IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DENNIS MONTGOMERY, et al

Plaintiffs,

v.

JAMES COMEY, et al

Defendants.

Case No: 17-cv-1074

PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

Pursuant to Fed R. Civ. P. 65 and LCvR 65.1, Plaintiffs Dennis Montgomery and Larry Klayman hereby move this Court to issue a Temporary Restraining Order and Preliminary Injunction enjoining Defendants from (1) illegally and unconstitutionally spying on and surveilling millions of Americans, including Plaintiffs, without probable cause or a warrant, and (2) destroying evidence of illegal and unconstitutional spying turned over to Defendant Comey and the FBI by Plaintiff Montgomery.

In support of this motion, Plaintiffs rely upon the attached Memorandum of Points and Authorities and Exhibits attached thereto. Oral argument is requested.

Dated: June 19, 2017

Respectfully submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
KLAYMAN LAW GROUP, P.A.
D.C. Bar No. 334581
7050 W. Palmetto Park Rd, #15-287
Boca Raton, FL, 33433
Tel: (561)-558-5536

Email: leklayman@gmail.com

Attorney for Plaintiffs

TABLE OF AUTHORITIES

Cases

Statutes and Rules

TABLE OF CONTENTS

MEMORANDUM OF POINTS AND AUTHORITIES

Plaintiffs Dennis Montgomery and Larry Klayman ("Plaintiffs" unless individually named) hereby file a motion for a temporary restraining order and preliminary injunction to enjoin the Defendants James Comey ("Defendant Comey"), Federal Bureau of Investigation ("FBI"), Michael S. Rogers ("Defendant Rogers"), National Security Agency ("NSA"), John Brennan ("Defendant Brennan"), Mike Pompeo ("Defendant Pompeo"), Central Intelligence Agency ("CIA"), James R. Clapper ("Defendant Clapper"), Dan Coats ("Defendant Coats"), and Barack Obama ("Defendant Obama") (collectively "Defendants" unless individually named) from (1) illegally and unconstitutionally spying on and surveilling millions of Americans, including Plaintiffs, without probable cause or a warrant, and (2) destroying evidence of illegal and unconstitutional spying turned over to Defendant Comey and the FBI by Plaintiff Montgomery. Pursuant to LCvR 65.1(d), generally, "a hearing on an application for preliminary injunction shall be set by the Court no later than 21 days after its filing…." Thus, Plaintiffs respectfully request that this Court set a hearing date for an evidentiary hearing and oral argument on Plaintiffs' Temporary Restraining Order and Preliminary Injunction at this Court's earliest possible convenience, given the imminent irreparable injury to Plaintiffs as set forth in detail below.

I. INTRODUCTION

Defendants, each and every one of them, have engaged in an ongoing conspiracy to illegally and unconstitutionally spy on millions of Americans, including Plaintiffs, without probable cause or a warrant. Defendants continue to engage in this illegal, unconstitutional

conduct despite the fact that this very Court, in *Klayman v. Obama*,[1] issued two preliminary injunctions, including one that "bars the Government from collecting…any telephone metadata associated with these plaintiffs' Verizon Business Network Services accounts and…requires the Government to segregate any such metadata in its possession that has already been collected.", ECF No. 158 at 42-43. Now, Defendants have again targeted Plaintiffs Montgomery and Klayman as part of their ongoing and continuing illegal and unconstitutional surveillance programs, which are set forth in detail below. In this regard, Plaintiffs respectfully request that this Court issue a temporary restraining order and preliminary injunction requested herein in order to avoid clear, irreparable injury to Plaintiffs, as set forth below.

II. STATEMENT OF RELEVANT FACTS

A. Defendants' Ongoing, Illegal, and Unconstitutional Surveillance Has Been Revealed in the Public Domain

Recent revelations have confirmed that Defendants have continued to engage in massive, illegal surveillance, which is still ongoing. Defendants' conduct is in clear violation of Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). This has been confirmed by a recently declassified order (the "Order") from and of the Foreign Intelligence Surveillance Court ("FISC"), which this Court may take judicial notice of, as a matter of public record.[2] As set forth in the Order, Defendants, each and every one of them, have continued their pattern and practice of illegally and unconstitutionally spying on millions of Americans, and Plaintiffs, in violation of Section 702 of the FISA. Indeed, as recently as October 24, 2016, by its own admission:

[1] 13-cv-851 (D.C.D).
[2] *Memorandum Opinion and Order*, April 26, 2017, available at: https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf

> [T]he government orally apprised the Court of significant non-compliance with the NSA's minimization procedures involving questions of data acquired under Section 702 using U.S. person identifiers." Order at 4.

In particular, the FBI - under the orders and direction of Defendant Comey and those acting in concert with him– were gross offenders of the FISA, as the Order "chronicles nearly 10 pages listing hundreds of violations of the FBI's privacy-protecting minimization rules that occurred on [Defendant] Comey's watch."[3]

> The behavior the FBI admitted to a FISA judge just last month ranged from illegally sharing raw intelligence with unauthorized third parties to accessing intercepted attorney-client privileged communications without proper oversight the bureau promised was in place years ago.[4]

Accordingly, the FISC took Defendant Comey and the FBI to task in the Order, finding that:

> The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI may be engaging in similar disclosures of raw Section 702 information that have not been reported.

Order at 87. A report from Circa News corroborates the findings made by the FISC in the Order.

> The FBI has illegally shared raw intelligence about Americans with unauthorized third parties and violated other constitutional privacy protections, according to newly declassified government documents that undercut the bureau's public assurances about how carefully it handles warrantless spy data to avoid abuses or leaks….Once-top secret U.S. intelligence community memos reviewed by Circa tell a different story, citing instances of "disregard" for rules, inadequate training and "deficient" oversight and even one case of deliberately sharing spy data with a forbidden party…. The behavior the FBI admitted to a FISA judge just last month ranged from illegally sharing raw intelligence with unauthorized third parties to accessing intercepted attorney-client privileged communications without proper oversight the bureau promised was in place years ago. [5]
>
> The Justice Department inspector general's office declassified a report in 2015 that reveals the internal watchdog had concerns as early as 2012 that the FBI was submitting 'deficient" reports indicating it had a clean record complying with spy

[3] John Solomon, Sara Carter, *Declassified Memos Show FBI Illegally Shared Spy Data On Americans With Private Parties*, Circa, May 25, 2017, available at: http://circa.com/politics/declassified-memos-show-fbi-illegally-shared-spy-data-on-americans-with-private-parties.
[4] *Id*.
[5] *Id*.

> data gathered on Americans without a warrant. The FBI normally is forbidden from surveilling an American without a warrant. But Section 702 of the Foreign Surveillance Act, last updated by Congress in 2008, allowed the NSA to share with the FBI spy data collected without a warrant that includes the communications of Americans with "foreign targets." But the FISA court watchdogs suggest FBI compliance problems began months after Section 702 was implemented. [6]
>
> Amy Jeffress, the former top security adviser to former Attorney General Eric Holder, was appointed by the intelligence court in 2015 to give an independent assessment of the FBI's record of compliance. Jeffress concluded agents' searches of NSA data now extend far beyond national security issues and thus were "overstepping" the constitutional protections designed to ensure the bureau isn't violating Americans' 4th Amendment protections against unlawful search and seizure. "The FBI procedures allow for really virtually unrestricted querying of the Section 702 data in a way the NSA and CIA have restrained it through their procedures," she argued before the court in a sealed 2015 proceeding.[7]

Exhibit A. Circa News also revealed that Defendant Obama, and the Defendants acting in concert with him, "distribut[ed] thousands of intelligence reports across government with the unredacted names of U.S. residents during the midst of a divisive 2016 presidential election."[8]

