

FILED
TONI L. MELLON
CLERK, SUPERIOR COURT

14 APR 14 PM 3:37

K. YLVISAKER, DEPUTY

1 MICHAEL G. RANKIN (Bar No.014876)
City Attorney
2 Dennis P. McLaughlin (Bar No. 009797)
Principal Assistant City Attorney
3 P.O. Box 27210
Tucson, AZ 85726-7210
4 Telephone: (520) 791-4221
Fax: (520) 623-9803
5 mike.rankin@tucsonaz.gov
dennis.mcLaughlin@tucsonaz.gov

6 Attorneys for Defendants

7
8 IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

9 IN AND FOR THE COUNTY OF PIMA

10 BEAU HODAI,

No. C20141225

11 Plaintiff,

CITY'S VERIFIED ANSWER

12 v.

13 THE CITY OF TUCSON, a municipal
corporation, and the TUCSON POLICE
14 DEPARTMENT, a municipal agency of the
CITY OF TUCSON

Judge James Marnier

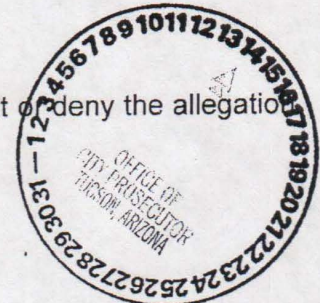
15 Defendants.

17 Defendant City of Tucson and its agency the Tucson Police Department, for its
18 Answer to Plaintiff's Complaint and Application for Order to Show Cause admit, deny,
19 and allege as follows:
20

CIVIL

21 1. With respect to Paragraph 1 of the Complaint, Defendant admits that it is
22 subject to the Arizona Public Records Act, as set forth in A.R.S. § 39-121, et. seq.
23 Defendant denies the remainder of the allegations in paragraph 1. Defendant alleges
24 that it has sought to comply with Plaintiff's requests for records.

25 2. Defendant is without sufficient information to admit or deny the allegation
26 in paragraph 2 and therefore denies the allegation.



Office of the City Attorney
P.O. Box 27210
Tucson, Arizona 85726-7210

RS



1 3. Defendant admits the allegation of paragraph 3.

2 4. With respect to Paragraph 4, Defendant admits that the Tucson Police
3 Department is a department of the City of Tucson subject to the requirements of the
4 Arizona Public Record Act, but deny that the Tucson Police Department is itself a jural
5 entity.
6

7 5. Defendant admits the allegations in Paragraph 5.

8 6. Defendant admits the allegations in Paragraph 6.

9 7. With respect to Paragraph 7, Defendant asserts that Plaintiff's October
10 11, 2013 public records request submitted to the City and TPD speaks for itself and is
11 the best evidence of its own contents.
12

13 8. With respect to Paragraph 8, Defendant asserts that Plaintiff's October
14 11, 2013 public records request submitted to the City and TPD speaks for itself and is
15 the best evidence of its own contents.
16

17 9. Defendant admits the allegations in Paragraph 9, but also additionally
18 alleges that the content of those documents, the redaction of those materials, and
19 information concerning the existence or non-existence of any additional information
20 sought by Plaintiff was discussed in detail with Plaintiff via telephone prior to the
21 disclosure of these materials to Plaintiff.

22 10. Defendant admits that Harris Corporation requested that Defendant
23 redact certain information pursuant to Harris Corporation's legal obligations under
24 federal law and its contractual obligations to the Federal Bureau of Investigation
25 regarding this technology. Defendant admits that TPD agreed to comply with these
26 requests in accordance with the Non-Disclosure Agreement ("NDA") between

1 Defendant and the Harris Corporation governing the use of the technology and other
2 applicable law.

3 11. Defendant asserts that the NDA referred to by Plaintiff in paragraph 11
4 speaks for itself and is the best evidence of its own contents.

