28/2013	X		USMS-Wanted Person	FDLE/USMS	1700 Joe Louis St. 45	N/A			No Copy on File w/TPD	
5/10/2013	X		Robbery	TPD	Jewelry Store-1950 Thomasville Rd.	13-8783/13-12178	13-CF-1585 OPEN	(850) 443	Court Order	X
5/13/2013	X		USMS-Wanted Person	LCSO/USMS		USMS	02-CF-115	(786) 325	Court Order	X
5/17/2013	X		Homicide	TPD	2808 Whanish Way	13-12829	13-CF-1647 OPEN	(850) 567	Court Order	X
5/22/2013	X	X	USMS-Wanted Person	TPD	Tampa, FL	13-11125		(813) 279	Exigent/Consent	
5/25/2013	X	X	Homicide	TPD	2125 Passo St.	13-13576	13-CF-1757	(850) 727	Court Order	X
5/26/2013	X		Sexual Battery	TPD	415 Chapel Dr.	13-13604		(904) 509	Exigent/Consent	
6/4/2013	X	X	Homicide	TPD	Poppy St/Osceola St.		TPD OPEN INACTIVE	(850) 408	Exigent/Consent	
6/6/2013	X		Wanted Person - Attempted Homicide	TPD	2501 S. Meridian Rd	13-13676	13-CF-1840 OPEN	(850) 980	Court Order	X
6/21/2013	X		Home Invasion Robbery	TPD	2042 Belle Vue Way	13-15950	TPD OPEN INACTIVE	(850) 339	Court Order	X
6/26/2013	X		Homicide	TPD	2525 Texas Street		13-CF-1597 13-CF-2123 13-CF-2125 OPEN	(850) 251 (850) 345 (850) 591	Court Order	X
7/9/2013	X	X	Abduction	LCSO/FDLE	Madison County	LCOS		(850) 345	Court Order	X
7/9/2013	X	X	Attempted Homicide	WCOS/FDLE	Chipley	WCOS		(850) 251	Exigent/Consent	
7/10/2013	X		Wanted Person-Robbery	TPD	2325 W Pensacola St	13-1256	13-CF-2276 OPEN	(850) 544	Court Order	X
7/15/2013	X		Robbery	TPD	2325 W Pensacola St	13-1256	13-CF-2276 OPEN	(850) 743	Court Order	X
8/7/2013	X		Online Solicitation	TPD	234 East 7th Ave	13-20044	13-CF-2550 OPEN	(850) 481	Court Order	X
8/19/2013	X		Wanted Person	LCSO/TPD/USMS	2502 Holton St.#H1256	SO 130125880	13-CF-2599	(904) 566	Court Order	X
8/20/2013	X		Homicide	TPD	400 FAMU Way		13-CF-2836 OPEN	(850) 597	Court Order	X
8/22/2013	X		Kidnapping Investigation	TPD	1600 Old Bairnbridge Rd		13-CF-2749 OPEN	(850) 688	Court Order	X
9/14/2013	X		Sex Battery- Suspect 24 Victim: 16-17	TPD	W Tharpie St/Ocala Rd	13-19171	13-CF-2968 OPEN	(850) 545	Court Order	X
9/14/2013	X	X	Missing Juvenile	TPD	Crowder/N. Monroe St.	13-23673		(850) 212	Exigent/Consent	
9/27/2013	X		VOP-Occupied Burglary	TPD	2711 Allen Rd	13-24635	10-CF-2484	(850) 459	Court Order	X
10/8/2013	X		Wanted Person	TPD/LCSO/USMS	4495 Shelter Rd.	SO 130510309	13-CF-2951 OPEN	(850) 294	Court Order	X
10/9/2013	X		Homicide	USMS/ECOS/ESST	Pensacola	N/A		(904) 982	No Copy on File w/TPD	
10/14/2013	X		Wanted Person	TPD	Saxon St/Manatee St	13-26929	13-CF-2326	(850) 933	Court Order	X

