FILED 02 FEB 115 11:52 USDC-ORE

Diane Roark 2000 N. Scenic View Dr. Stayton OR 97383 gardenofeden@wvi.com Telephone: (503) 767-2490

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

PLAINTIFF REPLY TO DEFENDANT'S RESPONSE TO CROSS-MOTION FOR SUMMARY JUDGMENT

UNITED STATES OF AMERICA

Defendant.

Plaintiff Diane Roark, *pro se*, submits the following response to Defendant's arguments against her cross-motion for partial summary judgment.

INTRODUCTION

The government argues that, although there was no criminal evidence against Plaintiff after search of her seized materials and an investigation of more than 5 years, it had a legal right to conduct two separate and distinctive additional searches of Plaintiff's seized written material and has a "continuing interest" in certain paper and electronic documents seized in 2007 that may not be reviewed by the Court.

Plaintiff argues that under the Fourth Amendment requirement for particularity,

Page 1 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

the Government had no right to conduct additional searches using key words other than those employed for the prior investigation without asking the court for two additional search warrants, which it failed to do. The Government also formerly denied that it had seized and retained distinctive paper documents mentioned in the warrant that were prima facie evidence of a prior unnotified, illegal search, but subsequently sent three of those documents to Plaintiff and now admits retaining an unknown number of additional such records.

There is evidence that during this case the Government may have conducted additional electronic searches of Plaintiff and an expert witness. Plaintiff observes that many illegal searches appear to have been conducted against her since 2006, and prays that the Court order discovery to ascertain the facts. This may justify the complete return of Plaintiff's property, as well as expose Government tactics and possibly secret interpretations of law affecting the body politic.

With two key word searches of more than 10,000 emails still to be reviewed, the partial search of Plaintiff's paper and electronic Word documents yielded seven unclassified documents marked "For Official Use Only" (FOUO), a "protected" designation. Plaintiff offered voluntarily to return these, despite her contention that she was allowed to keep them so long as she protected them as she had for five years at that point. Among unmarked electronic documents written by or sent to Plaintiff, NSA alleges to date that two (and copies thereof) are classified at the Secret/SI or TS/SCI level and may not be returned, their presence also justifying destruction of the computer hard drive.

Page 2 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Plaintiff points out that the allegedly TS/SCI document already was twice released by NSA as unclassified, but Defendant has not so acknowledged. Plaintiff argues that the allegedly Secret/SI document is in reality unclassified or at most contains only only a few clauses or sentences that the Government might possibly construe as classified, and that if so determined these could be redacted.

Defendant argues that the Government's burden of proof requires merely transmitting the decision of an Original Classification Authority to the Court. Plaintiff responds that "circumstances," as identified in precedent, call for judicial review in this case, and that in general judicial review is both permissable and essential in order to maintain constitutional checks and balances as well as a free society.

NSA says all unmarked FOUO documents to date are so designated solely because they contain at least one [presumably full first and last] name of a current or former NSA employee. However, NSA does not commit to this practice for remaining unreviewed material, that was sequestered after NSA searched twice with key words other than employee names. NSA continues to claim the right to withhold the entire document or compilation in which such a name or other information alleged to be sensitive appears.

Plaintiff establishes that for many decades NSA claimed vast statutory powers under the NSA Act of 1959 to confiscate unclassified information from its owners or withhold it from the public, but the legislative history proves this interpretation was never intended or permitted. Like other agencies, NSA properly should have been subject since 1966 to provisions of the Freedom of Information Act (FOIA), excepting its extra

Page 3 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

statutory privilege to protect employee information deemed sensitive from public knowledge.

Plaintiff also provides evidence that in protecting employee information, NSA permits its safekeeping at the homes of employees or former employees. Plaintiff argues that the situation has been similar for other "For Official Use Only" information, the designation and handling of which has not been regulated, and that this was certainly the case in 2002 when she retired.

In every case in which it argues it has a right to seize information, NSA improperly claims the right to confiscate entire documents rather than redact sensitive names or other unclassified information. Plaintiff responds that NSA has provided no legal justification for this practice and that it is explicitly forbidden under FOIA.

