

1 John Pierce
Themis PLLC
2 2305 Calvert Street NW
Washington DC 20008
3 tel. (202) 567-2040

4 SAIED KASHANI, SBN 144805, admitted Pro Hac Vice
5 800 West First Street Suite 400
Los Angeles, California 90012
6 tel. (213) 625-4320
7 fax (213) 652-1900
email: **saiedkashani@gmail.com**

8 Attorneys for Defendant
9 SHANTIA HASSANSHAHI

10
11 UNITED STATES DISTRICT COURT
12 DISTRICT OF COLUMBIA
13

14 UNITED STATES OF AMERICA,) CRIM. ACTION NO. 13-0274 (RC)
15)
Plaintiff,) DEFENDANT'S RESPONSE TO
16) GOVERNMENT FILING RE
v.) SYSTEMATIC STATUTORY VIOLATION
17) OF 21 U.S.C § 876
18 SHANTIA HASSANSHAHI,)
19)
Defendant.)
20)
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

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
27
28

SUMMARY..... 1

ANALYSIS..... 2

I. GOVERNMENT HAS ENGAGED IN A SYSTEMATIC AND PERVASIVE VIOLATION OF THE STATUTE, AND APPEARS TO CONTINUE TO WITHHOLD FULL INFORMATION ABOUT THE VIOLATION..... 2

II. THE STATUTORY VIOLATION PLUS THE CONCEDED CONSTITUTIONAL VIOLATION REQUIRES SUPPRESSION OF THE EVIDENCE..... 6

III. GOVERNMENT THUS ALSO CONCEDED STANDING..... 7

IV. THE VIOLATION WAS EGREGIOUS..... 8

CONCLUSION..... 8

SUMMARY

1
2 Title 21 USC § 876 allows the government to serve an
3 administrative subpoena in connection with a purely drug
4 enforcement investigation. Government has systematically
5 violated this statute for over a decade by using the subpoena
6 process to secretly gather a database of telephony information
7 on all Americans, and then utilizing the database (while
8 disguising its source) in all manner of investigations in all
9 fields not related to drugs at all. Government utilized this
10 pervasive scheme to "finger" defendant Hassanshahi and would not
11 have searched Mr. Hassanshahi's computer but for the scheme. As
12 this Court held on December 1, 2014 (Mem. Dec. p. 9), "the Court
13 finds that the existence of but-for causation between the law
14 enforcement database search and the forensic laptop examination
15 is quite plain."

16 This was not a one-time or negligent statutory violation
17 that happened to uncover evidence of another crime, or even the
18 sharing of information *legitimately gathered* for one purpose
19 with another agency. Cf. Johnson v. Quander, 440 F.3d 489
20 (D.C.Cir. 2006) (government may use DNA profiles gathered
21 pursuant to and in conformance with statute for other
22 investigations). By its very nature, the gathering of telephony
23 information was repeated and systematic, as was the making
24 available of the database to all government agencies, and all
25 aspects of the scheme (from gathering to dissemination outside
26 drug investigations) violated the statute.

27 In its latest filing, government claims a statutory
28 violation alone does not justify suppression of evidence absent

1 a constitutional or Fourth Amendment aspect. Sanchez-Llamas v.
2 Oregon, 548 U.S. 331, 347 (2006). Government forgets that in
3 this case, government *already stipulated* the use of the database
4 was unconstitutional. Mem. Dec. p. 9 ("Regrettably, the Court
5 therefore starts its analysis from the posture that HSI's
6 initial search of the mysterious law enforcement database... was
7 unconstitutional." Having prevailed at the last hearing by
8 concealing information, government is bound by its prior
9 admission and cannot reverse it now. Government's concession
10 also negates its current claim that Mr. Hassanshahi "lacks
11 standing" to assert the violation. Thus, per government's own
12 cited authorities, the resulting evidence must be suppressed.

13 It further appears that government agents were directed to
14 conceal and disguise the use of the database from defense
15 attorneys and the courts. Reuters, August 5, 2013 (attached).
16 At a minimum, further discovery and hearings are needed to
17 explore the nature of the program and the lengths the government
18 went to conceal it.

19 ANALYSIS

20 I. GOVERNMENT HAS ENGAGED IN A SYSTEMATIC AND PERVASIVE 21 VIOLATION OF THE STATUTE, AND APPEARS TO CONTINUE TO 22 WITHHOLD FULL INFORMATION ABOUT THE VIOLATION

23 21 USC § 786 provides:

24 In any investigation relating to his
25 functions under this subchapter with respect
26 to controlled substances, listed chemicals,
27 tableting machines, or encapsulating
28 machines, the Attorney General may . .
.require the production of any records
(including books, papers, documents, and
other tangible things which constitute or
contain evidence) which the Attorney General

1 finds relevant or material to the
2 investigation.

