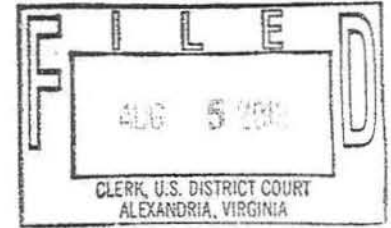


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE	)	UNDER SEAL
APPLICATION OF THE UNITED	)	
STATES OF AMERICA FOR AN ORDER	)	No. 1:13EC297
AUTHORIZING THE USE OF A PEN	)	
REGISTER/TRAP AND TRACE DEVICE	)	
ON AN ELECTRONIC MAIL ACCOUNT	)	
	)	
IN THE MATTER OF THE SEARCH AND	)	
SEIZURE OF INFORMATION	)	
ASSOCIATED WITH	)	No. 1:13SW522
[REDACTED] THAT IS	)	
STORED AT PREMISES CONTROLLED	)	
BY LAVABIT LLC	)	
	)	
In re Grand Jury	)	No. 13-1

MOTION FOR SANCTIONS

The United States, through the undersigned counsel, pursuant to Title 18, United States Code, Section 401, hereby moves for the issuance of an order imposing sanctions on Lavabit LLC and Ladar Levison, its owner and operator, for Lavabit's failure to comply with this Court's order entered August 1, 2013. In support of this motion, the United States represents:

1. At the hearing on August 1, 2013, this Court directed Lavabit to provide the government with the encryption keys necessary for the operation of a pen register/trap and trace order entered June 28, 2013. Lavabit was ordered to provide those keys by 5 p.m. on August 2, 2013. *See Order Denying Motions entered August 2, 2013.*
2. At approximately 1:30 p.m. CDT on August 2, 2013, Mr. Levison gave the FBI a printout of what he represented to be the encryption keys needed to operate the pen register. This

printout, in what appears to be 4-point type, consists of 11 pages of largely illegible characters. See Attachment A. (The attachment was created by scanning the document provided by Mr. Levison; the original document was described by the Dallas FBI agents as slightly clearer than the scanned copy but nevertheless illegible.) Moreover, each of the five encryption keys contains 512 individual characters – or a total of 2560 characters. To make use of these keys, the FBI would have to manually input all 2560 characters, and one incorrect keystroke in this laborious process would render the FBI collection system incapable of collecting decrypted data.

3. At approximately 3:30 p.m. EDT (2:30 p.m. CDT), the undersigned AUSA contacted counsel for Lavabit LLC and Mr. Levison and informed him that the hard copy format for receipt of the encryption keys was unworkable and that the government would need the keys produced in electronic format. Counsel responded by email at 6:50 p.m. EDT stating that Mr. Levison “thinks” he can have an electronic version of the keys produced by Monday, August 5, 2013.

4. On August 4, 2013, the undersigned AUSA sent an e-mail to counsel for Lavabit LLC and Mr. Levison stating that we expect to receive an electronic version of the encryption keys by 10:00 a.m. CDT on Monday, August 5, 2013. The e-mail indicated that we expect the keys to be produced in PEM format, an industry standard file format for digitally representing SSL keys. See Attachment B. The e-mail further stated that the preferred medium for receipt of these keys would be a CD hand-delivered to the Dallas office of the FBI (with which Mr. Levison is familiar). The undersigned AUSA informed counsel for Lavabit LLC and Mr. Levison that the government would seek an order imposing sanctions if we did not receive the encryption keys in electronic format by Monday morning.

5. The government did not receive the electronic keys as requested. The undersigned AUSA spoke with counsel for Lavabit and Mr. Levison at approximately 10:00 a.m. this morning, and he stated that Mr. Levison might be able to produce the keys in electronic format by 5 p.m. on August 5, 2013. The undersigned AUSA told counsel that was not acceptable given that it should take Mr. Levison 5 to 10 minutes to put the keys onto a CD in PEM format. The undersigned AUSA told counsel that if there was some reason why it cannot be accomplished sooner, to let him know by 11:00 a.m. this morning. The government has not received an answer from counsel.

6. The government therefore moves the Court to impose sanctions on Lavabit LLC and Mr. Levison in the amount of \$5000 per day beginning at noon (EDT) on August 5, 2013, and continuing each day in the same amount until Lavabit LLC and Mr. Levison comply with this Court's orders.

7. As noted, Attachment A to this motion is a copy of the printout provided by Mr. Levison on August 2, 2013. Attachment B is a more detailed explanation of how these encryption keys can be given to the FBI in an electronic format. Attachment C to this motion is a proposed order.