Plaintiff asks the Court to issue an injunction forbidding improper NSA invocation of the NSA Act for any purpose not justified by the legislative history, including but not limited to powers over unclassified information other than personnel information and the ability to seize entire documents rather than redact sensitive information.

Plaintiff's former employer, the House Permanent Select Committee on Intelligence (HPSCI), claims the right to search Plaintiff's personal papers and confiscate entire documents mentioning any generic topic that might ever have been presented in a paper or discussed in closed executive session, notably anything at all relating to the intelligence budget. HPSCI alleges a right to review NSA's search results and also had NSA conduct a separate search on HPSCI's behalf. It justifies this search and

Page 4 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

withholding of unclassified information on grounds that she signed two pre-publication agreements permitting the Committee to withhold unclassified information from publication.

Plaintiff not only rejects HPSCI's right to search her papers and computer without cause or warrant, but also rejects the legitimacy of the Committee's alleged right to seize her unclassified information, to seize privately held unclassified material not intended for publication, or to restrict the publication of non-FOUO unclassified information.

Plaintiff insists that a later and governing nondisclosure agreement removed the provision regarding unclassified information and asked HPSCI, beginning in 2007, for a copy of it. The Committee has been unresponsive, and Plaintiff prays that the Court require HPSCI to produce it.

In light of apparent illegal searches and decades of misleading various courts about NSA's legal authorities so as to violate the First and Fourth Amendment rights of victims and the public, as well as an undeniable record of misinforming Congress and the public about NSA domestic intelligence activities since the 9/11 attacks, Plaintiff also argues that Defendant comes to this case with "unclean hands."

ARGUMENT

A. The Scope of Plaintiff's Claim

1. Plaintiff no longer seeks the return of six items and a portion of a seventh.

The Government incorrectly states that Plaintiff "acknowledges that this property is executive branch material." This is true only for a Confidential and a Secret document that were not included in this lawsuit and to which Plaintiff *never* claimed a right.

Page 5 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Plaintiff offers more detail on the issue. After 17 years at the Committee, Plaintiff removed about 30 boxes of unclassified from her office upon departure and has not reviewed them since. This large volume was due to the fact that she had no time to review and throw away most of the material before departing, an extremely time-consuming job; she contemplated going through all the papers and keeping selected items because she was considering writing a newspaper column on national security issues.

This idea was abandoned after her experience in August 2006 with NSA's prepublication review process. She had no idea that a Confidential and a Secret document were packed among the unclassified items until the FBI found them, and she does not know whether she herself packed them, as other staff did some of the packing. The two documents are on separate and miscellaneous topics of no continuing interest to Plaintiff.

Plaintiff has vigorously contested, with documentation, HPSCI and NSA claims that there were established rules governing the generating/marking or handling of unclassified "sensitive" information or prohibiting its removal from the office. The Government has failed to document its assertions to the contrary.

Nonetheless, Plaintiff has no interest in the government FOUO documents.

According to dates provided by HPSCI, these concentrated in the late 1997 to 1999 time frame, 3 years before her departure, and doubtless were mixed in among other unclassified papers. It is unfortunate that Plaintiff's willingness voluntarily to return them is misrepresented and falsely portrayed by the Government as an admission of illegality.

Plaintiff also clarifies that this includes all government documents marked FOUO, due to an apparent discrepancy in the count..

Page 6 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

2. Government possession of additional seized property.

The Government alleges that there is "no basis" for this claim that specific emails without headers or footers are missing and not accounted for. "Plaintiff fails to allege facts which would call into question the property inventory," that her belief is "unsupported by any admissable evidence, such as a declaration or affidavit," that they may be among documents the government has not returned, and that there might be copies on Plaintiff's computer.

There are no copies on Plaintiff's computer. These are copies that were printed, and then deleted from her computer to protect Committee investigative sources under constitutional separation of powers. Thus their distinctive removal of headers and footers that might identify sources.

They were in Plaintiff's office and were not discussed with or shown to anyone else for the above reasons. Plaintiff attested to their nature, exact location and her prompt discovery that they were missing very soon after the FBI entered the house. She so stated in sworn documents before the Court, so an affidavit from Plaintiff should be unnecessary.