> The data, made available this week by the Office of the Director of National Intelligence, provides the clearest evidence to date of how information accidentally collected by the NSA overseas about Americans was subsequently searched and disseminated after President Obama loosened privacy protections to make such sharing easier in 2011 in the name of national security….The revelations are particularly sensitive since the NSA is legally forbidden from directly spying on Americans and its authority to conduct warrantless searches on foreigners is up for renewal in Congress later this year. And it comes as lawmakers investigate President Trump's own claims that his privacy was violated by his predecessor during the 2016 election. In all, government officials conducted 30,355 searches in 2016 seeking information about Americans in NSA intercept metadata, which include telephone numbers and email addresses. The activity amounted to a 27.5 percent increase over the prior year and more than triple the 9,500 such searches that occurred in 2013, the first year such data was kept. The government in 2016 also scoured the actual contents of NSA

[6] *Id*.
[7] *Id*. (emphasis added)
[8] John Solomon, *President Obama's Team Sought NSA Intel on Thousands of Americans During the 2016 Election*, Circa News, May 4, 2017, available at: http://circa.com/politics/president-obamas-team-sought-nsa-intel-on-thousands-of-americans-during-the-2016-election

> intercepted calls and emails for 5,288 Americans, an increase of 13 percent over the prior year and a massive spike from the 198 names searched in 2013.[9]
>
> Among those whose names were unmasked in 2016 or early 2017 were campaign or transition associates of President Trump as well as members of Congress and their staffers, according to sources with direct knowledge.[10]

Furthermore, WikiLeaks recently revealed that Defendants, including the CIA, "developed malware -- bearing names such as "Assassin" and "Medusa" - intended to target iPhones, Android phones, smart TVs and Microsoft, and Mac and Linux operating systems, among others. Exhibit B. An entire unit in the CIA is devoted to inventing programs to hack data from Apple products."[11]According to the WikiLeaks leaks, "[s]ome of the remote hacking programs can allegedly turn numerous electronic devices into recording and transmitting stations to spy on their targets, with the information then sent back to secret CIA servers." "One document appears to show the CIA was trying to 'infect' vehicle control systems in cars and trucks for unspecified means." "WikiLeaks hinted that the capabilities revealed in Tuesday's disclosure could have even darker utility than simply spying. 'It would permit the CIA to engage in nearly undetectable assassinations….'" [12] Furthermore, "[a]s an example, specific CIA malware revealed in 'Year Zero' is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts," the WikiLeaks release stated.[13]

Thus, based on the foregoing, it is clear that Defendants are continuing to engage in unconstitutional and illegal warrantless surveillance in violation of Section 702 of FISA. Thus, it

---

[9] *Id*.
[10] *Id*.
[11] Cody Derespina, *WikiLeaks Releases 'Entire Hacking Capacity of the CIA'*, Fox News, Mar. 7, 2017, available at: http://www.foxnews.com/us/2017/03/07/wikileaks-releases-entire-hacking-capacity-cia.html
[12] *Id*.
[13] *Id*.

is abundantly clear that Defendants' misconduct does and will continue regardless of what the law says, and as such, may only be remedied by the relief sought herein.

B. Plaintiffs Montgomery and Klayman Have Been the Target of Defendants' Illegal and Unconstitutional Spying and Surveillance

Indeed, Plaintiffs Montgomery and Klayman have worked visibly, in the public eye, to raise awareness of, and demand an investigation into, Defendant Comey's illegal obstruction of justice and the FBI's concerted illegal actions in conjunction with the CIA, NSA, and DNI, and their respective leaders and directors, to cover up evidence of mass illegal and unconstitutional spying and surveillance.

1. Plaintiff Montgomery

Plaintiff Montgomery is a former NSA, CIA, and Director of National Intelligence ("DNI") contractor and whistleblower who has intimate knowledge of Defendants', each and every one them, acting individually and in concert, longstanding pattern and practice of conducting illegal, unconstitutional surveillance on millions of Americans. *See* Exhibit C; *Affidavit of Dennis Montgomery*. On August 19, 2015 Plaintiff Montgomery was induced by Defendants Comey and the FBI and made to turn over 47 hard drives and 600,000,000 pages of evidence of the aforementioned illegal, unconstitutional activity, which hard drives alone are valued in excess of $50,000 dollars. Counsel for Montgomery, Plaintiff Klayman, was told and assured by the former General Counsel of the FBI, James Baker, that Defendant Comey was taking "hands on" supervision and conducting the FBI's Montgomery investigation, given its importance. As a result, on or about December 21, 2015, Plaintiff Montgomery was interviewed under oath at the FBI Field Office in the District of Columbia. There, over the course of an over three-hour interview, recorded on video, with Special Agents Walter Giardina and William

Barnett, Plaintiff Montgomery meticulously laid out the NSA, CIA, DNI's, and the other Defendants' – particularly Defendants Clapper and Brennan's - pattern and practice of conducting illegal, unconstitutional surveillance against millions of Americans, including prominent Americans such as the chief justice of the U.S. Supreme Court, other justices, 156 judges, prominent businessmen, and others such as Donald J. Trump, as well as Plaintiffs themselves. Plaintiffs again were assured that the FBI, under Defendant Comey, would conduct a full investigation into the grave instances of illegal and unconstitutional activity set forth by Plaintiff Montgomery. In fact, Plaintiff Montgomery was given immunity by the FBI for his evidence and testimony. However, the FBI, on Defendant Comey's orders, buried the FBI's investigation because the FBI itself is involved in an ongoing conspiracy to not only conduct the aforementioned illegal, unconstitutional surveillance, but also to cover it up as well. Thus, the FBI, under the leadership of, and at the direction of Defendant Comey, has engaged a massive scheme to cover up the fact that Defendants NSA, CIA, and DNI, and their respective directors and leaders, as well as Defendants Obama, Brennan, Clapper, Rogers, and Coats have continued to engage in ongoing, unlawful, and unconstitutional mass surveillance. In short, the FBI, under Defendant Comey, itself collaborates with, and continues to collaborate with, the Defendant spy agencies to conduct illegal surveillance. *See* Exhibit C.

Since the December 21, 2015 interview with Special Agents Giardina and Barnett, Plaintiff Montgomery has since been the victim of multiple hacking attempts against his home and business computers from Defendants, each and every one of them. Upon tracing the IP addresses of the origination of the hacking attempts, Plaintiff Montgomery discovered that numerous attempts also came from the FBI's Criminal Justice Information Systems office in Clarksburg, West Virginia. Upon tracing the IP addresses of the origination of the hacking

attempts, Plaintiff Montgomery discovered that numerous attempts also came from the Department of Defense's Network Information Center in Columbus, Ohio. Upon tracing the IP addresses of the origination of the hacking attempts, Plaintiff Montgomery discovered that numerous attempts also came from the the CIA in Washington, DC. In March of 2017, Plaintiff Montgomery was also notified that his Apple account was hacked. Upon tracing the IP addresses of the origination of the hacking attempts, Plaintiff Montgomery discovered that the attempt came from the CIA in Langley, Virginia. Exhibit C.