10/16/2013	X	X	Suicidal Person	TPD	3380 Fred George Rd.	13-26711	13-CF-3367 OPEN	(850) 251-████	Exigent/Consent	X
10/16/2013	X		Armed Robbery	TPD	3393 Lombladh Rd	13-26516	13-CF-3367 OPEN	(850) 459-████	Court Order	X
10/22/2013	X		Wanted Person	USMS	3383 Woodbriar	SO Booking 130517051	13-CF-3417 OPEN	(707) 230-████	Court Order	X
11/15/2013	X		Attempted Murder	TPD	2056 Hillsborough St	13-29909	13-CF-3667 OPEN	(850) 590-████	Court Order	X
11/18/2013	X		Wanted Person - Sex Batt vic < 1290a	FDLE	Graceville, FL	FDLE-ESSST		(863) 445-████	No Copy on File w/TPD	
11/21/2013	X		Robbery	TPD	415 N Gadsden Street #201	13-30408	13-CF-3694 OPEN	(941) 465-████	Court Order	X
	X							(530) 228-████	Court Order	X
	X							(850) 566-████	Court Order	X
11/22/2013	X		Armed Robbery	TPD	1710 W. Tennessee St.	13-30542	TPD OPEN INACTIVE	(850) 485-████	Court Order	X
12/5/2013	X		Wanted Person	TPD/USMS	2521 Pecan Rd	13-31964	13-CF-2952	(321) 213-████	Court Order	X
12/7/2013	X	X	Missing Person	TPD	2526 Nugget Ln	13-32041		(850) 566-████	Exigent/Consent	
12/7/2013	X	X	Armed Robbery	TPD	1102 S Adams St	13-32141		(850) 322-████	Exigent/Consent	
12/10/2013	X		Wanted Person	TPD-CCU	1700 Joe Louis St	13-31087	13-CF-996	(850) 459-████	Court Order	X
12/11/2013	X		Wanted Person	TPD	705 S Woodward Ave	13-32172	13-CF-3963 OPEN	(850) 345-████	Court Order	X
12/11/2013	X		Wanted Person	TPD/USMS	Lafayette St/Magnolia Dr	13-32613	11-CR-18-RH USDC	(850) 559-████	Court Order	X
			Attempted Homicide	TPD	1375 Pullen Rd		13-CF-4063 OPEN	(850) 509-████	Court Order	X
12/23/2013	X					13-33742		(850) 242-████	Court Order	X
								(850) 673-████	Court Order	X
	X							(850) 559-████	Court Order	X
								(850) 694-████	No Copy on File w/TPD	
12/27/2013	X		Auto Theft	TPD	1013 Sayers Dr	13-34132	14-CF-178 OPEN; 13-CJ- 873	(770) 557-████	Court Order	X
1/2/2014	X		Solicitation/Traveling to Meet Minor	TPD		13-34477	14-CF-16 OPEN	(850) 528-████	Court Order	X
1/10/2014	X		Burglary	TPD		14-831	14-CJ-40 OPEN	(239) 537-████	Court Order	X
1/14/2015	X	X	Escaped Prisoner	Thomas CO GA/USMS		N/A		(229) 305-████	Exigent/Consent	
1/16/2014	X		Homicide - Update to CE 13-238			13-29958	TPD OPEN ACTIVE	(850) 459-████	Court Order	X
2/4/2014	X		Wanted Person	USMS	2074 Midyette	14P20047 3RD CIR. TAYLOR CTY.		(347) 831-████	Court Order	X
2/9/2014	X	X	Burg Person Assaulted/Dom Battery	TPD	1019 Stearns St.	14-3909		(850) 284-████	Exigent/Consent	
2/10/2014	X	X	Armed Robbery	TPD	500 Mckethen	14-4048			Exigent/Consent	
2/14/2014	X		Wanted Person	TPD	1700 Joe Louis St.	12-13387, 14-6725	12-CF-2069 OPEN	(850) 688-████	Court Order	X
2/18/2014	X		Wanted Person	TPD/USMS		14-2553	14-CF-320 OPEN	(850) 694-████	Court Order	X
	X		Robbery	TPD		14-5075	14-CF-654 OPEN; 14-CF- 655 OPEN; 14- CF-729 OPEN; 14-CF-730 OPEN	(772) 318-████	Court Order	X
2/28/2014	X							(772) 323-████	Court Order	X
	X							(772) 834-████	Court Order	X
	X							(772) 359-████	Court Order	X

# **EXHIBIT NW1/13**

Electronic Surveillance Support Team, Multi-Agency Voluntary Cooperation Mutual Aid Agreement, executed by Florida Department of Law Enforcement and Plant City, Florida, Police Department (Jan. 9, 2013), released in response to public records request by the ACLU.