5 12. Defendant denies the allegations in paragraph 12. Defendant
6 affirmatively alleges that in the initial response to Plaintiff's records requests it has
7 complied with the NDA but that Defendant does not take any position as to whether
8 this Court can compel the release of some or all of the redacted portions of the
9 records. Defendant has provided notice of this litigation to Harris Corporation so that it
10 may present to this Court any legal basis under state or federal law it may have for
11 maintaining the restrictions on disclosure of the redacted materials.

12 13. Defendant denies the allegations in paragraph 13.

13 14. Defendant denies that it has failed to produce any public records for
14 Plaintiff as required by law. Defendant affirmatively alleges that it is aware of only five
15 cases within the relevant time period where the underlying technology has been used
16 by TPD. These cases do not include any specific reference to the technology and thus
17 do not include any record that would be responsive to Plaintiff's public records request.
18 Defendant is willing to provide the full case files for the cases with completed
19 investigations for in camera review by the Court. One, however, involves an open and
20 active high-profile case wherein any disclosure of records in that case will compromise
21 the ongoing investigation of that case. Defendant is willing to provide a summary of
22 the use of the technology in that case to the Court for in camera review. Defendant
23 further notifies the Court that in its efforts to prepare for this lawsuit it has found a
24
25
26

1 power point training presentation created by a TPD officer, an operational manual
2 created by Harris Corporation, three quick reference guides to calibration of the
3 technology and a blank form for a request to use the technology. Each of these newly
4 discovered documents has been reviewed by the Federal Bureau of Investigation
5 ("F.B.I."), which asserts that the disclosure of these documents would not be in the best
6 interest of the state and is subject to statutory confidentiality and claims of privilege
7 under federal law. See attached affidavit of FBI Special Agent Bradley Morrison.
8 Defendant is prepared to provide these documents to the Court for in camera
9 inspection as well.
10

11 15. Defendant admits that TPD redacted materials from the records produced
12 to Plaintiff at the request of the Harris Corporation as stated in paragraph 10 above.
13 Defendant alleges that these redactions have also been requested by the F.B.I. as
14 necessary to protect the integrity and secrecy of law enforcement technology as
15 required by federal law and as set forth in the attached affidavit of Bradley Morrison.
16 Defendants allege the redacted materials are therefore subject to the exception to the
17 public records law that disclosure is not in the best interest of the state, or that records
18 sought contain confidential or privileged information.
19

20 16. Defendant denies the allegation in paragraph 16.
21

22 17. Defendant admits the allegation in paragraph 17.
23

24 18. Defendant denies the allegation in paragraph 18.
25

26 19. Defendant admits that the NDA provides that the City of Tucson will not
voluntarily release information specified in the agreement.

1 20. Defendant is without sufficient information to respond to the allegations in
2 paragraph 20 and therefore denies the allegations.

3 21. Defendant denies the allegations in paragraph 21.

4 22. With respect to Paragraph 22, Defendant asserts that Plaintiff's
5 November 15, 2013 public records request submitted to the City and TPD speaks for
6 itself and is the best evidence of its own contents.
7

8 23. Defendant denies the allegations in paragraph 23. Defendant does not
9 currently have any non-disclosure agreement with the F.B.I. Defendant acknowledges
10 that it is in discussions with Harris Corporation and the F.B.I. regarding an upgrade of
11 its existing technology, which would include consent to a non-disclosure agreement
12 with the F.B.I. As set forth in the attached affidavit of Bradley Morrison, the disclosure
13 of those documents is not in the best interest of the state and subject to claims of
14 confidentiality and privilege.
15

16 24. With respect to Paragraph 24, Defendant asserts that Plaintiff's
17 December 9, 2013 public records request submitted to the City and TPD speaks for
18 itself and is the best evidence of its own contents.

19 25. Defendant denies the allegations contained in paragraph 25. Sgt. Maria
20 Hawke was in communication with Plaintiff concerning the existence of and ability to
21 retrieve any such records requested in the December 9, 2013 request. Defendant
22 does not seek pen registers in utilizing this technology, so there are no such records.
23 Defendant is not aware that a search warrant has been sought by TPD to utilize the
24 listed Harris Corporation technology within the relevant time period. Defendants
25
26

1 provided e-mail relevant to Harris technology previously and were not aware of any
2 additional e-mail concerning Harris technology within the requested time period.