2. Plaintiff Klayman

Plaintiff Klayman has met and communicated with the House Intelligence Committee, the Senate Intelligence Committee, the House Judiciary Committee, and the Senate Judiciary Committee and their members and staffs regarding the illegal and unconstitutional spying and surveillance at issue, and on behalf of Plaintiff Montgomery and himself, asked them to investigate Defendant Comey and the FBI's cover-up, and related matters involving Defendants' illegal and unconstitutional surveillance. *See* Exhibit D; *Affidavit of Larry Klayman*. Since Plaintiff Klayman has begun representing Plaintiff Montgomery in his whistleblowing attempts, Plaintiff Klayman has noticed objectively verifiable signals that he has been the subject of ongoing illegal surveillance. Plaintiff Klayman received a purported "software update" on his Samsung Galaxy S7 Edge Verizon cellular phone. After installing the software update, Plaintiff Klayman's phone began acting abnormally, including but not limited to the battery draining at an exponential rate as well as numerous other abnormalities. Plaintiff Klayman took his phone in to two different Verizon Wireless stores, where technicians confirmed to him that the effects from the purported "software update" were not normal, highly suspect, and not the result of either the phone or normal software. Plaintiff Montgomery informed Plaintiff Klayman that this is the way

that Defendants install malware used in spying in the phones of surveilled persons. Plaintiff Montgomery has confirmed that battery drainage is a tell-tale sign that the Defendants have successfully hacked into a cellular phone and that Defendants often insert malware onto recipients' phones using fake "software updates. As a result of Defendants' multiple hacking attempts, Plaintiff Klayman was forced to purchase a new Samsung Galaxy S8 phone. As recent as May of 2017, Plaintiff Klayman's Verizon Wireless Samsung Galaxy S8 phone began acting abnormally again, including but not limited to the battery draining at an exponential rate, as well as erasing and downloading files on its own and without Plaintiff Klayman's consent. Plaintiff Klayman took his phone in to another Verizon Wireless store where technicians confirmed that the phone was not acting normally. *See* Exhibit D.

III. LEGAL STANDARD

Plaintiffs seek both a temporary restraining order and preliminary injunctive relief. "The same standard applies to both temporary restraining orders and to preliminary injunctions." *Hall v. Johnson*, 599 F.Supp.2d 1, 6 n. 2 (D.D.C. 2009). Thus, the elements that Plaintiffs need only show to obtain a temporary restraining order are the same as those necessary to obtain a preliminary injunction.

When ruling on a motion for preliminary injunction [or a temporary restraining order], a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.*, 627 F.3rd 891, 893 (D.D.C. 2010) (internal quotation marks omitted); *Washington Metro. Area Transit Comm'n v. Holiday Tours, Inc*., 559 F.2d 841, 843 (D.C. Cir. 1977).

The D.C. Circuit has traditionally applied a 'sliding scale' approach to these four factors, viewing them as a continuum where greater strength in one factor compensates for less in the other: "If the arguments for one factor are particularly strong, an injunction may issue even if the arguments in other areas are rather weak." *CityFed Financial Corp. v. Office of Thrift Supervision*, 58 F.3d 739, 747 (D.C. Cir. 1995); *Davis v. Pension Benefit Guar. Corp.*, 571 F.3rd 1288, 1291 (D.C. Cir. 2009). In other words, "a strong showing on one factor could make up for a weaker showing on another." *Sherley v. Sebelius*, 644. F.3d 388, 392 (D.C. Cir. 2011).

IV. LEGAL ANALYSIS

A. Plaintiffs are Entitled to a Temporary Restraining Order and a Preliminary Injunction Enjoining Defendants From Conducting Illegal, Unconstitutional, and Warrantless Surveillance Against Plaintiffs

1. Substantial Likelihood of Success on the Merits

The Fourth Amendment to the U.S. Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The purpose of the Fourth Amendment, "as recognized in countless decisions [by the Supreme Court], is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Court*, 387 U.S. 523, 528 (1967) ("The Fourth Amendment [ ] gives concrete expression to a right of the people which 'is basic to a free society.'"). "An essential purpose of a warrant requirement is to protect privacy interests by assuring citizens subject to a search or seizure that such intrusions are not the random or arbitrary acts of government agents." *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 621-22 (1989).

To the extent that Defendants may attempt to argue that Plaintiff's requested relief is moot because the conduct to be enjoined has been been disallowed by the passage of the USA Freedom Act, such argument clearly fails based on the recent revelations of Circa News, WikiLeaks, and the FISC set forth in *supra* section II(A). These sources clearly show that Defendants are still engaging in massive unconstitutional and illegal surveillance despite the passage of the USA Freedom Act. Thus, the mere fact that the law has been changed is clearly of no consequence, and serves as no form of deterrence to Defendants' ongoing illegal and unconstitutional spying and surveillance. The "voluntary cessation" exception to the mootness doctrine does not apply here, either. "As a general rule, a defendant's voluntary cessation of allegedly illegal conduct does not deprive a court of power to hear and determine the case." *American Bar Association v. FTC*, 636 F.3d 641, 648 (D.C. Cir. 2011). The "rationale supporting voluntary cessation as an exception to mootness is that, without an order from the Court preventing [the defendant] from continuing the allegedly illegal practice, the defendant [would be] free to return to its old ways[,] thereby subjecting the plaintiff to the same harm but, at the same time, avoiding judicial review." *Jackson v. U.S. Parole Comm'n*, 806 F. Supp. 2d 201, 207-08 (D.D.C. 2011) (citation omitted); *see also Clarke v. United States*, 915 F.2d 699, 705 (D.C. Cir. 1990) (exception developed to prevent private defendants from "manipulating the judicial process").

a. Plaintiffs Have a Reasonable Expectation of Privacy

"A person generally has a reasonable expectation of privacy in the contents of his computer." *Palmieri v. United States*, 72 F. Supp. 3d 191, 210 (D.D.C. Nov. 3, 2014). This rule is well-decided and followed by numerous circuits. *See generally*, *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir.

2007*); United States v. Lifshitz,* 369 F.3d 173, 190 (2d Cir. 2004); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). A person's reasonable expectation of privacy in the contents of his computer may only be extinguished when the "computer user disseminates information to the public…" *Palmieri*, 72 F. Supp. 3d at 210.

Here, Plaintiff Montgomery's computer was the subject of numerous hacking attempts by Defendants, as set forth in *supra* section III(B)(1). Plaintiff Montgomery did not disseminate the information contained on his computer to the public, and has taken steps to maintain the secrecy of the contents therein. Thus, Defendants clearly and unequivocally violated Plaintiff Montgomery's reasonable expectation of privacy on his computer by hacking and retrieving content from Plaintiff Montgomery's computer.

Furthermore, this Court has already determined that cell phone users too enjoy a reasonable expectation of privacy in its November 9, 2015 Memorandum Opinion granting the preliminary injunction in *Klayman v. Obama*:

> Furthermore, the attitude with which cellphone users approach their devices presents a dramatically different context than the contexts in which courts have upheld "special needs" searches. Specifically, cellular phone technology does not present the same diminished expectation of privacy that typically characterizes "special needs" incursions. Take, for example, airports. In the context of air travel, courts have recognized that "society has long accepted a heightened level of security and privacy intrusion with regard to air travel." *Cassidy v. Chertoff*, 471 F.3d 67, 76 (2d Cir. 2006). Notably, Americans know that airports are discrete areas in which certain rights otherwise enjoyed are forfeited. *See id.* It is their choice to enter that space and, in so doing, to check certain rights at the door. Not so with cellphones. As already described, cellphones have become a constant presence in people's lives. While plaintiffs' privacy interests in their aggregated metadata may be somewhat diminished by the fact that it is held by third-party service providers, this is a *necessary* reality if one is to use a cellphone at all, and it is, therefore, simply not analogous to the context of voluntarily entering an airport. In this case, plaintiffs have asserted that the NSA's searches were a substantial intrusion on their privacy, and I have no reason to doubt that, nor to find that their privacy expectations should have been

> diminished given the context. Rather, I conclude that plaintiffs' privacy interests are robust.

Klayman v. Obama, 142 F. Supp. 3d 172, 191 (D.D.C. Nov. 9, 2015) (emphasis added). As set forth previously in *supra* section III(B)(2), Plaintiff Klayman has been the target of illegal, warrantless surveillance and spying by Defendants on his cell phone, to the extent that he has had to replace his cell phone twice in the past few months. This too is in clear violation of Mr. Klayman's reasonable expectation of privacy in his cell phone, as recognized by the Honorable Richard J. Leon ("Judge Leon") in this Court previously.

b. Defendants' Intrusion is Unreasonable

"The Fourth Amendment prohibits unreasonable searches. Whether a search is reasonable depends on the totality of the circumstances. Typically, searches not conducted pursuant to a warrant based on the requisite showing of probable cause are "*per se* unreasonable." *Klayman v. Obama*, 142 F. Supp. 3d 172, 189 (D.D.C. Nov. 9, 2015) (internal citations omitted). As set forth previously, Defendant's searches of Plaintiffs were made without a warrant or probable cause, and are, therefore, "*per se* unreasonable."