**ELECTRONIC SURVEILLANCE SUPPORT TEAM  
MULTI-AGENCY VOLUNTARY COOPERATION  
MUTUAL AID AGREEMENT**

This Voluntary Cooperation Mutual Aid Agreement (MAA hereinafter) is entered into by and between the below subscribed law enforcement agencies, to wit: the Florida Department of Law Enforcement (FDLE) and those agencies that, with approval of FDLE, choose to enter into this agreement pursuant to the Florida Mutual Aid Act, Section 23.12 -23.127, in furtherance of their respective duties under law for the purpose of facilitating and providing technical assistance and equipment in criminal investigations in Florida. The parties have determined that they can make efficient use of their powers and resources, in certain criminal cases which may require specialized expertise and have the potential to cross jurisdictional lines, through coordination and sharing of specialized technical resources and personnel of the parties. The parties agree to carry out their respective duties and responsibilities as outlined below, subject to controlling law, policies or procedures, and in consideration of the mutual interests and understandings herein expressed:

1. FDLE and each agency party to this agreement have executed the signature page attached hereto as Addendum A, which includes specific information concerning the geographic scope of this agreement, identification of the agency party entering into this agreement, and other particular information all of which is incorporated herein as though fully set out in the text of the main agreement.
2. FDLE and each agency party to this agreement has custody and control of technical assets including but not limited to covert camera systems (including internet-based systems), cellular locating equipment, global positioning satellite (GPS) tracking equipment, and video and audio enhancement equipment, all of which is used in surveillance and location of subjects of violent criminal or missing persons investigations. Use of this equipment will generally be referred to in this MAA as Electronic Surveillance Support (ESS).
3. Technical assistance is necessary for the deployment and effective use and operation of these technical assets, and certain requests for ESS services may require more resources, specially trained personnel or advanced technical equipment than a single agency can provide.
4. This MAA establishes and governs regional Electronic Surveillance Support Teams (ESST) in the state of Florida that may provide resources and equipment and the personnel to operate them anywhere in Florida upon request by any law enforcement agency within the state; however it is understood that such teams will normally operate within the geographical areas that comprise one or two FDLE Operations Center Regions. These "standard operational areas" for the teams are set forth in Addendum A. This assistance will include covert camera placement and operation, vehicle tracking device installation and monitoring, video and audio surveillance operations, cellular locating and tracking, audio and video enhancement, and other similar technical support as requested.
5. Each agency party to this MAA agrees to provide ESS upon request within their "standard operational area" as set forth in Addendum A, and may provide assistance elsewhere in the state contingent upon availability and approval of their agency.
6. Nothing contained in this MAA is intended to prevent personnel from performing their normal duties as assigned by their respective agencies.
7. Each party agrees that all unit members assigned to the ESST must be knowledgeable on the deployment and lawful use of the ESS equipment before utilizing it in the field.



8. Jurisdiction.

- 8.1. When engaged in ESST operations that have been approved by and involve FDLE, as contemplated by this MAA, ESST members who do not otherwise have jurisdictional authority shall have full jurisdictional authority anywhere in the State of Florida, although principally focused within their "standard operational area" as set forth in Addendum A, with full power to enforce Florida laws and to avail themselves of the provision of this Agreement
  - 8.2. Officers assigned to ESST operations pursuant to this MAA shall be empowered to render law enforcement assistance and take law enforcement action in accordance with the law and the terms of this MAA.
  - 8.3. Execution of this MAA and continued participation by FDLE and each Party Agency shall constitute a general reciprocal, continuing request for and granting of assistance between the members of the Team that shall be considered authorized in accordance with the provisions of this MAA. No additional or specific formal request for assistance is required.
  - 8.4. ESST members operating outside their agency's jurisdiction shall not enjoy extra-jurisdictional authority as law enforcement officers unless engaged in approved ESST activities as stated herein.
  - 8.5. Pursuant to Section 23.127(1), Florida Statutes, employees of agencies that are parties to this agreement participating in the ESST shall, when engaging in authorized mutual cooperation and assistance pursuant to this MAA, have the same powers, duties, rights, privileges and immunities as if the employees were performing duties inside the law enforcement jurisdictional area of their respective agencies.
  - 8.6. Activities shall be considered authorized only when approved and directed as provided herein by an FDLE supervisor or command designee. If at anytime an FDLE supervisor or command designee determines that ESS assistance pursuant to this MAA should be terminated, it shall be promptly terminated in a manner assuring the safety of all involved law enforcement officers.
  - 8.7. No ESST member shall engage in activities outside the jurisdictional territory of his or her agency, except as approved by the ESST coordinator or designee and any such activity must be documented as provided herein. The ESST coordinator or designee shall maintain activities logs that will demonstrate the involvement of specific employees or agents provided by the parties to this MAA, including each operation's supervisor or designated leader. Specific authorization and approval from both FDLE and the respective Party Agency supervisory personnel shall be obtained when non-FDLE team members will be acting with FDLE outside of their "standard operational area" as set forth in Addendum A. FDLE shall be entitled to conduct audits and inspections of task force operations and records.
  - 8.8. Whenever an operation occurs outside of a team's "standard operational area" set forth in Addendum A, the SAC for the FDLE office in the region affected shall be notified about the presence of the ESST personnel in his or her region.
  - 8.9. Nothing herein shall otherwise limit the jurisdiction and powers normally possessed by an employee or member of a Party Agency.
9. Each party hereto agrees that all unit members participating in any ESST team shall comply with all applicable FDLE policy and procedures while in any FDLE workplace. However, Party Agency policy and procedures shall govern such members if there is a conflict. Any such conflict regarding rules, standards, policies or procedures shall be promptly reported to the ESST coordinator or designee, and the ESST Unit Commander, if one has been