Further, the FBI in July 2007 itself attested to the documents' existence in a sworn affidavit to secure a warrant to search Plaintiff's home. "Attachment E: Items to be Seized" included as part of item one "classified documents missing headers and footers." This language was replicated in the search warrant. The relevant portion of the affidavit was attached to Plaintiff's cross-motion. As Defendant points out, an affidavit is legally acceptable evidence. However, Defendant still refuses to acknowledge the existence and

Page 7 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

proven content of its own pertinent affidavit.

NSA and FBI appear to have cooperated in attempts to muddy and confuse the issue, but given the clear language of the affidavit, it is hard to see how they envisioned being successful. It appears obvious that the motive is to withhold and cover up prima facie evidence of the truth of Plaintiff's allegation that there was a surreptitious search prior to the overt search, given that otherwise they could not have known about or described these highly distinctive documents.

NSA was party to these evasions because in the affidavit and warrant these are specifically listed as "classified" documents. The FBI is not an original or derivative classification authority (OCA) for NSA material and has little or no expertise in most of NSA's operations or in its classification standards. It is obvious that photos or copies of the documents that were "in plain view" on a shelf (albeit in a stack with only the top document showing) were taken during an unnotified and thus illegal "sneak and peak" search and provided to NSA, which proclaimed them classified before the now unsealed affidavit and the warrant were written. This also raises the question whether there was an affidavit or warrant for the surreptitious search, which was illegal because it was never notified but perhaps also because there was no affidavit or warrant justifying it.

Prior to her cross-motion, Plaintiff had belatedly received only three of these documents, or portions thereof, on October 1 and October 6, 2014. These pieces or shreds of the documents are reproduced at **Attachment 1**, plainly demonstrating their distinctive appearance.

It should be stressed that these three items alone are proof that documents

Page 8 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

meeting Plaintiff's description were seized, contrary to Defendant's denials during prior mediations, and therefore that federal agents almost certainly had previously searched Plaintiff's home. Pressed on this matter within the cross-motion, Defendants finally were forced to so acknowledge in this section of their response that they have an unknown number of additional such documents. They state "it is possible" that the documents are among the emails and faxes that the government has not returned "(HC1, HC5, HC16, HC19,HC20)." Footnote 3 acknowledges that the last two "include emails that have been cut from full-sized pages," while "email excerpts" in HC 17,18 and 38 were returned to Plaintiff – the first time Plaintiff received the numerical designations for 17 and 18.

So in the fine print the FBI finally admits to possession of still more email segments without headers or footers. But it doesn't admit how many. HC19 and HC20 "include" some. Plaintiff recalls a sizable stack of these documents, which took a significant amount of time for her to select, print out and process. There is no count of how many or the total number of these and other documents under those two numbers, nor is it revealed why numerous documents were bunched together under those two numbers.

Importantly, HC 16, 19 and 20 are not even included in the list of documents presented to the Court as still retained by Defendants, and when Plaintiff previously asked about missing numbers she was not told about these numbers and their contents. The FBI used a similar tactic to hide the seizure of these emails without headers or footers within its list of items seized. (also at **Attachment 1**). Some lines list items in

¹ Declaration of Miriam P., September 30, 2014, charts at pp. 5, 7 and 8.

Page 9 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

great detail, but others are in large amorphous groups. Although the emails without headers and footers were separately listed in the sealed affidavit and in the warrant, item 1 lists one dated email, item 4 "emails, articles and calendars," and item 19 "emails, USIC related doc. notebook." Such tactics can be used to hide inconvenient evidence of illegal search and seizure.

This is a good demonstration of why Plaintiff requests that the Court require descriptions of withheld documents that are sufficient to identify the contents and provide the opportunity for individual, reasoned opposition. It is also an example of why there should be judicial review of withholdings. These emails often revealed embarrassing information about NSA, a type of information that E.O. 13526 stipulates is not to be withheld from the public. In further indication of the dysfunction and inconsistency of the NSA classification process, the affidavit and warrant both claimed they emails in question were classified, but NSA now admits that they are not.