The narrow exception to this well-decided rule is when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987). However, as this Court in *Klayman v. Obama* already found, the "special needs" exception is inapplicable, since "plaintiffs [had] a substantial likelihood of showing that their privacy interests outweigh[ed] the Government's interest…." *Klayman v. Obama*, 142 F. Supp. 3d 172, 190 (D.D.C. Nov. 9, 2015).

2. Plaintiffs Would Suffer Irreparable Injury

It has long been established that the loss of constitutional freedoms, "for even minimal

periods of time, unquestionably constitutes irreparable injury." *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion)). In *Mills*, after finding a strong likelihood of success on the merits, the U.S. Court of Appeals for the D.C. Circuit had little to say on the irreparable injury prong, instead relying on the statement at the beginning of this paragraph that a constitutional violation, even of minimal duration, constitutes irreparable injury. As Plaintiffs in this case have shown a strong likelihood of success on the merits of a Fourth Amendment claim, they too have adequately demonstrated irreparable injury. Thus, Plaintiffs are entitled to both a temporary restraining order and preliminary injunctive relief.

3. A Temporary Restraining Order and Preliminary Injunction Would Not Substantially Injure Any Other Interested Parties

In *Klayman v. Obama*, the Government asserted that enjoining them from conducting illegal, unconstitutional searches would interfere with the public's interest in combating terrorism. Fortunately, Judge Leon saw through this vague, meritless assertion, stating:

> But the Government offers no real explanation as to how granting relief to these plaintiffs would be detrimental to that interest. Instead, the Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database…. Of course, the public has no interest in saving the Government from the burdens of complying with the Constitution! Then, the Government frets that such an order "could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants."….For reasons already explained, I am not convinced at this point in the litigation that the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so I am *certainly* not convinced that the removal of two individuals from the database will "degrade" the program in any meaningful sense.

Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. Dec. 16, 2013) (internal citations omitted). The same line of reasoning is applicable here, as an injunction against warrantless, illegal, and

unconstitutional surveillance against Plaintiffs Montgomery and Klayman could not possibly "degrade" Defendants' surveillance programs in any "meaningful sense." Neither Plaintiffs Montgomery nor Klayman pose any threat to national security, nor do they have any ties to terrorism. Plaintiff Klayman is a former U.S. Department of Justice attorney and an officer of the court. Exhibit D. Plaintiff Montgomery is a former contractor for the NSA, CIA, and the DNI who still has a security clearance. Exhibit C. Thus, Defendants' interest in continuing to illegally, unconstitutionally, and warrantless surveille Plaintiffs is entirely non-existent.

4. A Temporary Restraining Order and Preliminary Injunction Further the Public Interest

"[I]t is always in the public interest to prevent the violation of a party's constitutional rights.'" *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.*, 898 F.Supp.2d 73, 84 (D.D.C. 2012) (internal quotations and citations omitted); *see also Nat'l Fed'n of Fed. Emps. v. Carlucci*, 680 F. Supp. 416 (D.D.C. 1988) ("[T]he public interest lies in enjoining unconstitutional searches."). Here, the Fourth Amendment rights of Plaintiffs, as well as millions of Americans at large, have been, and continue to be violated by the illegal and unconstitutional conduct of Defendants. As such, an injunction enjoining Defendants' illegal and unconstitutional surveillance is clearly in the public's interest.

B. Plaintiff Montgomery is Entitled to a Temporary Restraining Order and a Preliminary Injunction Enjoining Defendants From Destroying Evidence of their Constitutional Violations Contained on Plaintiff Montgomery's Hard Drives and Other Property and From Conversion of Plaintiff's Property

1. Substantial Likelihood of Success of the Merits

"A substantial likelihood of success on the merits is shown if good reasons for anticipating that result are demonstrated," the plaintiff "demonstrate[s] a prima facie, clear legal right to the relief requested." *City of Jacksonville v. Naegele Outdoor Advertising Co.*, 634 So.2d

750, 753 (Fla. 1st DCA 1994). Plaintiffs are likely to succeed on the merits of their case, as Defendants' actions outlined in the Complaint are a clear violation of their Fourth Amendment right to protection against unreasonable search and seizure. *Supra* section IV(A).

Plaintiff Montgomery is also likely to succeed on his conversion claim against Defendants Comey and FBI. Montgomery, a former contractor for the CIA, NSA, and DNI and a whistleblower who has revealed the grand scale of the illegal surveillance of the American people perpetrated by Defendants, was induced to turn over hard drives containing evidence of the ongoing illegal and unconstitutional surveillance to Defendant Comey and the FBI under the promise that Defendant Comey would oversee a full investigation into Plaintiff Montgomery's revelations. Exhibit C. The 47 hard drives turned in to the FBI have a value in excess of $50,000 which Plaintiff Montgomery has not received back, despite several requests for their return. At all material times, the hard drives belonged to, and still belong to, Plaintiff Montgomery. Defendants FBI and Comey have exercised unlawful dominion and control over Plaintiff Montgomery's hard drives by refusing to return the hard drives the Plaintiff Montgomery. Exhibit C. Thus, Plaintiff Montgomery is likely to succeed on his claim for conversion against Defendants FBI and Comey.

2. Plaintiffs Would Suffer Irreparable Injury

Preservation of Plaintiff Montgomery's hard drives and video interviews with the FBI are crucial in proving Defendants' illegal conduct and unconstitutional spying of millions of Americans. Allowing the FBI to destroy this evidence would serve irreparable harm to Plaintiffs, as it is direct proof of Defendants' actions, on which this complaint is based. "Destruction of evidence may also rise to the level of irreparable harm", *see also. Am. Friends Serv. Comm. v. Webster,* 485 F. Supp. 222, 233 (D.D.C.1980) (finding that

the plaintiff "will suffer significant, irreparable injury if defendants' continuing destruction of FBI files [in accordance with its record destruction program] is not enjoined").

Indeed, Plaintiff Klayman has, on behalf of Plaintiff Montgomery, repeatedly asked for the return of Plaintiff Montgomery's hard drives. Exhibit D. Plaintiff Klayman has been ignored each time. Defendants FBI and Comey have also failed to respond to a Privacy Act request by Plaintiff Montgomery requesting "any and all documents that refer or relate in any way to any and all 302 reports of the interview in which Plaintiff Montgomery participated in with Special Agents Walter Giardina and William Barnett." Exhibit D. Defendant FBI has also ignored this request, which forms the basis for Plaintiffs' Sixth Cause of Action. Defendants FBI and Comey's stonewalling of Plaintiffs' requests raises the strong inference that they are hiding something, which, in turn, would lead Defendant FBI to destroy the evidence contained on Plaintiff Montgomery's hard drives and the video recording of his interview. In fact, the commencement of this action very likely served as the impetus for the FBI to actively destroy the evidence turned over by Montgomery, which necessitates an immediate temporary restraining order. If the FBI were to destroy the evidence, Plaintiffs would have no other proof of Defendants' activities and therefore, clearly suffer irreparable harm. *See also Citizens for Responsibility & Ethics in Washington v. Exec. Office of the President*, Civ. No. 07–1707 (D.D.C. Oct. 19, 2007) (JMF/HHK), Report and Recommendation at 3 ("[I]f, as [the plaintiff] contends, the e-mails have been deleted, then the backup media are the only place where they may be and the obliteration of this backup media obviously threatens [the plaintiff] with irreparable harm. Indeed, the threat of such obliteration is a text book example of irreparable harm.")

