

United States District Court

FILED
LOGGEDENTERED
RECEIVED

WESTERN DISTRICT OF WASHINGTON

JUN 12 2007 LK

In the Matter of the Search of any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER:

~~MS07-088~~ *MS07-5114*

FILED UNDER SEAL

MS07-5114

I, U.S. FBI Special Agent Norman B. Sanders, Jr., being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigations (FBI), and have reason to believe that () on the person of or (XX) on the property known as (name, description and/or location)

Any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

in the Western District of Washington, there is now concealed a certain person or property, namely:
(describe the person or property to be seized)

Network level messages, IP addresses, MAC addresses, other variables, and certain registry-type information.

THIS WARRANT DOES NOT SEEK AUTHORIZATION TO OBTAIN THE CONTENT OF ANY

ELECTRONIC COMMUNICATIONS.

which is (state one or more basis for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

Evidence of a crime

concerning a violation of Title 18 United States Code, Section(s) 875(c); 1030(a)(5)(A)(i) and (B)(iv). The facts to support a finding of Probable Cause are as follows:

See attached Affidavit of Special Agent Norman B. Sanders, Jr.

Continued on the attached sheet and made a part hereof.

(X) Yes () No

Signature of Affiant
NORMAN B. SANDERS, JR.

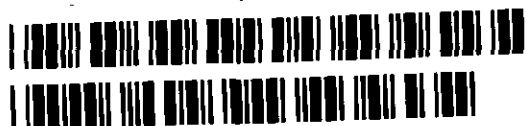
Sworn to before me, and subscribed in my presence:

June 12, 2007 2 pm at
Date

Seattle, Washington
City and State

JAMES P. DONOHUE, United States Magistrate Judge
Name and Title of Judicial Officer

James P. Donohue
Signature of Judicial Officer



JUN 12 2007 LK

AFFIDAVIT

CLERK AT SEATTLE
U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
JPD

MS07 088

SS:

STATE OF WASHINGTON
COUNTY OF KING

Norman B. Sanders Jr., being duly sworn on oath, deposes and says:

1. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), and have been such for the past five years. Prior to becoming a Special Agent, I was employed by the FBI as a Computer Forensic Examiner, for six and one-half years. I am currently assigned to the Seattle Office's Cyber Crime Squad, which investigates various computer, and Internet-related federal crimes.

2. My experience as an FBI Agent has included the investigation of cases involving Computer Intrusions, Extortion, Internet Fraud, Identity Theft, Crimes Against Children, Intellectual Property Rights, and other federal violations involving computers and the Internet. I have also received specialized training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, cyber crimes computer evidence identification, computer evidence seizure and forensic processing, and various other criminal laws and procedures. I have personally participated in the execution of arrest warrants and search warrants involving the search and seizure of computers and electronic evidence, as well as paper documents and personal belongings.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. Relative to this investigation, my duties include the investigation of offenses including violations of Title 18, United States Code, Sections 875(c) (Interstate Transmission of Communication Containing Threat to Injure), and 1030(a)(5)(A)(i) and

Warrant Issued

1 (B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

2 5. I submit this affidavit in support of the application of the United States for
3 a search warrant. This search warrant pertains to the Government's planned use of a
4 specialized technique in a pending criminal investigation. Essentially, if a warrant is
5 approved, a communication will be sent to the computer being used to administer
6 www.myspace.com¹ ("MySpace") user account "Timberlinebombinfo".

7 The communication to be sent is designed to cause the above referenced
8 computer to transmit data, in response, that will identify the computer and/or the
9 user(s) of the computer.² In this manner, the FBI may be able to identify the computer
10 and/or user of the computer that are involved in committing criminal violations of
11 United States Code specifically, Title 18, United States Code, Sections 875(c)
12 (Interstate Transmission of Communication Containing Threat to Injure), and
13 1030(a)(5)(A)(i) and (B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

14 More specifically, the United States is applying for a search warrant authorizing:

15 a). the use of a Computer & Internet Protocol Address³ ("IP address")
16

17 ¹ MySpace is a international free service that uses the Internet for online communication through
18 an interactive social network of photos, videos, weblogs, user profiles, blogs, e-mail, instant
19 messaging, web forums, and groups, as well as other media formats. MySpace users are capable of
20 customizing their user webpage and profile. Users are also capable of searching or browsing other
MySpace webpages and adding other users as "friends". If the person identified approves your
"friend" request, he or she will be added to your list of friends. Users are capable of sending MySpace
messages and posting comments on other user's MySpace webpages.