3. Basis for relief allegedly unrelated to property claims. The Government's allegations here that there is "no basis" for this relief are mere assertions that are not backed by factual or legal content or any other analysis. Plaintiff, in contrast, has documented in excruciating detail the manner in which NSA misrepresented its powers under the NSA Act for decades and in various venues, including the Interagency Security Classification Appeals Panel. The discussion and evidence in item 2 directly above provides evidence of illegal search and efforts to conceal it. This and other apparent illegal searches, discussed elsewhere, justify Plaintiff's request for discovery.

B. Justification for Return of Remaining Paper Documents

Page 10 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

1a. Government Burden of Proof re OpEd paper. The Government claims it "has demonstrated" that the Op Ed is classified at the Secret/SI level, downgraded from the TS/SCI level "due to the passage of time."

This burden of proof allegedly is met simply by getting an Original Classification Authority (OCA) to stamp it so. The Court and Plaintiff allegedly must accept this unquestioningly because the Executive Branch has the 'sole authority to classify." It is alleged that Plaintiff has shown no "genuine dispute of material fact" about the Government's right to keep this document and represents Plaintiff's objections as ignoring the obvious reality that different publications about the same topic may have different classifications. Plaintiff is said to wrongly question the Government's motives.

In a separate section on the legal history of Judicial Review of classified information, Plaintiff rejects the implication that Courts must or should simply accept the opaque classification decision of an NSA OCA, especially in the instant 41g cases that have exhibited many classification and transparency problems.

Plaintiff suggests that Martin Peck's software would be useful in evaluating publicly available information about this paper to provide useful background for a substantive *in camera* discussion of points NSA deems classified within this paper. If the Maryland case is indicative, the number of papers deemed classified will be few, and this could be the only one.

In the Maryland case of *Wiebe et al. v. NSA et al.*, the Magistrate Judge acknowledged that even in the case precedent on which she relied (and which she interpreted as preventing judicial review), if the government alleged the information to be

Page 11 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

classified, the Court could review "whether the information had previously entered the public domain." That is precisely what this software is meant to do, efficiently and fairly comprehensively. The system does not make claims about classification or level of classification, nor is it intended to substitute for a classification authority. It is merely a robust way to compare a potentially protected document against the entirety of the public knowledge base, insofar as the latter has been compiled and processed in its database and made available for reference. It can benefit the courts as well as both parties to civil or criminal actions.

If specific text nonetheless is found to be classified, that part can be redacted.

NSA has not and cannot demonstrate any authority to withhold entire papers when only a portion is classified. It also admits that prior redactions within the OpEd paper are now excessive, since the classification has been lowered.

Plaintiff discusses these issues in depth in her section on the Freedom of Information Act. With its interpretation of the NSA Act discredited, Defendant has no authority to withhold unclassified information except under the Freedom of Information Act, which has a strong presumption favoring release even when in doubt, plus a requirement for minimal redaction.

NSA has mischaracterized Plaintiff's arguments that the paper is not classified. She has alleged that the major chunks of the paper alleged to be classified are virtually identical to or less specific than those elsewhere that are officially deemed unclassified. It is also obvious from Plaintiff's summary that the overall themes of the paper were

Page 12 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

^{2 (}U.S. v. Marchetti, 466 F.2d 1309, 1317 (4th Cir. 1972, cited in Defendant's Motion for Summary Judgment, Exhibit 2, p. 4).

unclassified; but by the time the censors got done, the themes were scarcely distinguishable.

Plaintiff's only uncertainty about classification involves her inability to remember part of one paragraph, the only paragraph that by any stretch of the imagination could be related to "technical and intelligence information derived from foreign communications signals and data," thus meriting an SI designation. The theme of this paragraph is that the government wasted a lot of money and degraded capability through ill-advised and sometimes expensive actions that undermined performance and achievement of modernization goals [as verified by its current inability to find domestic terrorists despite massive infringement on Fourth Amendment liberties]. This is embarrassing but it is not classified, and it is forbidden to hide embarrassment or waste of money behind classification. This information is also something that the American taxpayer deserves to know.