Furthermore, preservation of evidence is necessary so that it may be turned over the the

proper investigative bodies, including but not limited to the Office of the Inspector General, so that a thorough investigation into Defendants Comey and FBI's behavior in covering up the conspiracy between each and every Defendant to conduct massive, illegal, and unconstitutional surveillance may be performed. Allowing the imminent destruction of this evidence, should Plaintiffs' requested relief be denied, constitutes clear, irreparable harm.

Lastly, the hard drives themselves are material proof of Defendant Comey and FBI's illegal conversion of Plaintiff Montgomery's property, valued in excess of $50,000. Exhibit C. The danger of the FBI destroying this evidence is imminent and a true concern, as exemplified by their refusal to release both the hard drives and the interviews upon Plaintiffs' request. Thus, the irreparable harm to evidence that would result from Defendants' destruction of evidence is a highly likely probability that must be prevented by a temporary restraining order and preliminary injunctive relief.

3. A Temporary Restraining Order and Preliminary Injunction Would Not Substantially Injure Any Other Interested Parties

The purpose of preliminary injunctive relief is to preserve the status quo between the parties and to prevent irreparable injury until the merits of the lawsuit itself can be reviewed. *Devose v. Herrington*, 42 F.3d 470, 471 (8th Cir. 1994); *Penn v. San Juan Hosp*., 528 F.2d 1181, 1185 (10th Cir. 1975). It is of utmost importance that all evidence of Defendant's unconstitutional actions be preserved. The threatened injury to Plaintiffs heavily outweighs any possible damage to Defendants, which is non existent. Without preservation of Plaintiff's hard drives and interview tapes, Plaintiffs will lose the material evidence in this case. On the other hand, preservation of the evidence does not harm Defendants in any way. Any inconvenience to Defendants would be inconsequential compared to the harm that will be suffered by the

Plaintiffs.

4. A Temporary Restraining Order and Preliminary Injunction Further Public Interest

As this Court previously found: "`[I]t is always in the public interest to prevent the violation of a party's constitutional rights.'" *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.,* 898 F.Supp.2d 73, 84 (D.D.C. 2012) (quoting *G & V Lounge, Inc. v. Mich. Liquor Control Comm'n,* 23 F.3d 1071, 1079 (6th Cir. 1994)); *see also Hobby Lobby Stores, Inc. v.Sebelius,* 723 F.3d 1114, 1145 (10th Cir. 2013) (same), *cert. granted,* ___S. Ct.__, 2013 WL 5297798 (2013); *Melendres v. Arpaio,* 695 F.3d 990, 1002 (9th Cir. 2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci,* 680 F.Supp. 416 (D.D.C. 1988) ("[T]he public interest lies in enjoining unconstitutional searches."). Defendants violated the Fourth Amendment rights of Plaintiffs and **millions of other Americans** when they unreasonably searched and seized and continue to search phone and internet records without a warrant based on reasonable suspicion or probable cause. Therefore, the public interest would be best served by injunctive relief that would prevent the destruction of evidence of Defendants' constitutional violations. Finally, as to the conversion claim, the public has an interest in holding the government responsible for confiscating personal property without any compensation and remuneration. Plaintiff's hard drives are concrete proof that conversion occurred, and as such, this evidence must be preserved.

V. CONCLUSION

For the foregoing reasons, the Court should grant Plaintiffs' motion and enter a temporary restraining order and preliminary injunction to restrain Defendants from violating the Fourth Amendment and to ensure that they do not continue to violate constitutional rights, and to exercise continuing jurisdiction over such illegal surveillance to ensure compliance. This

continuing jurisdiction is necessary no matter what law is in effect, as the Government Defendants have engaged in a continuing practice of violating the constitutional rights of Plaintiffs and hundreds of millions of Americans, and then lying about it to Congress, the courts, and the American people. As held in *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns,* 427 U.S. 347, 373 (1976)), and as this Court has also recognized, one day of a constitutional violation, particularly of this magnitude and severity, is one day too many. Furthermore, the Court should grant Plaintiff's motion and enter a temporary restraining order and preliminary injunction to prevent the FBI from destroying Plaintiff Montgomery's 47 hard drives and 600,000,000 plus pages of information and recordings of his December 21, 2015 interview with the FBI. "The court has broad discretion when determining whether to order a party to preserve evidence." *In re African–American Slave Descendants' Litigation*, 2003 WL 24085346, *2 (N.D. Ill. July 15, 2003). The Court should grant such relief as these articles are decisive pieces of evidence in this action that will prove Defendants' violation of Plaintiffs' constitutional rights, and their unlawful conversion of Plaintiff Montgomery's property. Furthermore, preservation of evidence is necessary so that it may be used as evidence in this case and be turned over to the proper investigative bodies, including but not limited to the Office of the Inspector General of the U.S. Department of Justice and the House Intelligence Committee, the Senate Intelligence Committee, the House Judiciary Committee, and the Senate Judiciary Committee and their members and staffs so that a thorough investigation into Defendants Comey and FBI's behavior in covering up the conspiracy between each and every Defendant to conduct massive, illegal, and unconstitutional surveillance may be performed.

///

Dated: June 19, 2017

Respectfully submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
KLAYMAN LAW GROUP, P.A.
D.C. Bar No. 334581
7050 W. Palmetto Park Rd, #15-287
Boca Raton, FL, 33433
Tel: (561)-558-5536
Email: leklayman@gmail.com

Attorney for Plaintiffs

CERTIFICATE PURSUANT TO LCvR 65.1

I HEREBY CERTIFY that on June 19, 2017, I caused a copy of this Motion for Temporary Restraining Order and Accompanying Memorandum of Points and Authorities, along with copies of all pleadings and papers filed in the action to date or to be presented to the Court at the hearing to be sent via Federal Express overnight delivery service to each Defendant's last known address, set forth below:

James Comey
1350 Beverly Road
McLean, VA 22101

Barack Obama
2446 Belmont Rd.
Washington DC 20008

Michael S. Rogers
4628 English Ave
Fort George G Meade, MD 20755

Dan Coats
2041 Mayfair McLean Ct
Falls Church, VA 22043

James Clapper
5366 Ashleigh Rd
Fairfax, VA 22030

John Brennan
13351 Point Rider Ln
Herndon, VA 20171

Mike Pompeo
1350 Beverly Road
McLean, VA 22101

Federal Bureau of Investigation
935 Pennsylvania Ave, NW
Washington, DC, 20535

National Security Agency
9800 Savage Road, #6272

Ft George G. Meade, MD, 20755

Central Intelligence Agency
Office of Public Affairs
950 Pennsylvania Ave NW
Washington, DC, 20530

U.S. Attorney for the District of Columbia
555 4th Street NW
Washington, DC, 20530

Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Ave NW
Washington, DC, 20530

/s/ Larry Klayman
Larry Klayman, Esq.

EXHIBIT A

May 26, 2017

WATCH: Circa's Sara Carter explains the extensive nature in which raw intelligence was shared by the FBI.

1 of 33

The FBI has illegally shared raw intelligence about Americans with unauthorized third parties and violated other constitutional

privacy protections, according to newly declassified government documents that undercut the bureau's public assurances about how carefully it handles warrantless spy data to avoid abuses or leaks.

2 of 33

FISA court transcript

READ

3 of 33

In his final congressional testimony before he was fired by President Trump this month, then-FBI Director James Comey unequivocally told lawmakers his agency used sensitive espionage data gathered about Americans without a warrant only when it was "lawfully collected, carefully overseen and checked."

Once-top secret U.S. intelligence community memos reviewed by Circa tell a different story, citing instances of "disregard" for rules, inadequate training and "deficient" oversight and even one case of deliberately sharing spy data with a forbidden party

one case of deliberately sharing spy data with a forbidden party.