3 26. With respect to Paragraph 26, A.R.S. § 39-121.01 speaks for itself and is
4 the best evidence of its own content.

5 27. Paragraph 27 states legal arguments, but does not allege facts and
6 therefore does not require any answer. Moreover, A.R.S. § 39-121.01 speaks for itself
7 and is the best evidence of its own content.

8 28. Paragraph 28 states legal arguments, but does not allege facts and
9 therefore does not require any answer. Moreover, A.R.S. § 39-121.01 speaks for itself
10 and is the best evidence of its own content.

11 29. With respect to Paragraph 29, Defendant admits that Plaintiff submitted
12 public records requests on October 11, November 15, and December 9, 2013, and
13 denies the remainder of the allegations.

14 30. Defendant admits the allegations contained in paragraph 30.

15 31. Defendant admits the allegations contained in Paragraph 31.

16 32. Defendant is without sufficient information to respond to the allegations in
17 paragraph 32, and therefore denies the allegations.

18 33. Defendant denies the allegations in paragraph 33.

19 34. Defendant denies the allegations in paragraph 34.

20 35. Paragraph 35 states legal arguments, but does not allege facts and
21 therefore does not require any answer.

22 36. Paragraph 36 states legal arguments, but does not allege facts and
23 therefore does not require any answer.

1 37. Paragraph 37 states legal arguments, but does not allege facts and
2 therefore does not require any answer.

3 38. Paragraph 38 states legal arguments, but does not allege facts and
4 therefore does not require any answer.

5 39. Paragraph 39 states legal arguments, but does not allege facts and
6 therefore does not require any answer.

7 40. Paragraph 40 states legal arguments, but does not allege facts and
8 therefore does not require any answer.

9 41. Defendant denies the allegations in paragraph 41.

10 42. Defendant denies the allegations in paragraph 42.

11 43. Defendant denies the allegations in paragraph 43 and alleges that such
12 information was provided to Plaintiff in multiple telephone conversations.

13 44. Defendant denies the allegations in paragraph 44 and alleges that
14 records that are responsive to Plaintiff's requests were provided.

15 45. Paragraph 45 states legal arguments, but does not allege facts and
16 therefore does not require any answer.

17 46. Defendant denies any allegations in the Complaint not specifically
18 admitted in this Answer.

19 47. Plaintiff's Complaint fails to state a claim upon which relief can be granted
20 and should be dismissed pursuant to ARCP 12(b)(6).

21 WHEREFORE, having fully answered Plaintiff's Complaint, Defendant prays for
22 judgment against Plaintiff as follows:
23

24 ...
25
26

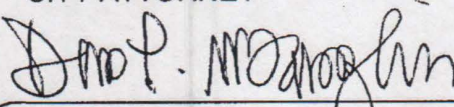
Office of the City Attorney
P.O. Box 27210
Tucson, Arizona 85726-7210

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

- (a) That Plaintiff's complaint be dismissed.
- (b) That Plaintiff be denied any expenses, costs, and attorney's fees.
- (c) For such as other and further relief as the Court deems just and proper.

RESPECTFULLY SUBMITTED this 14th day of April, 2014.

MICHAEL G. RANKIN
CITY ATTORNEY

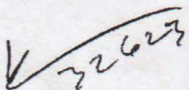


for Lisa Allison Judge
Principal Assistant City Attorney
Attorneys for Defendant City of Tucson

VERIFICATION

STATE OF ARIZONA)
) ss
COUNTY OF PIMA)

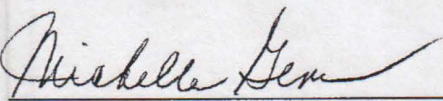
KEVIN R. HALL, being duly sworn upon his oath states that he is familiar with the allegations in the City's Verified Answer and that upon information and belief those allegations are true and correct.



Kevin R. Hall

SUBSCRIBED AND ACKNOWLEDGED before me this 14th day of April,
2014.