Plaintiff has presented many problems and inconsistencies with OCA classifications during the criminal case involving Thomas Drake and in the investigation and 41g cases of Plaintiff and her four associates. Mr. William Leonard, former Director of the Information Security Oversight Office responsible for classification policy for the entire Intelligence Community, was so upset by egregious nature of these errors and the failure to hold anyone at NSA accountable that he persuaded the court to unseal one of the five documents involved and engaged in an open dialogue with a successor at ISOO about it. See **Attachment 2.** These are factual issues that NSA did not address or refute and relate directly to whether there should be judicial review.

Page 13 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

- **1b.** Government burden of proof re ThinThread paper. The Government failed to address specific factual allegations about this paper, e.g.:
 - that its alleged classification varied according to the needs and whims of the Government (herein documented in affidavits at Attachment 3);
 - that it was released as Unclassified to J. Kirk Wiebe in the companion
 Maryland Rule 41g) case (previously documented by affidavit), whereas
 here it is designated TS/SCI; and
 - that it is unlawful to reclassify a paper that has been released without many high-level approvals.

Mr. Wiebe has also since informed me that the version released twice was the earlier one, with a subsystem name that Plaintiff had subsequently removed as possibly classified.

Surely NSA maintains records in this regard and can confirm release of the paper.

Alternatively, Plaintiff will provide the Court a copy of the released paper if requested.

By failing to refute such facts, Defendant admits them.

2. The National Security Agency Act of 1959.

The government fails to address or refute dispositive evidence that it has interpreted the NSA Act as providing far more power than specified in Legislative history. It is inconceivable that this was accidental. The General Counsel's Office surely maintained these seminal documents. If the congressional history was lost, it could have been recovered at a law library. One does not decide to assert truly sweeping powers, derived from only one partial sentence in the law, without such due diligence, or continue to do so for decades.

Page 14 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

NSA used this interpretation to win numerous Court decisions, including the related Maryland case of *Wiebe et al. v. NSA et al.*, in which the Magistrate Judge relied on NSA's alleged "*statutory* privilege protecting against the disclosure of NSAA [i.e. the NSA Act of 1959 and unclassified] information relating to its activities" not just personnel information. She concluded that "the Government has established as a *matter of law* that the information it deems to be classified *or NSAA* information...cannot be returned to Petitioners." (emphasis added).³ That is, NSA had as much power over release of unclassified information regarding any NSA "activities" as it had over classified information due to this interpretation.

Defendant's protest that it has released some documents are unavailing and obviously inadequate. It is true that NSA still may redact personnel information according to evolving standards of security, if fairly applied. It is not true that the NSA Act or any other law or regulation permit NSA to withhold entire documents or compilations rather than simply redacting, in current practice, last names except the first initial. This has been an egregious violation of standards, particularly since FOIA was first passed in 1966 and required only minimal redactions, specifically barring this NSA practice. It appears that NSA claimed a unique statutory exception although FOIA was enacted later than NSAA and normally might have superceded it.

If the Court does not accept Plaintiff's argument that FOUO may be kept in a residence under Intelligence Community and NSA practices, the law – not a regulation but a law – requires that all items withheld because only part of them contain classified

³ Id, Defendant's Motion for Summary Judgment, Exhibit 2, pp. 4, 9, emphasis added.

Page 15 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

or restricted information must be minimally redacted and returned to Plaintiff. NSA's assertion that it can find one last name and withhold voluminous material on that basis is facially false and NSA has not even attempted to support it legally. This applies not only to all of Plaintiff's agenda books and telephone logs, which she herself purchased for combined personal and business use, but also all of her other paper and electronic documents.

Defendant merely asserts that NSA does not permit sending or keeping

Unclassified FOUO information at an employee or retiree's residence. It has not
produced any current or past written NSA or Intelligence Community policy to this
effect, and it has not produced any from 2002 when Plaintiff retired. NSA has not refuted
information to the contrary presented by Plaintiff, regarding both NSA and the
Intelligence Community at large. Presidential attempts finally to impose some order and
regularity on the realm of unclassified but protected information are at **Attachment 4**.

Plaintiff demonstrated that FOUO and similar designations have been unregulated, inconsistent and lack formal standards for imposing the designation or handling the information. She specifically documented that this situation persisted for years after her retirement in 2002. Nor has either NSA or HPSCI addressed Plaintiff's assertion that she can be held only to the standards and the pre-publication agreement in existence when she retired.