4 of 33

For instance, a ruling declassified this month by the Foreign Intelligence Surveillance Court (FISA) chronicles nearly 10 pages listing hundreds of violations of the FBI's privacy-protecting minimization rules that occurred on Comey's watch.

The behavior the FBI admitted to a FISA judge just last month ranged from illegally sharing raw intelligence with unauthorized third parties to accessing intercepted attorney-client privileged communications without proper oversight the bureau promised was in place years ago.

5 of 33

April 2017 FISA court document

READ

6 of 33

The court also opined aloud that it fears the violations are more

The court also opined aloud that it fears the violations are more extensive than already disclosed.

"The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI is engaging in similar disclosures of raw Section 702 information that have not been reported," the April 2017 ruling declared.

7 of 33

The court isn't the only oversight body to disclose recent concerns that the FBI's voluntary system for policing its behavior and self-disclosing mistakes hasn't been working.

The Justice Department inspector general's officedeclassified a report in 2015 that reveals the internal watchdog had concerns as early as 2012 that the FBI was submitting 'deficient" reports indicating it had a clean record complying with spy data gathered on Americans without a warrant.

8 of 33

The FBI normally is forbidden from surveilling an American without a warrant. But Section 702 of the Foreign Surveillance Act, last updated by Congress in 2008, allowed the NSA to share with the FBI spy data collected without a warrant that includes the communications of Americans with "foreign targets."

But the FISA court watchdogs suggest FBI compliance problems began months after Section 702 was implemented.

9 of 33

The FBI's very first compliance report in 2009 declared it had not found any instances in which agents accessed NSA intercepts supposedly gathered overseas about an American who in fact was on U.S. soil.

But the IG said it reviewed the same data and easily found evidence that the FBI accessed NSA data gathered on a person who likely was in the United States, making it illegal to review without a warrant.

10 of 33

Review of FBI activities under Section 702

READ

11 of 33

"We found several instances in which the FBI acquired communications on the same day that the NSA determined through analysis of intercepted communications that the person was in the United States," the declassified report revealed.

It called the FBI's first oversight report "deficient" and urged better oversight.

FBI officials acknowledged there have been violations but insist they are a small percentage of the total counterterrorism and counterintelligence work its agents perform.

12 of 33

Almost all are unintentional human errors by good-intentioned agents and analysts under enormous pressure to stop the next major terror attack, the officials said.

Others fear these blunders call into the question the bureau's rosy assessment that it can still police itself when it comes to protecting Americans' privacy 17 years after the war on terror began.

13 of 33

That doubt, heaviest among civil libertarian Democrats but also growing among Republicans, is particularly sensitive because the law that allows the bureau to access warrantless spy data about Americans - Section 702 of the Foreign Intelligence Surveillance Act - is up for renewal later this year.

Lawmakers in both parties and both chambers of Congress are writing reforms behind closed door, leaving the intelligence community anxious it might lose some of the spy powers it considers essential to fighting terrorism, cyber attacks and unlawful foreign influence.

14 of 33

"No one on the Hill wants to look like we are soft on terrorism when you have increasing threats like Manchester-style attacks. But the evidence of abuse or sloppiness and the unending leaks of sensitive intelligence in the last year has emboldened enough of us to pursue some reforms," a senior congressional aide told Circa, speaking only on condition of anonymity because he wasn't authorized to talk to the media. "Where that new line between privacy and security is drawn will depend on how many more shoes fall before the 702 renewal happens."

15 of 33

Rep. Trent Frank, R-Ariz., a member of the House Judiciary Committee that will help craft the 702 renewal legislation, said the rising revelation of problems about improper spying on Americans are having an effect on lawmakers who have long supported the intelligence community

supported the intelligence community.

“The bottom line is the law has to be followed and when it isn’t there has to be consequence that is of significance so that it deters others from breaking the same law,” he told Circa.

16 of 33

One of the biggest concerns involves so-called backdoor searches in which the FBI can mine NSA intercept data for information that may have been incidentally collected about an American. No warrant or court approval is required, and the FBI insists these searches are one of the most essential tools in combating terrorist plots.

17 of 33

But a respected former Justice Department national security prosecutor questions if the searching has gotten too cavalier. AmyJeffress, the former top security adviser to former Attorney General Eric Holder, was appointed by the intelligence court in 2015 to give anindependent assessmentof the FBI’s record of compliance.

18 of 33

October 2015 FISA court document

READ

19 of 33

Jeffress concluded agents' searches of NSA data now extend far beyond national security issues and thus were "overstepping" the constitutional protections designed to ensure the bureau isn't violating Americans' 4th Amendment protections against unlawful search and seizure.

"The FBI procedures allow for really virtually unrestricted querying of the Section 702 data in a way the NSA and CIA have restrained it through their procedures," she argued before the court in a sealed 2015 proceeding.

20 of 33

"I think that in this case the procedures could be tighter and more restrictive, and should be in order to comply with the Fourth Amendment," she added.

The court thanked Jeffress for her thoughtful analysis but ultimately rejected her recommendation to impose on the FBI a requirement of creating a written justification why each search would help pursue a national security or criminal matter.

21 of 33

The Justice Department argued in that matter that the extra restriction would keep FBI agents from connecting the dots in terror cases and compared NSA searches to something Americans do every day.

"If we require our agents to write a full justification every time think about if you wrote a full justification every time you used Google. Among other things, you would use Google a lot less," a lawyer told the court.

22 of 33

That was late in 2015. But by early 2017, the court became more concerned after the Obama administration disclosed significant violations of privacy protections at two separate intelligence agencies involved in the Section 702 program.

23 of 33

The most serious involved the NSA searching for American data it was forbidden to search. But the FBI also was forced to admit its agents and analysts shared espionage data with prohibited third parties, ranging from a federal contractor to a private entity that did not have the legal right to see the intelligence.

24 of 33

Such third-party sharing is a huge political concern now as Congress and intelligence community leaders try to stop the flow of classified information to parties that could illegally disclose or misuse it, such as the recent leak that disclosed intercepted communications between the Russian ambassador and Trump's first national security adviser, Michael Flynn.

25 of 33

The court's memo suggested the FBI's sharing of raw intelligence to third parties, at the time, had good law enforcement intentions but bad judgment and inadequate training.

"Nonetheless, the above described practices violated the governing minimization procedures," the court chided.

A footnote in the ruling stated one instance of improper sharing was likely intentional.

26 of 33

"Improper access" to NSA spy data for FBI contractors "seems

to have been the result of deliberate decision-making," the court noted.

The recently unsealed ruling also revealed the FBI is investigating more cases of possible improper sharing with private parties that recently have come to light.

The government "is investigating whether there have been similar cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems," the court warned.

27 of 33

The ruling cited other FBI failures in handling Section 702 intel, including retaining data on computer storage systems "in violation of applicable minimization requirements."

Among the most serious additional concerns was the FBI's failure for more than two years to establish review teams to ensure intercepts between targets and their lawyers aren't violating the attorney-client privilege.

28 of 33

"Failures of the FBI to comply with this 'review team' requirement for particular targets have been focus of the FISC's (FISA's?)

for particular targets have been focus of the FISC's (FISAs?)

concerns since 2014," the court noted.

The FBI said it is trying to resolve the deficiencies with aggressive training of agents.

That admission of inadequate training directly undercut Comey's testimony earlier this month when questioned by Sen. Dianne Feinstein, D-Calif.

29 of 33

"Nobody gets to see FISA information of any kind unless they've had the appropriate training and have the appropriate oversight," the soon-to-be-fired FBI director assured lawmakers.

The struggle for the intelligence court and lawmakers in providing future oversight will be where to set more limits without hampering counterterrorism effort

30 of 33

The FBI told Circa in a statement, "As indicated in its opinion, the Court determined that the past and current standard minimization procedures are consistent with the Fourth Amendment and met the statutory definition of those procedures under Section 702."

under Section 702.