[Seal and Expiration Date]



Notary Public



Office of the City Attorney
P.O. Box 27210
Tucson, Arizona 85726-7210

1 ORIGINAL of the foregoing filed
2 this 14th day of April, 2014 with:

3 Clerk of the Court
4 Pima County Superior Court
5 110 W. Church
6 Tucson, Arizona 85701

7 COPY of the foregoing
8 delivered this same date to:

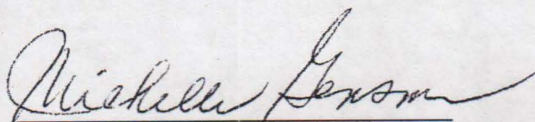
9 Honorable James Marnier
10 Pima County Superior Court
11 110 W. Church
12 Tucson, Arizona 85701

13 COPY of the foregoing
14 mailed this same date to:

15 Daniel J. Pochoda, Esq.
16 Darrel L. Hill, Esq.
17 ACLU Foundation of Arizona
18 3707 N. 7th St., #235
19 Phoenix, AZ 85014

20 Larry Lohman, Associate General Counsel
21 and Vice President, Contracts and Legal
22 Government Communications Systems
23 Harris Corporation
24 1025 West NASA Blvd.
25 Melbourne, FL 32919-0001

26 Bradley S. Morrison, Supervisory Special Agent
Chief, Tracking Technology Unit
Operational Technology Division
Federal Bureau of Investigation
935 Pennsylvania Ave. NW
Washington, DC 20535



Bradley S. Morrison, being duly sworn, deposes and states:

I am a Supervisory Special Agent (SSA) with the Federal Bureau of Investigation (FBI), currently assigned as the Chief, Tracking Technology Unit, Operational Technology Division (OTD) in Quantico, Virginia. I have been employed as a FBI Special Agent since 1996. As Unit Chief, I am responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of all FBI investigative, intelligence collection, and operational programs. I am responsible for establishing and advising on policy guidance for the FBI, including whether a particular tool or technique my program manages meets the criteria for protection as law enforcement sensitive, while ensuring that state-of-the-art technical investigative assets remain available to field technical programs to enable them to assist in a wide range of technical investigative missions. This includes the use and deployment of electronic surveillance devices such as the cell site simulator at issue in this case.

Title 5, United State Code, Section 301 empowers the head of an executive department to set regulations that govern the dissemination of information belonging to that department. With respect to the FBI, as a component of the Department of Justice (DOJ), the Attorney General has promulgated 28 C.F.R. §16.21, in which the Attorney General set forth procedures to follow upon receiving a request for information relating to material contained in the files of the department, or acquired from the department as part of one's official duties. DOJ officials are required to consider several factors in deciding whether to allow privileged information to be released, including whether disclosure of the information sought would "reveal investigatory records compiled for law enforcement purposes, and would... disclose investigative techniques and procedures" whose effectiveness would be impaired by disclosure. 28 C.F.R. §16.26(b)(5).

The FBI OTD has always asserted that the cell site simulators are exempt from discovery pursuant to the "law enforcement sensitive" qualified evidentiary privilege, as information concerning this equipment, if made public, could easily impair use of this investigative method. Likewise, the FBI protects information about its use of this technology in response to requests under the federal Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. Law enforcement techniques and procedures enjoy categorical protection under FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), in order to preserve the utility of those techniques and procedures, and mitigate the risk that they will be circumvented. Under FOIA Exemption 7(E), the FBI protects a range of information about cell site simulators, including operational details such as how, when, where, and under what circumstances the FBI uses cell site simulators, and technical details, such as the particular technology and equipment that the FBI uses. Disclosure of even minor details about the use of cell site simulators may reveal more information than their apparent insignificance suggests because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself. Thus, disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information about the capabilities, limitations, and circumstances of their use, and would allow those adversaries to accumulate information and draw conclusions about the

BSM

use and technical capabilities of this technology. In turn, this would provide them the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology. Doing so would thus allow them to evade detection by law enforcement and circumvent the law.