3 The statute thus confines the administrative subpoena to
4 controlled substances (drug enforcement) *and also* to an
5 *investigation* concerning controlled substances. In context this
6 can only mean a *specific* investigation (Code uses the phrases
7 "in any investigation... material to *the* investigation").

8 Here the government secretly and systematically violated
9 every aspect of the statute. The government served
10 administrative subpoenas, not in connection with any particular
11 investigation of controlled substances, but systematically.
12 Most probably the government automatically served a subpoena on
13 every telecommunications provider every month, demanding full
14 telephony records, possibly in electronic form. The result was
15 a systematic database of telephone records of every call to and
16 from every American to and from abroad.¹ This is of necessity.
17 If there were "gaps" in the subpoenae -- for example if the
18 government only served a subpoena on a specific provider from
19 time to time as said provider came up in a specific drug
20 investigation -- there would be large gaps in the telephony data
21 and the resulting database would not work as intended.

22 The government also violated the statute because neither
23 the subpoenae nor the resulting database were confined to drug
24 enforcement. Government concedes that this case, for example,

25 ¹ Government claims the subpoenae sought records of calls to and
26 from "countries associated with drug trafficking." Every
27 country in the world, including the Vatican, has been
28 "associated" with drug trafficking. Thus the government most
likely demanded monthly records of every single call to or from
abroad.

1 has nothing to do with drugs, but the database was obviously
2 freely accessible to the agents in charge. Government must have
3 known of the unrestricted use of the database while serving the
4 subpoenae (at some point it became obvious that the database was
5 being used for non-drug investigations, but government continued
6 gathering the telephony records). Thus both in *gathering* and
7 *disseminating* the data, government engaged in a systematic
8 statutory violation.

9 Nor is this a matter of "sharing" legitimately gathered
10 information among agencies. In Johnson v. Quander, 440 F.3d 489
11 (D.C.Cir. 2006), the relevant statute specifically permitted and
12 called for collection of DNA from parolees and probationers.
13 Said information, legitimately gathered, could be shared with
14 other agencies. No statute permitted the gathering of telephone
15 records in this case -- by contrast, the statute precluded
16 subpoenae except for drug enforcement investigations. No case
17 has ever immunized the sharing of data gathered through a
18 systematic statutory violation.

19 Nor has government "come clean" even at this stage. In
20 2013, Reuters reported (attached):

21 A secretive US Drug Enforcement
22 Administration unit is funneling information
23 from intelligence intercepts, wiretaps **and a**
24 **massive database of telephone records** to
authorities across the nation to help them
launch criminal investigations of Americans.

25 [D]ocuments reviewed by Reuters show that
26 law enforcement agents have been directed to
27 conceal how such investigations truly begin
-- not only from defense lawyers but
sometimes from prosecutors and judges.

28 . . .

1 The unit of the DEA that distributes the
2 information is called the Special Operations
3 Division, or SOD.

 . . .

4 Today, much of the SOD's work is classified,
5 and officials asked that its precise location
6 in Virginia not be revealed. **The documents
7 reviewed by Reuters are marked "Law
8 Enforcement Sensitive," a government
9 categorization that is meant to keep them
10 confidential.**

11 "Remember that the utilization of SOD cannot
12 be revealed or discussed in any investigative
13 function," a document presented to agents
14 reads. The document specifically directs
15 agents to omit the SOD's involvement from
16 investigative reports, affidavits,
17 discussions with prosecutors and courtroom
18 testimony. Agents are instructed to then use
19 "normal investigative techniques to recreate
20 the information provided by SOD."

21 The SOD program as reported by Reuters, resembles the
22 events in the instant case. The government refused to disclose
23 any details of the database until this Court ordered disclosure.
24 The Court will recall that the government's revised affidavit
25 mentioned, for the first time, that the agent had consulted
26 another database (TECS) -- was this an attempt to "recreate" an
27 investigative trail that originated with SOD? The current
28 affidavit is also marked "Law Enforcement Sensistive." At a
29 minimum, the reports merit further investigation and discovery
30 in this case. Was there not only a systematic statutory
31 violation, but also a systematic program to conceal the
32 violation and disguise the improper origin of information used
33 in this and other case?