21 ² In submitting this request, the Government respectfully does not concede that a reasonable
22 expectation of privacy exists in the internet protocol address assigned by a network service provider or
23 other provider to a specific user and used to address and route electronic communications to and from
24 that user. Nor does the government concede that a reasonable expectation of privacy is abridged by the
use of this communication technique, or that the use of this technique to collect a computer's IP
address, MAC address or other variables that are broadcast by the computer whenever it is connected
to the Internet, constitutes a search or seizure.

25 ³ Conceptually, IP addresses are similar to telephone numbers, in that they are used to identify
26 computers that exchange information over the Internet. An IP address is a unique numeric address
27 used to direct information over the Internet and is a series of four numbers, each in the range 0-255,
separated by periods (e.g., 121.56.97.178). In general, information sent over the Internet must
28 contain an originating IP address and a destination IP address, which identify the computers sending
and receiving the information. Section 216 of the USA Patriot Act (P.L. 107-56) amended 18 U.S.C.
§§3121 *et seq* to specifically authorize the recovery of "addressing" and "routing" information of

1 Verifier ("CIPAV") in conjunction with any computer that administers MySpace user
2 account "Timberlinebombinfo" (<http://www.myspace.com/timberlinebombinfo>),
3 without prior announcement within ten days from the date this Court authorizes the use
4 of the CIPAV;

5 b). that the CIPAV may cause any computer - wherever located - that
6 activates any CIPAV authorized by this Court (an "activating computer") to send
7 network level messages⁴ containing the activating computer's IP address and/or MAC
8 address,⁵ other environment variables, and certain registry-type information⁶ to a
9 computer controlled by the FBI;

10 c). that the FBI may receive and read within ten days from the date
11 this Court authorizes the use of the CIPAV, at any time of day or night, the information
12 that any CIPAV causes to be sent to the computer controlled by the FBI; and

13 d). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification
14

15

electronic As used here, a network-level message refers to an exchange of technical information
16 between computers. communications by a pen register/trap & trace order.

17 ⁴ Such messages work in established network protocols, determining, for example, how a given
18 communication will be sent and received. Every time a computer connected to a local area network
19 (LAN) or to the Internet connects to another computer on the LAN or the Internet, it broadcasts
20 network-level messages, including its IP address, and/or media access control (MAC) address, and/or
21 other "environment variables." A MAC address is a unique numeric address of the network interface
22 card in a computer. Environment variables that may be transmitted include: operating system type and
version, browser type and version, the language the browser is using, etc. These network-level
messages also often convey network addressing information, including origin and destination
information. Network-level messages are used to make networks operate properly, transparently, and
consistently.

23 ⁵ Computers that access, and communicate on LANs do so via a network interface card (NIC)
24 installed in the computer. The NIC is a hardware device and every NIC contains its own unique MAC
25 address. Every time a computer connected to a LAN communicates on the LAN, the computer
broadcasts its MAC address.

26 ⁶ As used here, "registry-type information" refers to information stored on the internal hard
27 drive of a computer that defines that computer's configuration as it relates to a user's profile. This
28 information includes, for example, the name of the registered owner of the computer and the serial
number of the operating system software installed. Registry information can be provided by a
computer connected to the Internet, for example, when that computer connects to the Internet to request
a software upgrade from its software vendor.

1 requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay
2 providing a copy of the search warrant and the receipt for any property taken until no
3 more than thirty (30) days after such time as the name and location of the owner or user
4 of the activating computer is positively identified or a latter date as the court may, for
5 good cause shown, authorize. Provision of a copy of the search warrant and receipt
6 may, in addition to any other methods allowed by law, be effectuated by electronic
7 delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully
8 executed documents.

9 6. I am thoroughly familiar with the information contained in this Affidavit,
10 which I have learned through investigation conducted with other law enforcement
11 officers, review of documents, and discussions with computer experts. Because this an
12 application for a search warrant and pen register, not every fact known about the
13 investigation is set forth, but only those that are pertinent to the application. As a result
14 of the investigation, I submit there is probable cause to believe the MySpace
15 "Timberlinebombinfo" account, e-mail account "dougbriggs123@gmail.com"; e-mail
16 account "dougbrigs@gmail.com"; e-mail account "dougbriggs234@gmail.com"; e-mail
17 account "thisisfromitaly@gmail.com"; and e-mail account
18 "timberline.sucks@gmail.com" have been used to transmit interstate communications
19 containing threats to injure, and involve computer intrusion causing a threat to public
20 safety in violation of Title 18, United States Code, Sections 875(c) and 1030(a)(5)(A)(i)
21 and (B)(iv). I further submit that there is probable cause to believe that using a CIPAV
22 in conjunction with the target MySpace account (Timberlinebombinfo) will assist in
23 identifying the individual(s) using the activating computer to commit these violations of
24 the United States Code.