Jeffress, however, warned in her 2015 brief of another dynamic that will pose a challenge too, an FBI culture to use a tool more just because it can.

31 of 33

"These scenarios suggest a potentially very large and broad scope of incidental collection of communications between a lawful target and U.S. persons that are not the type of communications Section 702 was designed to collect," she told the court in a written memo.

And when questioned at a subsequent hearing, Jeffress observed: "I don't think that the FBI will voluntarily set limits on its querying procedures, because law enforcement agencies tend not to take steps to restrict or limit what they can do, for obvious reasons."

32 of 33

Circa congressional correspondent Kellan Howell contributed to this story.

EXHIBIT B

Print Close

WikiLeaks releases 'entire hacking capacity of the CIA'

By Cody Derespina

Published March 07, 2017

Fox News

WikiLeaks on Tuesday released what it said is the full hacking capacity of the CIA in a stunning 8,000-plus page disclosure the anti-secrecy website contends is “the largest ever publication of confidential documents on the agency.”

The 8,761 documents and files -- released as “Vault 7 Part 1” and titled “Year Zero” -- were obtained from an “isolated, high-security network” at the CIA’s Center for Cyber Intelligence in Langley, Va., a press release from the website said. The trove had been “circulated among former U.S. government hackers and contractors,” one of whom “recently” gave the archive to WikiLeaks. The CIA allegedly employs more than 5,000 people in its cyber spying operation and had produced more than 1,000 programs as of 2016.

“We do not comment on the authenticity or content of purported intelligence documents," a CIA spokesperson told Fox News.

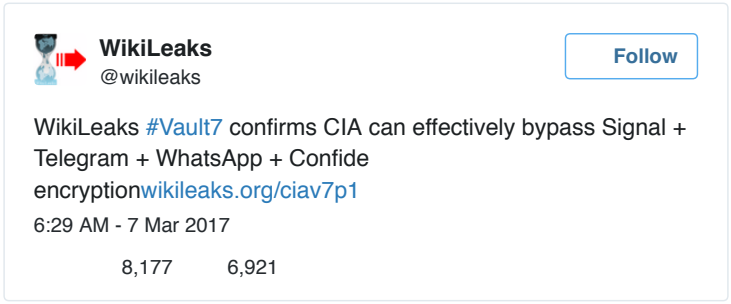
The collection of purported intelligence documents includes information on CIA-developed malware -- bearing names such as “Assassin” and “Medusa” -- intended to target iPhones, Android phones, smart TVs and Microsoft, Mac and Linux operating systems, among others. An entire unit in the CIA is devoted to inventing programs to hack data from Apple products, according to WikiLeaks.

WIKILEAKS OFFERS REWARD FOR INFO ON OBAMA MISDEEDS

Some of the remote hacking programs can allegedly turn numerous electronic devices into recording and transmitting stations to spy on their targets, with the information then sent back to secret CIA servers. One document appears to show the CIA was trying to “infect” vehicle control systems in cars and trucks for unspecified means.

WikiLeaks hinted that the capabilites revealed in Tuesday's disclosure could have even darker utility than simply spying.

“It would permit the CIA to engage in nearly undetectable assassinations,” the release stated.



FLASHBACK: WIKILEAKS REVEALS CLINTON 'HITS' FILE ON SANDERS

The site said the CIA additionally failed to disclose security vulnerabilities and bugs to major U.S. software manufacturers, violating an Obama administration commitment made in January 2014. Instead, the agency used the software vulnerabilities -- which could also be exploited by rival agencies, nations and groups -- for its own ends, WikiLeaks said.

WikiLeaks
@wikileaks

Follow

CIA hackers celebrated what they saw as the financial largesse of Obama towards them with "Make It Rain" gifwikileaks.org/ciav7p1/cms/fi…

6:57 AM - 7 Mar 2017

4,338 4,369

“As an example, specific CIA malware revealed in ‘Year Zero’ is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts,” the WikiLeaks release stated.

Digital rights non-profit Access Now said in a statement on Tuesday it was "fantasy to believe only the 'good guys'" would be able to use the discovered vulnerabilities.

“Today, our digital security has been compromised because the CIA has been stockpiling vulnerabilities rather than working with companies to patch them," Senior Legislative Manager Nathan White said.

The CIA allegedly also maintains a database of malware created in other nations -- WikiLeaks specifically cites Russia -- in order to disguise its own hacking attempts as the work of another group.

In what is described by WikiLeaks as "one of the most astounding intelligence own goals in living memory," the CIA is said to have made most of its programs unclassified to avoid legal consequences for transmitting classified information through the Internet -- a move that increased the risk of outside groups pirating the cyber spying tools.

WikiLeaks also revealed the U.S. Consulate in Frankfurt is a hacking base, and the website provided the methods by which agents obfuscate customs officers to gain entry to Germany, pretending to provide technical consultation.

WikiLeaks said its source released the files because they believed questions surrounding the CIA's reach "urgently need to be debated in public," echoing the motives of many previous leakers.

One such former leaker, Edward Snowden, tweeted Tuesday afternoon about the WikiLeaks release.

"Still working through the publication, but what @Wikileaks has here is genuinely a big deal. Looks authentic," wrote Snowden, who has been granted asylum in Russia as he seeks to avoid criminal prosecution in the U.S.

Some of the WikiLeaks files include redacted information, such as tens "of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States."

Print Close

URL

http://www.foxnews.com/us/2017/03/07/wikileaks-releases-entire-hacking-capacity-cia.html

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et al.*, Plaintiffs, v. JAMES COMEY, et al., Defendants.	Case No: 17-cv-1074

AFFIDAVIT OF DENNIS MONTGOMERY

1. My name is Dennis Montgomery, I am over 18 years old. I am an adult citizen of the United States and I am the Plaintiff in the above stated case. I have personal knowledge of the facts stated in this declaration.

2. I am a former National Security Agency ("NSA"), Central Intelligence Agency ("CIA"), and Director of National Intelligence ("DNI") contractor and/or whistleblower. I have worked with each of these groups at all material times on domestic surveillance programs.

3. I have intimate knowledge of Defendants', each and every one them, acting individually and in concert, longstanding pattern and practice of conducting illegal, unconstitutional surveillance on millions of Americans.

4. On August 19, 2015, I was induced by Defendants Comey and the Federal Bureau of Investigation ("FBI") and made to turn over 47 hard drives containing over 600,000,000 pages of data on 20 plus million Americans that are evidence of the aforementioned illegal, unconstitutional

activity. Much of the domestic data I collected on behalf of the US Government was collected on computers supplied by the FBI.

5. I am the owner of the hard drives and their contents.

6. The hard drives alone are valued in excess of $50,000 dollars.

7. I did not disseminate the classified information contained on the hard drives to the public, and have taken steps to maintain the secrecy of the contents therein.

8. My counsel, Plaintiff Larry Klayman, was told and assured by the former General Counsel of the FBI, James Baker, that Defendant Comey was taking "hands on" supervision and conducting my investigation, given its importance.

9. On or about December 21, 2015, I was interviewed under oath at the FBI Field Office in Washington, D.C. The FBI offered me immunity in exchange for my testimony.

10. There, over the course of an over three-hour interview, recorded on video, with Special Agents Walter Giardina and William Barnett, I described the NSA, CIA, DNI's, and the other Defendants' pattern and practice of conducting illegal, unconstitutional surveillance against millions of Americans, including prominent Americans such as the chief justice of the U.S. Supreme Court, other justices, 156 judges, prominent businessmen, and others such as Donald J. Trump, as well as Plaintiffs themselves.

11. I was assured that the FBI, under Defendant Comey, would conduct a full investigation into the grave instances of illegal and unconstitutional activity set forth by the information I provided.