NSA claims that its active and retired employee policies are identical regarding maintenance of FOUO at home. This makes it even more important for it to address the policies of the Phoenix Society, with which it cooperates, that exists precisely to maintain

Page 16 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

and distribute current lists of retirees' names and locations, arrange social outings and exchange personal updates. Nor has NSA provided formal policy as of 2002 or any other time about distribution of the NSA Newsletter. Facts are more convincing than blanket assertions and documented contrary facts cannot be simply ignored.

Plaintiff continues to insist that her last pre-publication agreement did not cover unclassified information, and HPSCI continues to attempt artfully to misconstrue these plain statements, having since 2007 refused to provide a copy of the agreement. It is possible that HPSCI lost the last agreement that Plaintiff signed. It is not conceivable that it lost the agreements of the entire staff, all of whom were forced to sign it at the same time.

C. Computer Information and Hard Drive.

1. Material fact regarding classified information on the hard drive.

The Government has not addressed material facts presented by the Plaintiff, simply claiming that none were presented, and merely repeats its assertions that the Court must accept the judgment of any OCA despite the poor record of classification probity and consistency in this and related cases. It is a material fact that the ThinThread paper previously was formally released as unclassified, for instance; therefore, no Top Secret/SCI material has been found on the hard drive, thus allegedly requiring its destruction.

2 Government willingness to return unclassified, unprotected information on the computer. Plaintiff appreciates the willingness to do so, so long as "unprotected information" is interpreted to include personnel names only and so long as the

Page 17 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Government convincingly refutes evidence that FOUO information could be taken or sent home and retained or destroyed there, providing it was protected from public disclosure.

This is the original meaning of "protected" material, and it did not include classified.

Past statements tended to mislead the reader into believing that most of Plaintiff's total material had been returned, rather than most of the tiny portion reviewed to date; the grouping of unknown numbers of documents under a single identifying number is misleading even now, and some numbers containing multiple documents are not even listed. Plaintiff deserves a listing and description of every single document still in government possession. In the Maryland case, emails appear to have constituted the great bulk of unclassified material withheld, and there are over 10,000 emails on Plaintiff's computer. Thus judicial decisions could deprive Plaintiff of vastly more records than would appear from current totals that have been minimized through grouping under one number.

CONCLUSION

For the foregoing reasons, Plaintiff is entitled to return of her property in its entirety and to discovery regarding apparently illegal Defendant searches conducted against her by the Government beginning in 2006 and repeating or persisting until at least December 2014. She seeks relief in the manner outlined in the Introduction to her November 26, 2014 submission and an injunction against any further attempt by NSA to exercise illegal authorities under the NSA Act of 1959. Plaintiff respectfully requests that the Court grant her cross-motion for partial summary judgment, with discovery regarding illegal searches, and deny Defendant's motion for summary judgment and dismissal with

Page 18 Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

prejudice.

DATED this 30th day of January 2015.

Respectfully submitted,

Dune Koark

Diane Roark, pro se

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Plaintiff's Reply to Defendant's Response to Cross-Motion for Summary Judgment was emailed to James E. Cox, Jr., on January 30, 2015 to the following email address: jim.cox@usdoj.gov.

It was then sent by United States Mail from Stayton, Oregon to:

James E. Cox, Jr., Esq. AUSA, United States Attorney's Office 1000 SW Third Ave., Suite 600 Portland, Oregon 97204-2902

ATTACHMENTS

Attachment 1 Attachment E of FBI affidavit for a warrant

Returned emails lacking headers and footers,

Attachment 2 William Leonard's communications with ISOO re classification errors

exposed in Drake pre-trial hearings

Attachment 3 Affidavits of Binney, Wiebe and Drake

Attachment 4 Information on "For Official Use Only" designation

Wall Street Journal article Dec. 15, 2009

President's memorandum to department and agency heads

E.O. 13556

Roark v. U.S., Plaintiff Reply, Cross-motion

Attachment E

Items to be Seized

Any items which constitute evidence, instrumentalities, or fruits of violation of Title 18, United States Code, Sections 371 (Conspiracy To Commit An Offense Against The United States), 793 (Unlawful Disclosure of Classified National Defense Information), and 798 (Unlawful Disclosure of Classified Information), including specifically:

- 1. U.S. government documents, classified documents (<u>including classified documents</u> <u>missing headers and footers</u>), national defense intelligence documents and papers, and other documents relating to the National Security Agency (NSA).
- Papers or documents relating to the transmittal of U.S. government documents, national defense and classified intelligence to representatives of the news media, or individuals not authorized to receive the information;
- 3. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as floppy disks, compact disks/CD-roms, hard disk drives, flash drives, tapes, or similar data storage devices/media); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections); and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as "dongles," keycards, physical keys, and locks).
- 4. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
- Computer-related documentation, meaning, any written, recorded, printed, or electronically-stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- Computer passwords and data security devices, meaning any devices, programs, or data – whether themselves in the nature of hardware or software – that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any

Roark v. 2.5., Attachment 1

Diane: FF's Xformation 3.0 (aka TU*) is heavy into J2EE. The major companies supporting it r Essex, Booz, and to a lesser extent, Boing (the omitted e is intentional). However, the funding of the programs is done via task orders and the task orders r typically solid for just 90 days. If there's no useful light at the end of the 90-day tunnel, future \$ r at risk. I'm aware of funded programs being "de-obligated" in order to churn \$ for TU*. If he's interested in living on the edge (as it looks like will be the case during Alexander's tenure), he may want to press some flesh with those companies.

Anybody see or read about the Bush press conference today?

1/27/06

>>> Yes.

He is now saying that the 1978 Foreign Intelligence Surveillance Act is outdated, given the realities of 2006!

>>> Agree, it is outdated! And I tried convincing KP of that fact 7 years ago. FISA is fine for an analog, point-to-point comms world as written. However, it needs to be brot into the 21st century where for the digital, packet-switched world of today. And once it's recaste, then U18 needs to be drastically revised! That thing still refers to office authorities for offices that no longer exist (e.g. DDO) and has no mention of the role played by the NID! Shear lunacy now that u asked.

Huh?

Does that REALLY mean the Executive Branch can ignore what it deems unilaterally is now outdated, even if it is the law, simply because the Executive Branch says so?

>>> No, BUT he is right!

And what about the fact that FISA has been amended SINCE 1978, and most recently as a result of the Patriot Act?!

Like the provision in the Patriot Act that further expands FISA to permit "roving wiretap" authority, thus allowing for the interception of ANY communications made to or by an intelligence target without specifying the particular telephone line, the computer or even the facility to be monitored!

And...

As well...

The Patriot Act removed the pre-existing statutory requirement that the government prove the surveillance target is "an agent of a foreign power" before obtaining a pen register/trap and trace surveillance order under FISA and can now obtain a pen register/trap and trace device "for any investigation to gather foreign intelligence information," without showing that the device has, is or will be used by a foreign agent or by an individual engaged in international terrorism or clandestine intelligence activities!

So...

Seems rather unambiguous to me that Congress and the Courts have clearly NOT unduly restrained (or constrained) the Executive Branch hardly at all now, in pursuit of its legitimate national security authorities and responsibilities, for monitoring the activities of foreign powers and their agents, and now goes even further with the removal of the "foreign power" requirement

Roork v. U.S., Attachment 1

for pen register/trap and trace surveillance!!

What is the problem, then?

>>> It's not written for a digitally-connected world. It's written for an old comms paradigm.

I just don't get it!

However, the Patriot Act DOES include a provision prohibiting the use of a FISA pen register and trace surveillance under ANY circumstances against a United States citizen where the investigation is conducted "solely on the basis of activities protected by the First Amendment."

Is that what is outdated?!

>>> It might be, depending on the legal definition of a "pen register." Since u won't find that in the Constitution, it's up to interpretation.

Seems pretty up to date to me!

Why then the need to bypass FISA???!!!

And...

Any of you hear about the following?

That Representative Rush D. Holt, Democrat from New Jersey, and a member of HPSCI apparently complained over what Holt described as deception by Gen Alexander??!