8. A copy of this motion, filed under seal, was delivered by email to counsel for Lavabit LLC on August 5, 2013.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By:



United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

Attachment A

1. The first step in the process of the development of a new product is the identification of a market need. This is often done through market research, which can be conducted in a variety of ways, including surveys, focus groups, and interviews. The goal is to understand what customers want and need, and to identify any gaps in the current market.

2. Once a market need has been identified, the next step is to develop a concept for a new product that meets that need. This involves brainstorming ideas and creating a prototype. The prototype is a simplified version of the final product, used to test the concept and gather feedback from potential customers.

3. The third step is to conduct a feasibility study. This involves assessing the technical, financial, and market viability of the product. Technical feasibility involves determining whether the product can be manufactured using current technology. Financial feasibility involves estimating the costs of development and production, and comparing them to the potential revenue. Market feasibility involves assessing the size and growth of the target market, and the competitive landscape.

4. If the feasibility study is positive, the next step is to develop a business plan. This document outlines the company's strategy for developing and marketing the product, and provides a detailed financial forecast. The business plan is used to secure funding from investors or lenders.

5. The final step is to launch the product. This involves manufacturing the product, distributing it to retailers or directly to customers, and promoting it through advertising and marketing efforts. The company should continue to monitor the product's performance in the market, and be prepared to make adjustments as needed.

1. The first step in the process of the development of the new system is the identification of the need for a new system. This is done by the management of the organization, who recognize the need for a new system to meet the changing requirements of the organization. The next step is the selection of a system, which is done by the management of the organization, who select a system that meets the requirements of the organization. The third step is the implementation of the system, which is done by the management of the organization, who implement the system in the organization. The fourth step is the evaluation of the system, which is done by the management of the organization, who evaluate the system to determine if it meets the requirements of the organization. The fifth step is the maintenance of the system, which is done by the management of the organization, who maintain the system to ensure it continues to meet the requirements of the organization.

1. The first step in the process of the investigation is the identification of the problem. This involves a thorough review of the available information and a clear definition of the issue at hand. Once the problem is identified, the next step is to gather relevant data and information. This can be done through various methods, including interviews, surveys, and document analysis. The third step is to analyze the data and information gathered. This involves identifying patterns, trends, and potential causes of the problem. The final step is to develop and implement a solution. This may involve creating a plan, allocating resources, and monitoring progress. Throughout the process, it is important to maintain clear communication and documentation.

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
29
30
31
32
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
84

1. The first part of the document is a list of names and addresses, which are arranged in a columnar fashion. The names are written in a cursive script, and the addresses are written in a more formal, printed style. The list is organized into three main sections, each separated by a horizontal line. The first section contains names and addresses, the second section contains names and addresses, and the third section contains names and addresses. The list is organized into three main sections, each separated by a horizontal line. The first section contains names and addresses, the second section contains names and addresses, and the third section contains names and addresses.