designated. FDLE and the respective agency shall attempt to resolve the conflict in a manner that will allow this MAA to continue in full effect.

10. Each party hereto agrees that all unit members assigned to any ESST team during ESST activities will remain under the supervision of the FDLE ESST coordinator or designee. ESST unit members will for all other purposes remain agents and employees of their respective agencies and are not FDLE employees.
11. Each party hereto, agrees that each will retain full responsibility for and payment of salary (including overtime compensation or compensatory time), retirement/pension, insurance, disability, worker's compensation benefits and any other employment benefits for the respective agency's members participating in an ESST team.
12. Each party acknowledges that its employees acting pursuant to the MAA are obligated to follow applicable law regarding their activities and are to seek legal guidance and approval prior to engaging in activity that has not been clearly addressed by statute or case law. Each party agrees that each party will assume its own liability and responsibility for the acts, omissions or conduct of such its own employees while such employees are engaged in activities or initiatives pursuant to this MAA.
13. Each party agrees to maintain its own comprehensive general liability insurance, professional liability insurance, and automotive liability insurance or maintain a self-insuring fund for the term of this MAA in the amounts determined by each party to insure adequately such party's liability assumed herein. However, in no event shall such coverage be less than the statutory waiver of sovereign immunity. Each party agrees to provide the other parties with a copy of the respective insurance required hereunder, including the endorsements thereto and renewals thereto. In the event a party maintains a self-insurance fund, such party agrees to provide the other parties with documentation to substantiate the existence and maintenance of such self-insurance fund.
14. Each party agrees that except as otherwise provided herein, each agency will furnish to its own employees the necessary property, police equipment, vehicles, resources and training in order to effect the purposes of this MAA and further agree to bear the costs of expenses associated with the operation, maintenance, loss or damage to its equipment, vehicles or property so provided.
15. Each party agrees that the privileges and immunities from liability, exemption from laws, ordinances and rules and application of all pension, insurance, relief, disability, worker's compensation, salary (including overtime compensation or compensatory time), death and other benefits that apply to the activity of an employee when performing the employee's duties shall apply to the employee to the same degree, manner and extent while such employee acts under this MAA.
16. Each party hereto agrees that all unit members assigned to an ESST must pass a FDLE background investigation. Members may be issued keys and/or access cards to limited areas within the FDLE facilities by FDLE, if approved by the FDLE Regional Special Agent in Charge, and that thereafter assigned ESST members will abide by all FDLE building security procedures. Each party agrees that its members, other than unit members, must be escorted while inside FDLE buildings, in accordance with FDLE building security protocols.
17. This MAA shall become effective upon signature of the authorized representative of the parties, and shall remain in effect unless otherwise terminated until June 30, 2016. Any party, upon ninety (90) days written notice, may terminate this MAA. This agreement may be renewed every four years.