12. However, the FBI, on Defendant Comey's orders, buried the FBI's investigation because the FBI itself is involved in an ongoing conspiracy to not only conduct the aforementioned illegal, unconstitutional surveillance, but to cover it up as well.

13. Circa News has disclosed that the FBI has illegally shared raw intelligence about Americans

with unauthorized third parties and violated other constitutional privacy protections, according to newly declassified government documents.[1]

14. I have requested for the return of my 47 hard drives confiscated by the FBI, as well as the videos of my interview with the FBI. The FBI has refused my request.

15. I am fearful that, given the implications of my complaint and a possible investigation, the FBI will destroy the hard drives and video interviews.

16. The FBI itself collaborates with, and continues to collaborate with, the Defendant spy agencies to conduct illegal surveillance.

17. I do not pose any threat to national security, nor do I have any ties to terrorism. I am a former contractor for the NSA, CIA, and the DNI who still has a security clearance. Defendants do not have any probable cause to continue to illegally surveil Plaintiffs my phone and internet activity.

18. Since the December 21, 2015 interview with the FBI, I have been the victim of multiple hacking attempts against my home and business computers from Defendants.

19. Upon tracing the IP addresses of the origination of the hacking attempts, I discovered that numerous attempts also came from the FBI's Criminal Justice Information Systems office in Clarksburg, West Virginia.

20. Upon tracing the IP addresses of the origination of the hacking attempts, I discovered that numerous attempts also came from the Department of Defense's Network Information Center in Columbus, Ohio.

21. Upon tracing the IP addresses of the origination of the hacking attempts, I discovered that numerous attempts also came from the CIA in Washington, DC.

---

[1] John Solomon, Sara Carter, *Declassified Memos Show FBI Illegally Shared Spy Data On Americans With Private Parties*, Circa, May 25, 2017, available at: http://circa.com/politics/declassified-memos-show-fbi-illegally-shared-spy-data-on-americans-with-private-parties.

22. In March 2017, I was also notified that my Apple account was hacked.

23. Upon tracing the IP addresses of the origination of the hacking attempts, I discovered that the attempt came from the CIA in Langley, Virginia.

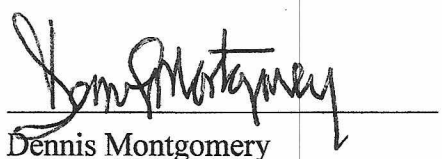
24. Defendants' illegal spying has directly and significantly impacted me and my ability to communicate via telephone, email, and otherwise, given the concerns that confidential, private, and legally privileged communications will be overheard or obtained by Defendant's illegal spying, and use against me and my contacts concerning government abuses and corruption.

25. Defendants' illegal spying has prevented me from being able to speak to my legal counsel, Larry Klayman, which is a breach of my attorney-client privilege.

26. These coercive tactics are designed to compromise me, my family, and my friends' security, silence me and my legal advocacy, and put me in fear of the government and its unconstitutional surveillance that I am trying to stop.

Sworn under penalty of perjury

Dated: June 19, 2017



Dennis Montgomery

EXHIBIT D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et al.*, Plaintiffs, v. JAMES COMEY, et al., Defendants.	Case No: 17-cv-1074

AFFIDAVIT OF LARRY KLAYMAN

1. My name is Larry Klayman, I am over 18 years old. I am an adult citizen of the United States and I am a Plaintiff in the above stated case. I have personal knowledge of the facts stated in this declaration.

2. I am an attorney licensed to practice in Florida and in the District of Columbia. I am also the Founder, Chairman and General Counsel of Freedom Watch, a public interest organization dedicated to preserving civil and individual liberties and freedoms. Such advocacy includes pursuing matters related to national security, government transparency, addressing constitutional violations by the government including issues related to freedom of speech, freedom of religion, voting rights, due process rights, and other protected liberties.

3. I have been a subscriber and user of Verizon Wireless for my cellular phone service for many years and have been a subscriber and user of Verizon Wireless at all material times. I am also a user of internet services by Apple, Microsoft, YouTube, Yahoo, Google, Facebook, AT&T, and Skype and have been a user of these services at all material times. I routinely communicate with members of the public, as well as journalists, clients, and associates by telephonic communications

and electronic messages through Facebook, Google, Apple, and Skype.

4. I have gained public exposure and recognition by bringing numerous high profile lawsuits as a strong public advocate for matters involving public concern and public interest. *See* www.freedomwatchusa.org.

5. As part of my work, and as part of Freedom Watch, I routinely communicate by telephone with existing and potential clients, whistleblowers, and other confidential sources of government abuse and corruption about their legal and other representation and discuss confidential issues, which constitute legally privileged attorney–client and other privileged communications regarding ongoing legal and other proceedings and potential proceedings.

6. I have previously filed several lawsuits against the National Security Agency ("NSA"), seeking to prevent it from pursuing its unconstitutional surveillance of the American people.

7. I have met and communicated with the House Intelligence Committee, the Senate Intelligence Committee, the House Judiciary Committee and the Senate Judiciary Committee, and their members and staffs regarding the illegal and unconstitutional spying and surveillance at issue, and on behalf of my client, Plaintiff Montgomery, and myself, asked these committees and staffs to investigate Defendant Comey and the Federal Bureau of Investigation's ("FBI") cover-up of matters involving Defendants' illegal and unconstitutional surveillance.

7. Because of these actions and my previous lawsuits against the NSA, I have become a prime target for the NSA and FBI.

8. I do not pose any threat to national security, nor do I have any ties to terrorism. I am a former U.S. Department of Justice attorney and an officer of the court. Defendants do not have any probable cause to continue to illegally surveille Plaintiffs my phone and internet activity.

9. Since I began representing Plaintiff Montgomery in his whistleblowing attempts, I have noticed objectively verifiable signals that I have been the subject of ongoing illegal surveillance.

10. I received a purported "software update" on my Samsung Galaxy S7 Edge Verizon cellular phone.

11. After installing the software update, my cellular phone began acting abnormally, including but not limited to the battery draining at an exponential rate as well as numerous other abnormalities.

12. I took my phone into two different Verizon Wireless stores, where technicians confirmed to me that the effects from the purported "software update" were not normal and not the result of either the phone or normal software.

13. I contacted Verizon Wireless and confirmed that they had not initiated the "software update".

14. I have been informed by Plaintiff Montgomery that this is one way Defendants install malware used in spying in the phones of surveilled persons.

15. Plaintiff Montgomery confirmed that battery drainage is a tell-tale sign that the Defendants have successfully hacked into a cellular phone and that Defendants often insert malware onto recipients' phones using fake "software updates".

16. As a result of Defendants' multiple hacking attempts, I was forced to purchase a new Samsung Galaxy S8 phone.

17. As recent as May 2017, my new Verizon Wireless Samsung Galaxy S8 phone began acting abnormally again, including but not limited to the battery draining at an exponential rate, as well as erasing and downloading files on its own and without my consent.

18. I took my phone into another Verizon Wireless store where technicians confirmed that the phone was not acting normally.

19. Defendants' illegal activity at issue in this case poses a substantial threat to my ability as a lawyer, as well as the ability of Freedom Watch to do its work, which includes legal advocacy on controversial issues.

20. Defendants' illegal spying has directly and significantly impacted me and my ability to communicate via telephone, email, and otherwise, given the concerns that confidential, private, and legally privileged communications will be overheard or obtained by Defendants' illegal spying, and used against me, my clients, whistleblowers, and contacts concerning government abuses and corruption.

21. These coercive tactics are designed to compromise me, my family, and my friends' security and relationship with clients, whistleblowers, and other sources of government abuse and corruption, silence me and my legal advocacy, and put me in fear of the government and its unconstitutional surveillance that my client, Plaintiff Montgomery, is trying to stop.

Sworn under penalty of perjury

Dated: June 19, 2017

Larry Klayman