1-10 1-11 1-12 1-13 1-14 1-15 1-16 1-17 1-18 1-19 1-20 1-21 1-22 1-23 1-24 1-25 1-26 1-27 1-28 1-29 1-30 1-31 1-32 1-33 1-34 1-35 1-36 1-37 1-38 1-39 1-40 1-41 1-42 1-43 1-44 1-45 1-46 1-47 1-48 1-49 1-50 1-51 1-52 1-53 1-54 1-55 1-56 1-57 1-58 1-59 1-60 1-61 1-62 1-63 1-64 1-65 1-66 1-67 1-68 1-69 1-70 1-71 1-72 1-73 1-74 1-75 1-76 1-77 1-78 1-79 1-80 1-81 1-82 1-83 1-84 1-85 1-86 1-87 1-88 1-89 1-90 1-91 1-92 1-93 1-94 1-95 1-96 1-97 1-98 1-99 1-100 1-101 1-102 1-103 1-104 1-105 1-106 1-107 1-108 1-109 1-110 1-111 1-112 1-113 1-114 1-115 1-116 1-117 1-118 1-119 1-120 1-121 1-122 1-123 1-124 1-125 1-126 1-127 1-128 1-129 1-130 1-131 1-132 1-133 1-134 1-135 1-136 1-137 1-138 1-139 1-140 1-141 1-142 1-143 1-144 1-145 1-146 1-147 1-148 1-149 1-150 1-151 1-152 1-153 1-154 1-155 1-156 1-157 1-158 1-159 1-160 1-161 1-162 1-163 1-164 1-165 1-166 1-167 1-168 1-169 1-170 1-171 1-172 1-173 1-174 1-175 1-176 1-177 1-178 1-179 1-180 1-181 1-182 1-183 1-184 1-185 1-186 1-187 1-188 1-189 1-190 1-191 1-192 1-193 1-194 1-195 1-196 1-197 1-198 1-199 1-200 1-201 1-202 1-203 1-204 1-205 1-206 1-207 1-208 1-209 1-210 1-211 1-212 1-213 1-214 1-215 1-216 1-217 1-218 1-219 1-220 1-221 1-222 1-223 1-224 1-225 1-226 1-227 1-228 1-229 1-230 1-231 1-232 1-233 1-234 1-235 1-236 1-237 1-238 1-239 1-240 1-241 1-242 1-243 1-244 1-245 1-246 1-247 1-248 1-249 1-250 1-251 1-252 1-253 1-254 1-255 1-256 1-257 1-258 1-259 1-260 1-261 1-262 1-263 1-264 1-265 1-266 1-267 1-268 1-269 1-270 1-271 1-272 1-273 1-274 1-275 1-276 1-277 1-278 1-279 1-280 1-281 1-282 1-283 1-284 1-285 1-286 1-287 1-288 1-289 1-290 1-291 1-292 1-293 1-294 1-295 1-296 1-297 1-298 1-299 1-300 1-301 1-302 1-303 1-304 1-305 1-306 1-307 1-308 1-309 1-310 1-311 1-312 1-313 1-314 1-315 1-316 1-317 1-318 1-319 1-320 1-321 1-322 1-323 1-324 1-325 1-326 1-327 1-328 1-329 1-330 1-331 1-332 1-333 1-334 1-335 1-336 1-337 1-338 1-339 1-340 1-341 1-342 1-343 1-344 1-345 1-346 1-347 1-348 1-349 1-350 1-351 1-352 1-353 1-354 1-355 1-356 1-357 1-358 1-359 1-360 1-361 1-362 1-363 1-364 1-365 1-366 1-367 1-368 1-369 1-370 1-371 1-372 1-373 1-374 1-375 1-376 1-377 1-378 1-379 1-380 1-381 1-382 1-383 1-384 1-385 1-386 1-387 1-388 1-389 1-390 1-391 1-392 1-393 1-394 1-395 1-396 1-397 1-398 1-399 1-400 1-401 1-402 1-403 1-404 1-405 1-406 1-407 1-408 1-409 1-410 1-411 1-412 1-413 1-414 1-415 1-416 1-417 1-418 1-419 1-420 1-421 1-422 1-423 1-424 1-425 1-426 1-427 1-428 1-429 1-430 1-431 1-432 1-433 1-434 1-435 1-436 1-437 1-438 1-439 1-440 1-441 1-442 1-443 1-444 1-445 1-446 1-447 1-448 1-449 1-450 1-451 1-452 1-453 1-454 1-455 1-456 1-457 1-458 1-459 1-460 1-461 1-462 1-463 1-464 1-465 1-466 1-467 1-468 1-469 1-470 1-471 1-472 1-473 1-474 1-475 1-476 1-477 1-478 1-479 1-480 1-481 1-482 1-483 1-484 1-485 1-486 1-487 1-488 1-489 1-490 1-491 1-492 1-493 1-494 1-495 1-496 1-497 1-498 1-499 1-500 1-501 1-502 1-503 1-504 1-505 1-506 1-507 1-508 1-509 1-510 1-511 1-512 1-513 1-514 1-515 1-516 1-517 1-518 1-519 1-520 1-521 1-522 1-523 1-524 1-525 1-526 1-527 1-528 1-529 1-530 1-531 1-532 1-533 1-534 1-535 1-536 1-537 1-538 1-539 1-540 1-541 1-542 1-543 1-544 1-545 1-546 1-547 1-548 1-549 1-550 1-551 1-552 1-553 1-554 1-555 1-556 1-557 1-558 1-559 1-560 1-561 1-562 1-563 1-564 1-565 1-566 1-567 1-568 1-569 1-570 1-571 1-572 1-573 1-574 1-575 1-576 1-577 1-578 1-579 1-580 1-581 1-582 1-583 1-584 1-585 1-586 1-587 1-588 1-589 1-590 1-591 1-592 1-593 1-594 1-595 1-596 1-597 1-598 1-599 1-600 1-601 1-602 1-603 1-604 1-605 1-606 1-607 1-608 1-609 1-610 1-611 1-612 1-613 1-614 1-615 1-616 1-617 1-618 1-619 1-620 1-621 1-622 1-623 1-624 1-625 1-626 1-627 1-628 1-629 1-630 1-631 1-632 1-633 1-634 1-635 1-636 1-637 1-638 1-639 1-640 1-641 1-642 1-643 1-644 1-645 1-646 1-647 1-648 1-649 1-650 1-651 1-652 1-653 1-654 1-655 1-656 1-657 1-658 1-659 1-660 1-661 1-662 1-663 1-664 1-665 1-666 1-667 1-668 1-669 1-670 1-671 1-672 1-673 1-674 1-675 1-676 1-677 1-678 1-679 1-680 1-681 1-682 1-683 1-684 1-685 1-686 1-687 1-688 1-689 1-690 1-691 1-692 1-693 1-694 1-695 1-696 1-697 1-698 1-699 1-700 1-701 1-702 1-703 1-704 1-705 1-706 1-