25 7. In general, a CIPAV utilizes standard Internet computer commands
26 commonly used commercially over local area networks (LANs) and the Internet to
27 request that an activating computer respond to the CIPAV by sending network level
28

1 | messages, and/or other variables, and/or registry information, over the Internet⁷ to a
2 | computer controlled by the FBI. The exact nature of these commands, processes,
3 | capabilities, and their configuration is classified as a law enforcement sensitive
4 | investigative technique, the disclosure of which would likely jeopardize other on-going
5 | investigations and/or future use of the technique. As such, the property to be accessed
6 | by the CIPAV request is the portion of the activating computer that contains
7 | environmental variables and/or certain registry-type information; such as the
8 | computer's true assigned IP address, MAC address, open communication ports, list of
9 | running programs, operating system (type, version, and serial number), internet
10 | browser and version, language encoding, registered computer name, registered
11 | company name, current logged-in user name, and Uniform Resource Locator (URL)
12 | that the target computer was previously connected to.

13 | 8. An Internet Service Provider (ISP) normally controls a range of several
14 | hundred (or even thousands) of IP addresses, which it uses to identify its customers'
15 | computers. IP addresses are usually assigned "dynamically": each time the user
16 | connects to the Internet, the customer's computer is randomly assigned one of the
17 | available IP addresses controlled by the ISP. The customer's computer retains that IP
18 | address until the user disconnects, and the IP address cannot be assigned to another
19 | user during that period. Once the user disconnects, however, that IP address becomes
20 | available to other customers who connect thereafter. ISP business customers will
21 | commonly have a permanent, 24-hour Internet connection to which a "static" (i.e.,
22 | fixed) IP address is assigned. Practices for assigning IP addresses to Internet users
23 | vary, with many providers assigning semi-persistent numbers that may be allocated to a
24 | single user for a period of days or weeks.

25 | 9. Every time a computer accesses the Internet and connects to a web site,

26 | ⁷ The "Internet" is a global computer network, which electronically connects computers and
27 | allows communications and transfers of data and information across state and national boundaries. To
28 | gain access to the Internet, an individual utilizes an Internet Service Provider (ISP). These ISP's are
available worldwide.

1 that computer broadcasts its IP address along with other environment variables.
2 Environment variables, such as what language the user is communicating in, allows the
3 web site to communicate back and display information in a format that the computer
4 accessing the web site can understand. These environment variables, including but not
5 limited to, the IP address and the language used by the computer, may assist in locating
6 the computer, as well as provide information that may help identify the user of the
7 computer.

8 10. The hard drives of some computers contain registry-type information. A
9 registry contains, among other things, information about what operating system
10 software and version is installed, the product serial number of that software, and the
11 name of the registered user of the computer. Sometimes when a computer accesses the
12 Internet and connects to a software vendor's web site for the purpose of obtaining a
13 software upgrade, the web site retrieves the computer's registry information stored on
14 its internal hard drive. The registry information assists the software vendor in
15 determining if that computer is running, among other information, a legitimate copy of
16 their software because the registry information contains the software's product
17 registration number. Registry information, such as the serial number of the operating
18 system software and the computer's registered owner, may assist in locating the
19 computer and identifying its user(s).

20 21 THE INVESTIGATION

22 11. On May 30, 2007, a handwritten note was discovered on the premises of
23 the Timberline High School in Lacey, Washington. Subsequently, school
24 administrators ordered an evacuation of the students based on the handwritten bomb
25 threat note.

26 a). On June 4, 2007, Timberline High School received a bomb threat
27 e-mail from sender: "dougbriggs123@gmail.com". The Unknown Subject(s)
28 (UNSUB) stated in the e-mail "I will be blowing up your school Monday, June 4,

1 2007. There are 4 bombs planted throughout timberline high school. One in the math
2 hall, library hall, main office and one portable. The bombs will go off in 5 minute
3 intervals at 9:15 AM." In addition, the UNSUB(s) stated, "The email server of your
4 district will be offline starting at 8:45 am." The UNSUB(s) launched a Denial-of-
5 Service (DOS)⁸ attack on the Lacey School District computer network, which caused
6 over 24,000,000 hits on the system within a 24 hour period. School administrators
7 ordered an evacuation of the school on June 4, 2007.