In recognition of this vulnerability, the FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed. The FBI routinely asserts the law enforcement sensitive privilege over cell site simulator equipment because discussion of the capabilities and use of the equipment in court would allow criminal defendants, criminal enterprises, or foreign powers, should they gain access to the items, to determine the FBI's techniques, procedures, limitations, and capabilities in this area. This knowledge could easily lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations. This, in turn, could completely prevent the successful prosecution of a wide variety of criminal cases involving terrorism, kidnappings, murder, and other conspiracies where cellular location is frequently used. See United States v. Rigmaiden, 845 F.Supp. 982 (D.Ariz. 2012); United States v. Garey, 2004 WL 2663023 (M.D.Ga. Nov. 15, 2004); see also generally FBI's Technical Personnel and Technical Equipment and Use Policy Implementation Guide (0631DPG), sections 1.2.1, 1.2.3, and 1.3, and the FBI's Manual of Investigative Operations and Guidelines, §§ 6-2.1, 6-5.3, 10-10.13, 16-4.8.6 and 16-4.8.14.

Further, the FBI has entered into a non-disclosure agreement (NDA) with our state and local law enforcement partners. The NDA is specific to state and local law enforcement use of cell site simulator technology, and was entered into in an effort to protect law enforcement sensitive details about the technology. The NDA acknowledges that "[d]isclosing the existence of and the capabilities provided by [cell site simulator equipment] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation...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 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 [cell site simulator] equipment 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...to the public..."

Adding to the sensitive nature of the FBI's cell site simulator equipment, the same techniques and tools used in criminal cases are often used in counterterrorism and counterintelligence investigation. Thus, the compromise of the law enforcement community's investigational tools and

methods in a criminal case or public records disclosure could have a significant detrimental impact on the national security of the United States.

Specifically, any information shared by the federal government with a state concerning cell site simulator technology is considered homeland security information under the Homeland Security Act. The Act defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act. See 6 U.S.C. §§ 482(f)(1)(B)-(D). Cell site simulator technology meets all three criteria. Accordingly, under 6 U.S.C. §482(e), homeland security information "obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." The FBI does not consent to release of the information, including technical specifications, technique limitations and vulnerabilities, and training and operational materials.

Additionally, cell site simulator technology is a regulated defense article on the United States Munitions List (USML) (see 22 C.F.R. §121.1 – the US Munitions List, Category XI – Military Electronics, subpart (b) – electronic equipment specifically designed for intelligence, security or military use in surveillance, direction-finding of devices which operate on the electromagnetic spectrum). As such, technical details concerning this technology are subject to the non-disclosure provisions of the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. The ITAR implements the Arms Export Control Act, 22 U.S.C. §2778, and Executive Order 13637, which control the export and import of defense-related articles and services listed on the United States Munitions List (USML). Because this equipment is explicitly governed by the ITAR, 22 C.F.R. §123.1 requires anyone, prior to making an export, to obtain a license from the Department of State. Notably, technical information does not have to leave the borders of the United States to be deemed an export subject to the regulation. (see 22 C.F.R. §120.17, which defines an export as the disclosure of technical data about a defense article to a foreign national, even while located in the United States).

Accordingly, if a state disseminates any part of the technical information knowing that a media organization intends to release the information to the public through the media or via a website, due to the accessibility of the information to non-US citizens, or the requesting media organization employs or has any non-US citizens present at its offices, this may constitute a violation of the Arms Control Export Act. Any unauthorized disclosure of ITAR-controlled information is a felony punishable by up to 20 years imprisonment and up to \$1 million per occurrence. See 22 C.F.R. Part 127.

Specifically, with respect to the cell site simulator used in this case, given the media attention to this case and the inability to control the unauthorized release of information in the internet age, once information about the simulator is publically confirmed, the FBI, as well as the larger law enforcement community, will not be able to employ the equipment again in the future with the same degree of success. Although there is information about cell site simulators and their operation on the Internet, the specific capabilities, settings, limitation and tradecraft used in their deployment were not authoritatively disclosed or confirmed by the FBI. Therefore, should this type of information be

authoritatively disclosed or endorsed, criminal defendants will gain valuable intelligence on the specific capabilities of the law enforcement community to effect surveillance of and locate individuals.