1. The first step is to identify the problem or question that needs to be answered. This involves understanding the context and the specific requirements of the task.

2. Next, it is important to gather relevant information and data. This can be done through research, consultation with experts, or by analyzing existing data sets.

3. Once the information is gathered, the next step is to develop a plan or strategy to address the problem. This may involve breaking the problem down into smaller, more manageable parts.

4. The fourth step is to implement the plan. This involves putting the strategy into action and monitoring progress as you go.

5. Finally, it is important to evaluate the results of the process. This involves comparing the actual outcomes with the expected results and identifying any areas for improvement.

1. The first step is to identify the main components of the system. This involves understanding the hardware and software involved, as well as the data flow and control logic.

2. The second step is to define the system requirements. This includes specifying the functional requirements, performance requirements, and constraints.

3. The third step is to design the system architecture. This involves creating a high-level overview of the system and its components, as well as detailed designs for each component.

4. The fourth step is to implement the system. This involves writing the code, configuring the hardware, and testing the system.

5. The fifth step is to maintain the system. This involves monitoring the system's performance, updating the code and hardware as needed, and troubleshooting any issues.

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
29
30
31
32
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
84

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
29
30
31
32
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

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. 29. 30. 31. 32. 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. 84

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
29
30
31
32
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
84

[illegible][illegible]

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
 29
 30
 31
 32
 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

ATTACHMENT B

Lavabit uses 2048-bit Secure Socket Layer (SSL) certificates purchased from GoDaddy to encrypt communication between users and its server. SSL encryption employs public-key cryptography, in which both the sender and receiver each have two mathematically linked keys: a "public" key and a "private" key. "Public" keys are published, but "private" keys are not. In this circumstance, a Lavabit customer uses Lavabit's published public key to initiate an encrypted email session with Lavabit over the internet. Lavabit's servers then decrypt this traffic using their private key. The only way to decrypt this traffic is through the usage of this private key. A SSL certificate is another name for a published public key.

To obtain a SSL certificate from GoDaddy, a user needs to first generate a 2048-bit private key on his/her computer. Depending on the operating system and web server used, there are multiple ways to generate a private key. One of the more popular methods is to use a freely available command-line tool called OpenSSL. This generation also creates a certificate signing request file. The user sends this file to the SSL generation authority (e.g. GoDaddy) and GoDaddy then sends back the SSL certificate. The private key is not sent to GoDaddy and should be retained by the user. This private key is stored on the user's web server to permit decryption of internet traffic, as described above. The FBI's collection system that will be installed to implement the PR/TT also requires the private key to be stored to decrypt Lavabit email and internet traffic. This decrypted traffic will then be filtered for the target email address specified in the PR/TT order.

Depending on how exactly the private key was first generated by the user, it itself may be encrypted and protected by a password supplied by the user. This additional level of security is useful if, for example, a backup copy of the private key is stored on a CD. If that CD was lost or stolen, the private key would not be compromised because a password would be required to access it. However, the user that generated the private key would have supplied it at generation time and would thus have knowledge of it. The OpenSSL tool described above is capable of decrypting encrypted private keys and converting the keys to a non-encrypted format with a simple, well-documented command. The FBI's collection system and most web servers requires the key to be stored in a non-encrypted format.

A 2048-bit key is composed of 512 characters. The standard practice of exchanging private SSL keys between entities is to use some electronic medium (e.g., CD or secure internet exchange). SSL keys are rarely, if ever, exchanged verbally or through print medium due to their long length and possibility of human error. Mr. Levison has previously stated that Lavabit actually uses five separate public/private key pairs, one for each type of mail protocol used by Lavabit.

PEM format is an industry-standard file format for digitally representing SSL keys. PEM files can easily be created using the OpenSSL tool described above. The preferred medium for receiving these keys would be on a CD.