8 b). On June 5, 2007, the UNSUB(s) sent an e-mail from
9 "dougbriggs@gmail.com" stating the following:

10 < <Read This ASAP> >

11 Now that the school is scared from yesturdays fake bomb threat it's
12 now time to get serious. One in a gym locker, the girls. It's in a
13 locker hidden under a pile of clothes. The other four I will only
14 say the general location. One in the Language Hall, One in the
15 math hall, One underneath a portable taped with strong ducktape.
16 This bomb will go off if any vibrations are felt. And the last one,
17 Is in a locker. It is enclosed in a soundproof package, and litteraly
18 undetectable. I have used a variety of chemicals to make the
19 bombs. They are all different kinds.

20 They will all go off at 10:15AM. Through remote detonation.
21 Good Luck. And if that fails, a failsafe of 5 minutes later.

22 The UNSUB(s) goes on to state:

23 Oh and for the police officers and technology idiots at the district
24 office trying to track this email and yesturdays email's location. I can
25 give you a hint. The email was sent over a newly made gmail
26 account, from overseas in a foreign country. The gmail account was
27 created there, and this email and yesturdays was sent from there. So
28 good luck talking with Italy about getting the identify of the person
who owns the 100Mbit dedicated server

29 c). In another e-mail from sender "dougbriggs234@gmail.com"
30 the UNSUB(s) states the following:

31 Hello Again. Seeing as how you're too stupid to trace the email
32 back lets get serious." [The UNSUB(s) mentions 6 bombs set to

33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

⁸ A DOS attack is an Internet based computer attack in which a compromised system attacks a single target, thereby causing a denial of service for users of the targeted computer system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. The DOS attack is generally targeted at a particular network service, such as e-mail or web access.

1 detonate between 10:45-11:15 AM, and adds] Seriously, you are not
2 going to catch me. So just give up. Maybe you should hire Bill
3 Gates to tell you that it is coming from Italy. HAHAAH Oh wait I
4 already told you that. So stop pretending to be "tracing it" because I
5 have already told you it's coming from Italy. That is where trace
6 will stop so just stop trying. Oh and this email will be behind a
7 proxy behind the Italy server.

8 d). School administrators ordered an evacuation of the school on June
9 5, 2007.

10 e). On June 6, 2007, Principle Dave Lehnis of Timberline High
11 School received an e-mail from sender: "dougbriggs911@gmail.com". The e-mail
12 contained the following text: "ENJOY YOUR LIFE ENDING".

13 f). In another e-mail from "dougbriggs911@gmail.com," the
14 UNSUB(s) states the following,

15 Well hello Timberline, today is June 6, 2007 and I'M just emailing
16 you today to say that school will blow up and that's final! There
17 are 2 bombs this time (Iran short on money to buy things at home
18 depot). They will go off at exactly 10:45:00 AM. One is on
19 located on a portable. And the other is somewhere else. Keep
20 trying to 'trace' this email. The only thing you will be able to
21 track is that it came from Italy. There is no other information that
22 leads it back to the United States in any way so get over it.
23 You should hire Bill Gates to track it for you. HAHAAHAAH. He
24 will just tell you that it came from over seas, so if you have close
25 relations with the POPE you might get some information. But
26 other than that, have fun looking in Italy. :-)

27 Also, stop advising teachers to no show this email to classmates.
28 Everyone would be amused by this email and I might stop if you
do. Funny how I can trick you all into thinking that I included my
name to show that it isn't me, because who the hell would put their
name? Or is that just what I want you to think.
And yet again, this email was sent from overseas to a newly made
email account that has
already been deleted of all information by the time you read this
email. Get your ass on a plane to Italy if you want it to stop.

g). School administrators ordered an evacuation of the school on
June 6, 2007.

h). On June 7, 2007, Timberline High School received an e-mail from
sender "thisisfromitaly@gmail.com." The UNSUB(s) states:

1 "There are 3 bombs planted in the school and they're all different
2 kinds. I have premeditated these weeks in advance and tested the timers
3 to make sure they work to exact millisecond. Locking the doors is
a good plan, but too late."