1 **II. THE STATUTORY VIOLATION PLUS THE CONCEDED CONSTITUTIONAL**
2 **VIOLATION REQUIRES SUPPRESSION OF THE EVIDENCE.**

3 Government claims a statutory violation alone will not
4 require suppression of the evidence. The Supreme Court did not
5 in Sanchez-Llamas, 548 U.S. at 348:

6 The few cases in which we have suppressed
7 evidence for statutory violations do not help
8 Sanchez-Llamas. In those cases, the excluded
9 evidence arose directly out of statutory
10 violations that implicated important
11 Fourth and Fifth Amendment interests.

12 Query the application of this rule in this case, as the
13 rule came about in the context of a one-time or negligent
14 violation, not a systematic, intentional violation. For example
15 in Sanchez-Llamas, the individual defendant, a Mexican citizen,
16 was not afforded a chance to consult with his consulate per
17 provision of international treaty. This treaty or statutory
18 violation was held not to be grounds for suppression absent a
19 constitutional aspect. But unlike the instant case, there was
20 no suggestion in Sanchez-Llamas that the government was
21 systematically denying suspects of their rights under the
22 treaty, or routinely preventing foreign nationals from reaching
23 their consulates. That would be the proper analogy to the
24 instant case, where the statutory violation is intentional and
25 systematic at all levels (issuance of subpoenae, gathering of
26 information, dissemination to other agencies, and concealing the
27 true origin of the data).

28 Defendant herein submits that a *systematic* statutory
violation, or a program whose purpose is to violate the statute
continuously over decades, presents a case of first impression
not governed by Sanchez-Llamas or other government cases.

1 But the Court need not reach the novel issue because in the
2 instant case, the government *already conceded* that use of the
3 database was a constitutional violation *of Mr. Hassanshahi's*
4 *rights*. Indeed the Court asked this Court to *assume* the
5 constitutional violation. Mem. Dec. p. 9. Where there is a
6 statutory violation *plus* an individual constitutional violation,
7 the evidence shall be suppressed even under government's cited
8 cases.

9 Nor can the government withdraw its concession, because the
10 government has already benefited by the favorable result at the
11 last hearing. Allowing a "switch" now would be unfair and a
12 denial of due process at the hearing. Government cannot take
13 one position at one hearing and a different position in
14 subsequent proceedings. In Steagald v. United States, 451 U.S.
15 204, 210-211 (1981), government originally connected defendant
16 to the house that was searched, but later sought to argue
17 defendant lacked a reasonable expectation of privacy in the
18 searched home. The Supreme Court held the government to its
19 original position and precluded changing course. Similarly
20 here, having conceded that the database violated Mr.
21 Hassanshahi's constitutional protections, government cannot now
22 switch course and claim "merely" a statutory violation.

23 **III. GOVERNMENT THUS ALSO CONCEDED STANDING.**

24 Government now argues Mr. Hassanshahi "lacks standing" to
25 contest the statutory violation. Again, government forgets it
26 previously conceded that use of the database was
27 unconstitutional, meaning unconstitutional *as to defendant*
28 (otherwise the concession was meaningless and afforded no

1 grounds to withhold information). Mr. Hassanshahi obviously has
2 standing to assert a *conceded* constitutional violation.

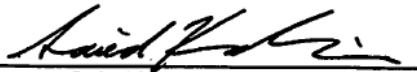
3 **IV. THE VIOLATION WAS EGREGIOUS.**

4 Going back to the prior ruling, it is now clear that
5 government's conceded constitutional violation was systematic
6 and in violation of statute, i.e. egregious. This is further
7 grounds to suppress the evidence, particularly if, as appears,
8 the evidence was gathered as part of a systematic program to
9 conceal its true origin.

10 **CONCLUSION**

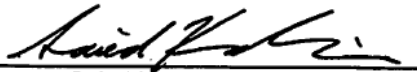
11 The evidence should be suppressed. Alternatively, a
12 further hearing is necessary to explore the scope of the program
13 and, for example, whether this was part of the SOD program and
14 whether agents were instructed to conceal or disguise the origin
15 of the information. The latter is particularly applicable due
16 to the change in affidavits in this case, which may have been an
17 attempt to "recreate" the investigation without disclosing the
18 program.

19 DATED: April 12, 2015

20 
21 Saied Kashani
22 Attorney for Defendant
SHANTIA HASSANSHAH

23 CERTIFICATE OF SERVICE

24 I hereby certify that a true and correct copy of the
25 foregoing opposition was served electronically on Frederick
26 Yvette, counsel for the government, via email to Mr. Yvette's
confirmed email address on April 12, 2015.

27 
28 Saied Kashani