18. This MAA represents the entire agreement between the parties. Any alteration or amendment of the provisions of this MAA shall only be valid upon being reduced to writing, duly signed by authorized personnel of each of the parties and attached to the original.
19. This Agreement shall remain in full force as to all participating Agency Parties until or unless earlier canceled in writing by the Florida Department of Law Enforcement as to all or separate Parties, or as canceled in writing by an individual Party as provided herein. However, if the ESST continues operations beyond June 30, 2016, the Agreement shall be automatically extended on a month-by-month basis, not to extend past December 31, 2016, until such time as each participating Party has ratified a revised or subsequent written Agreement.
20. This Agreement may be duplicated for dissemination to all Parties, and such duplicates shall be of the same force and effect as the original. Execution of this Agreement may be signified by properly signing a separate signature page, the original of which shall be returned to, and maintained by, the Office of the Special Agent in Charge (SAC), Florida Department of Law Enforcement for the areas as specified in Addendum A attached hereto and made a part hereof. Under no circumstances may this agreement be renewed, amended, or extended except in writing. A copy of this agreement, with all signature pages, will be filed with the FDLE Mutual Aid Office pursuant to statute.

IN WITNESS WHEREOF, the Commissioner of FDLE has signed below and the authorized representative of the Agency Party has signed Addendum A (attached) on the date specified.

  
Gerald Bailey, Commissioner,  
Florida Department of Law Enforcement

4/10/17  
Date signed

Legal Review by  (attorney initials)

**ADDENDUM A**

**Party Agency's Acceptance of the Electronic Surveillance Team (ESST) Voluntary  
Cooperation Mutual Aid Agreement (2012 Renewal)**  
(Duration: Signature date to June 30, 2016)

Pursuant to F.S. 23.1225(3), this mutual aid agreement may be entered into by a chief executive officer of the agency that is authorized to contractually bind the agency. By signing below, an indication of such authorization is being made. Any signatory may attach to this signature page any further evidence of authorization you wish to remain on file at FDLE along with this signature page.

**Team standard operational area:** Operational area and conditions listed below:

The ESST Workgroup will provide services to the following counties: Citrus, Sumter, Hernando, Pasco, Pinellas, Hillsborough, Polk, Hardee, Charlotte, Collier, Lee, Manatee, Sarasota, DeSoto, Glades, Hendry, Highlands, and Okeechobee.

Agency Party: PLANT CITY POLICE DEPARTMENT

[Redacted Signature]

Chief of Police

1/9/13

Date signed

**ADDENDUM B**

**Party Agency's Acceptance of the Electronic Surveillance Team (ESST) Voluntary Cooperation Mutual Aid Agreement (2012 Renewal)**

(Duration: Signature to June 30, 2016)

Additional Conditions:

A) The Workgroup, as of December 19, 2012, is comprised of Florida Department of Law Enforcement (FDLE) Tampa Bay Regional Operations Center (TBROC) and the Hillsborough County Sheriff's Office (HCSO).

B) Pursuant to the ESST MAA, the ESST Coordinator will be the Special Agent Supervisor from the FDLE/TBROC Squad G or his/her designee. The Unit Commander will be the Assistant Special Agent in Charge from FDLE/TBROC.

C) **RESPONSIBILITY FOR THE ESST VEHICLE AND RELATED EQUIPMENT:**  
The ESST Vehicle and Related Equipment will be maintained and stored in a secure site at an HCSO or FDLE facility. Workgroup Members, including ESST Coordinator, will be issued an access pass providing them with access to the secure storage site 24 hours per day/seven days per week. Operation of the ESST Vehicle and its related equipment will be restricted to ESST Workgroup Members only.

D) **INSURANCE COVERAGE FOR WORKGROUP MEMBERS:**  
The HCSO Workgroup Members are covered through the HCSO's self-insurance policy, while the FDLE/TBROC Workgroup Members are covered by FDLE, through by the State of Florida via though its self-insurance or otherwise through the Division of Risk Management.

E) Each Workgroup Member, including their immediate supervisor, will be provided a copy of the guidelines set forth in the FDLE/FBI Non-Disclosure Agreement (NDA) concerning the use of the Harris Corporation Wireless Collection Equipment/Technology and will sign the FDLE/FBI Non-Disclosure Acknowledgement Form and prior to utilizing the Harris ESST Related Equipment agree to abide by the NDA .

Agency Party: **PLANT CITY POLICE DEPARTMENT**



1/9/13  
Date signed

Agency Party: **FLORIDA DEPARTMENT OF LAW ENFORCEMENT**  
Tampa Bay Regional Operations Center

\_\_\_\_\_  
Special Agent in Charge Rick Ramirez

\_\_\_\_\_  
Date signed