I declare under penalty of perjury that the foregoing facts are true and correct.

4/11/14

Date

Bradley S. Morrison

Bradley S. Morrison
Supervisory Special Agent (SSA)
Chief, Tracking Technology Unit
Federal Bureau of Investigation



Kelly A. Haden
NOTARY PUBLIC
Commonwealth of Virginia
Reg. #353472
My Commission Expires
March 31, 2016

City/County of Stafford
Commonwealth of Virginia
The foregoing instrument was acknowledged before me
this 11 day of April 2014
by Bradley S. Morrison
Kelly A. Haden Notary Public
My commission expires 3-31-2016

BSM

AFFIDAVIT OF
KEVIN R. HALL

State of Arizona)
) ss.
County of Pima)

I, Kevin R. Hall, being of full age, and being duly sworn according to law, upon my oath, state the following:

1. I have personal knowledge of all matters set forth in this Affidavit.
2. I have been a sworn member of the Tucson Police Department since February 1992.
3. I hold the rank of Lieutenant and am currently assigned as a Patrol Commander in Operations Division South.
4. My previous assignment was as the Sergeant supervising the Home Invasion Unit/Special Investigations Division. I held this assignment from October 2010, until I was promoted to the rank of Lieutenant in February 2014.
5. The Home Invasion Unit has primary responsibility for investigation of all adult and suspected narcotics-related abductions of persons.
6. As the supervisor of the Home Invasion Unit, I was primarily responsible for the use and maintenance of the Harris equipment that is the subject of this litigation. The purpose of acquiring this equipment was to assist in on-going abduction/kidnapping investigations. I was responsible for determining when and under what conditions the equipment would be utilized.

7. I, along with three detectives, attended training on the Harris equipment in March 2011. I personally prepared a training presentation on this equipment based upon my own training. Those materials have only been used in two classes with department supervisors.

8. Upon information and belief, the equipment has been rarely used (five instances) and I was personally involved in all but one of those operations.

9. The Harris equipment provides a method for surveillance. Any written reference to the use of this technology in TPD reports would not distinguish this type of surveillance and thus there I have no reason to believe that there are any case reports, requests for warrants or other such documents that would specifically identify the use this type of surveillance equipment in the course of an investigation.

10. In each of the five cases where I personally know that the technology was used, there is no written record of that use in the respective case reports and other documents, and no public record that I can find documenting the use of the technology in those cases.

11. One of the five cases involves an investigation that is still open. It is my opinion and belief that the release of any information about this case, including the case name, would be detrimental to and would interfere with the further investigation of that case.

12. I have identified all case reports I have been able to locate for the other four cases and have provided those to the City Attorney's Office so that they may be submitted to the Court for in camera inspection. I do not believe

that any of these case files contains any reference to the technology involved in this case and thus are not public records that respond to the Plaintiff's requests.

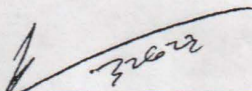
13. There is no way to search for instances in which this technology may have been utilized, as it is not distinguished from any other type of surveillance means.

14. I am not aware of a use of this equipment by the Tucson Police Department wherein a warrant was obtained by the Tucson Police Department.

15. Data produced during the use of this technology is not kept in the ordinary course of business at the conclusion of an investigation as it has no independent evidentiary value. Such data is routinely overwritten.

16. I do solemnly swear and certify that the foregoing statements are true to the best of my knowledge and belief. I am aware that willful false statements can subject me to punishment under the law.

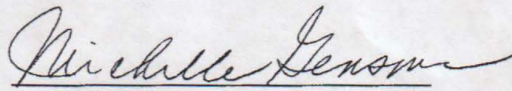
DATED this 14th day of April, 2014.



Kevin R. Hall

Subscribed and sworn to before me on this 14th day of April, 2014.

[Seal and Expiration Date]



Notary Public