4 i). School administrators ordered an evacuation of the school on
5 June 7, 2007.

6
7 j). On June 7, 2007, the UNSUB(s) posted three of the threatening
8 e-mails in the comments section of the online news publication service, "theolympian".
9 The administrator from theolympian.com" removed the threatening e-mail postings.
10 Shortly thereafter, the UNSUB(s) re-posted the threatening e-mails. Eventually, the
11 administrator of "theolympian.com" disabled the "Comments" section.

12
13 k). On June 7, 2007, Detective Jeremy Knight, Lacey Police
14 Department (LPD), received information from the Thurston County Sheriff's Office,
15 which had revealed a complaint from a person identified as AG. AG stated that she
16 received an invitation through myspace.com from the MySpace profile of
17 "Timberlinebombinfo" wanting her to post a URL link to
18 <http://bombermails.hyperphp.com> on her myspace.com webpage. The UNSUB(s)
19 advised her that failure to comply would result in her name being associated with future
20 bomb threats. Similarly, Knight received a phone call from a parent alleging that her
21 son received the same request from the UNSUB(s). According to Knight, 33 students
22 received a request from the UNSUB(s) to post the link on their respective myspace.com
23 webpages. Subsequent interviews performed by Knight yielded limited information.

24
25 l). On June 7, 2007, VW and BP received MySpace private invitations
26 from an individual utilizing the MySpace moniker "Timberlinebombinfo". VW
27 accepted the invitation from "Timberlinebombinfo" and received an America Online
28 Instant Message (AIM) from an individual utilizing AIM screen name

1 "Alexspi3ring_09." Communication ceased with "Alexspi3ring_09" after VW
2 requested additional information related to the bomb threats. VW believed screen name
3 "Alexspi3ring_09" was associated to ALEX SPIERING, a student at Timberline High
4 School. VW stated "Alexspi3ring_09" and "Timberlinebombinfo" used to have the
5 identical graphic on their MySpace webpage. "Timberlinebombinfo" recently changed
6 his/her graphic from a picture of guns to a picture of a bomb.

7
8 m). On June 7, 2007, Thurston County School District reported ALEX
9 SPIERING resides at 6133 Winnwood Loop SE, Olympia, WA, 98513, telephone (360)
10 455-0569, date of birth [REDACTED], 19[REDACTED].

11
12 n). On June 8, 2007, Comcast Internet, Thorofare, New Jersey,
13 reported that residential address 6133 Winnwood Loop SE, Olympia, WA, 98513
14 received Comcast Internet services for the following subscriber:

15 Sara Spiering
16 6133 Winnwood Loop SE, Lacey, WA 98513
17 Telephone (360) 455-0569
18 Dynamically Assigned Active Account
19 Account Number: 8498380070269681

20
21 o). On June 8, 2007, Thurston County School District received two
22 additional bomb threat e-mails from "Timberline.Sucks@gmail.com," which resulted in
23 the evacuation of the Timberline High School.

24
25 12. On June 4, 2007, Google provided subscriber, registration, and IP Address
26 log history for e-mail address "dougbriggs123@gmail.com" with the following results:

27 Status: Enabled (user deleted account)

28 Services: Talk, Search History, Gmail

1 Name: Doug Briggs

2 Secondary Email:

3 Created on: 03-Jun-2007

4 Lang: en

5 IP: 80.76.80.103

6 LOGS: All times are displayed in UTC/GMT

7 dougbriggs123@gmail.com

8 Date/Time IP

9 04-Jun-2007 05:47:29 am 81.27.207.243

10 04-Jun-2007 05:43:14 am 80.76.80.103

11 03-Jun-2007 06:19:44 am 80.76.80.103

12
13 a). On June 6, 2007, a SmartWhoIs lookup of IP Address 80.76.80.103
14 resolved to Sonic S.R.L, Via S.Rocco 1, 24064, Grumello Del Monte, Italy,
15 Phone: +390354491296, E-mail: Staff@sonic.it. Your affiant connected to
16 http://sonic.it, which displayed an Italian business webpage for Sonic SRL Internet
17 Service Provider.

18
19 b). On June 7, 2007, a request to MySpace for subscriber and IP
20 Address logs for MySpace user "Timberlinebombinfo" provided the following results:

21 User ID: 199219316

22 First Name: Doug

23 Last Name: Briggs

24 Gender: Male

25 Date of Birth: 12/10/1992

26 Age: 14

27 Country: US

28 City: Lacey

1 Postal Code: 985003
2 Region: Western Australia
3 Email Address: timberline.sucks@gmail.com
4 User Name: timberlinebombinfo
5 Sign up IP Address: 80.76.80.103
6 Sign up Date: June 7, 2007 7:49PM
7 Delete Date: N/A
8 Login Date June 7, 2007 7:49:32:247 PM IP Address 80.76.80.103
9

10 c). FBI Seattle Division contacted FBI Legate Attache Rome, Italy and
11 an official request was provided to the Italian National Police requesting assistance in
12 contacting Sonic SRL and locating the compromised computer utilizing IP Address
13 80.76.80.103.

14 d). On June 7, 2007, the System Administrator for the
15 www.theolympian.com advised the posting of the bomb threat e-mails originated from
16 IP Address 192.135.29.30. A SmartWhois lookup resolved 192.135.29.30 to "The
17 National Institute of Nuclear Physics (INFN), LNL - Laboratori Nazionali di Legnaro,
18 Italy".

19 13. Based on my training, experience, and the investigation described herein, I
20 know the following among other things:

21 a). that network level messages, including the originating IP address
22 and MAC address, other variables, and certain registry-type information of a computer
23 can be used to assist in identifying the individual(s) using that computer; and

24 b). the individual(s) using the aforementioned activated computer
25 utilized compromised computers to conceal their true originating IP address and thereby
26 intentionally inhibiting the individual(s)' identification. Compromised computers are
27 generally infected with computer viruses, trojans, or other malevolent programs, which
28 can allow a user the ability to control computer(s) on the Internet or particular services

1 of compromised computer(s) without authorization. It is common for individuals
2 engaged in illegal activity to access and control compromised computer(s) to perform
3 malicious acts in order to conceal their originating IP addresses.

4 14. Based on training, experience, and the investigation described herein, I
5 have concluded that using a CIPAV on the target MySpace "Timberlinebombinfo"
6 account may assist the FBI to determine the identities of the individual(s) using the
7 activating computer. A CIPAV's activation will cause the activating computer to send
8 network level messages, including the activating computer's originating IP address and
9 MAC address, other variables, and certain registry-type information. This information
10 may assist the FBI in identifying the individual(s) using the activating computers.

11 15. The CIPAV will be deployed through an electronic messaging program
12 from an account controlled by the FBI. The computers sending and receiving the
13 CIPAV data will be machines controlled by the FBI. The electronic message deploying
14 the CIPAV will only be directed to the administrator(s) of the "Timberlinebombinfo"
15 account.

- 16 a). Electronic messaging accounts commonly require a unique user
17 name and password.
- 18 b). Once the CIPAV is successfully deployed, it will conduct a one-
19 time search of the activating computer and capture the information
20 described in paragraph seven.
- 21 c). The captured information will be forwarded to a computer
22 controlled by the FBI located within the Eastern District of
23 Virginia.
- 24 d). After the one-time search, the CIPAV will function as a pen register
25 device and record the routing and destination addressing information
26 for electronic communications originating from the activating
27 computer.
28

1 e). The pen register will record IP address, dates, and times of the
2 electronic communications, but not the contents of such
3 communications or the contents contained on the computer, and
4 forward the IP address data to a computer controlled by the
5 FBI, for a period of (60) days.
6

7 CONCLUSION

8 16. Based upon my review of the evidence, my training and experience, and
9 information I have gathered from various computer experts, I have probable cause to
10 believe that deploying a CIPAV in an electronic message directed to the administrator(s)
11 of the MySpace "Timberlinebombinfo" account will assist in identifying a computer and
12 individual(s) using the computer to transmit bomb threats and related communications in
13 violation of Title 18, United States Code Sections 875(c) and 1030(a)(5)(A)(i) and
14 (B)(iv).

15 17. Because notice as required by Federal Rule of Criminal Procedure
16 41(f)(3) would jeopardize the success of the investigation, and because the investigation
17 has not identified an appropriate person to whom such notice can be given, I hereby
18 request authorization to delay such notice until an appropriate person is identified.
19 Further, assuming providing notice would still jeopardize the investigation after an
20 appropriate person to receive notice is identified, I request permission to ask this Court
21 to authorize an additional delay in notification. In any event, the United States
22 government will notify this Court when it identifies an appropriate person to whom to
23 give notice, so that this Court may determine whether notice shall be given at that time.

24 18. Because there are legitimate law enforcement interests that justify an
25 unannounced use of the CIPAV and review of the messages generated by the activating
26
27
28

1 computer in this case,⁹ I ask this Court to authorize the proposed use of a CIPAV
2 without the prior announcement of its use. One of these legitimate law enforcement
3 interests is that announcing the use of the CIPAV would assist a person controlling the
4 activating computer(s) to evade revealing its true IP address, other variables, and certain
5 registry-type information - thereby defeating the CIPAV's purpose.

6 19. Rule 41(e)(2) requires that (A) the warrant command the FBI "to execute
7 the warrant within a specified time no longer than 10 days" and (B) "execute the
8 warrant during the daytime unless the judge for good cause expressly authorizes
9 execution at another time..." In order to comply with Rule 41, the Government will
10 only deploy CIPAV between the hours of 6:00 a.m. and 10:00 p.m. (PST) during an
11 initial 10-day period. However, the Government seeks permission to read any messages
12 generated by the activating computer as a result of a CIPAV at any time of day or night
13 during the initial 10-day period. This is because the individuals using the activating
14 computer may activate the CIPAV after 10:00 p.m. or before 6:00 a.m., and law
15 enforcement would seek to read the information it receives as soon as it is aware of the
16 CIPAV response given the emergent nature of this investigation. If the CIPAV is not
17 activated within the initial 10-day period, the Government will seek further authorization
18 from the Court to read any information sent to the computer controlled by the FBI as a
19 result of that CIPAV after the 10th day from the date the Court authorizes the use of the
20 first CIPAV.

21 20. Because the FBI cannot predict whether any particular formulation of a
22 CIPAV to be used will cause a person(s) controlling the activating computer to activate
23 a CIPAV, I request that this Court authorize the FBI to continue using additional
24 CIPAV's in conjunction with the target MySpace account (for up to 10 days after this
25 warrant is authorized), until a CIPAV has been activated by the activating computer.

26
27 ⁹ See Wilson v. Arkansas, 514 U.S. 927, 936 (1995) (recognizing that "law enforcement
28 interests may . . . establish the reasonableness of an unannounced entry.")

21. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a). the use of multiple CIPAVs until one CIPAV is activated by the activating computer in conjunction with the target MySpace "Timberlinebombinfo" account, without prior announcement, within 10 days from the date this Court authorizes the use of the first CIPAV;

b). the CIPAV may cause an activating computer - wherever located - to send network level messages containing the activating computer's IP address, and/or MAC address, and/or other variables, and/or certain registry-type information to a computer controlled by the FBI and located within the Eastern District of Virginia;

c). that the FBI may receive and read, at any time of day or night, within 10 days from the date the Court authorizes of use of the CIPAV, the information that any CIPAV causes to be sent to the computer controlled by the FBI;

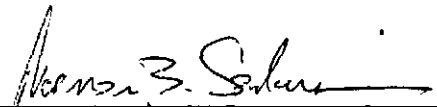
d). that once the FBI has received an initial CIPAV response from the activating computer consisting of network level messages containing the activating computer's IP address, and/or MAC address, and/or other variables, and/or certain registry-type information, the FBI will thereafter only be collecting the types of addressing and routing information that can be collected pursuant to a pen register order; and

e). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay providing a copy of the search warrant and the receipt for any property taken until no more than thirty (30) days after such time as the name and location of the individual(s) using the activating computer is positively identified or a latter date as the court may, for good cause shown, authorize. Provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully executed documents.

1 22. It is further requested that this Application and the related documents be
2 filed under seal. The information to be obtained is relevant to an on-going investigation.
3 Premature disclosure of this Application and related documents may jeopardize the
4 success of the above-described investigation.

5 WHEREFORE, Affiant respectfully requests that a warrant be issued authorizing
6 the FBI to utilize a CIPAV and receive the attendant information according to the terms
7 set forth in this Affidavit.

8
9 **THIS APPLICATION DOES NOT SEEK AUTHORIZATION TO OBTAIN**
10 **THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS, AND THE**
11 **WARRANT WILL SO SPECIFY.**

12
13 
14 Norman B. Sanders
Special Agent
Federal Bureau of Investigation

15 Sworn to and subscribed before
16 me this 12th day of June, 2007

17 
18 Hon. James P. Donohue
19 United States Magistrate Judge
20
21
22
23
24
25
26
27
28