Apparently, Holt visited FF in early December 2005 for a briefing given by Alexander and FF lawyers about the protection of privacy for Americans.

He was apparently assured that FF singled out Americans for eavesdropping ONLY under warrants from the Foreign Intelligence Surveillance Court!!

Is it possible that FF lied to Holt, or the lawyers at FF were simply quoting the law??!!

>>> Sure it's possible. FF lied to Congress and its staff numerous times when we were working in the SARC. Why wud the wolf change colors when he knew there already had been a tempest brewing with Tice?

So...

Who is advising who, here??!

FISA PERMITS WARRANTLESS WIRETAPPING UNDER CERTAIN CONDITIONS!!!

Besides the 72 hour condition and the 15 day condition when Congress has declared war is the following:

The President may authorize, through the Attorney General, electronic surveillance **WITHOUT** a court order for a period of one year provided it is only for foreign intelligence information targeting foreign powers as defined by 50 U.S.C. §1801(a)(1),(2),(3) or their agents; and there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.

The Attorney General IS required to make a certification of these conditions under seal to the FISA Court and report on their compliance to the HPSCI and SSCI.

What is the problem?!

The compliance issue?!

· .	Case 6:12-cv-01354-MC	Document 100-1	Filed 02/02/15	Page 7 of 26
	>>> The problem is an outdated law, when I pressed him on it for several y the attempt backfired and it got tighter	and KP was the problem pears. His lame excuse was	erson who wudn't pres s that every time an att	s to have it modernized legally
	And yes			the made to loosen it,
	Under FISA, anyone who engages both criminal penalties and civil lial	in electronic surveilland bilities.	e except as authoriz	ed by statute is subject to
to too overl begin	trying to say (and he's been well coached leav's time-sensitive requirements. Well, you haul. HOWSOMESOEVER (as some red (I hope). If he's basing his defense on a sous argument at best and won't hold up us	eah, if you accept the fact th necks say), that is a lame ex an outdated business proces	at the implementation is cuse and he will be rudo s and hasn't make any o	s sophomoric and in need of ely awakened when hearings

Page 2 of 3

What ethics?!

I checked with my sources on this one with respect to the books and got the sardonic "Right" response when I asked.

Said everything to me.

It is a mess.

So Alex is VERY constrained right now in terms of the monies he can move to TU.

And yes...

He thought he could finesse getting around the hoops given his "new" approach to acquisition with SPINs.

Also...

Corporate "taxing" has been a method in the past to pay for higher priority things.

And what about the CBJB?

Largely ignored.

Roark v. U.S., Attachment 1

INFORMATION SECURITY OVERSIGHT OFFICE

NATIONAL ARCHIVES and RECORDS ADMINISTRATION 700 PENNSYLVANIA AVENUE. NW, ROOM 100 WASHINGTON. DC 20408-0001 www.archives.gov/isoo



December 26, 2012

J. William Leonard P.O. Box 2355 Leonardtown, MD 20650 VIA E-MAIL

Dear Mr. Leonard,

I am responding to your letter of July 30, 2011, in which you asked that I, in accordance with my assigned duties under Executive Order 13526, "Classified National Security Information" ("the Order"), consider and take action with regard to what you viewed as a violation of the Order. Specifically, you requested I "ascertain if employees of the United States Government, to include the National Security Agency (NSA) and the Department of Justice (DOJ), have willfully classified or continued the classification of information in violation of the Order" in the matter of *United States v. Thomas A. Drake*. I have concluded my inquiries into this matter, having consulted with the above-mentioned agencies, drawn upon the Order, its implementing Directive, and examined relevant portions of each agency's security regulations, and now share with you my findings and observations.

With regard to your complaint, I conclude that neither employees of the Department of Justice nor of the National Security Agency willfully classified or continued the classification of the "What a Wonderful Success" document in violation of the Order. I wish to note that your complaint suggests this was done "in the matter of *United States v. Thomas A. Drake.*" I think it is important to point out that my process in addressing your complaint examined (and distinguished between) the classification of the document in its first instance and any continuation of its classification "in the matter of *United States v. Thomas A. Drake.*" I find no violation in either case. In fact, as materials you provided with your complaint make clear, NSA discontinued the classification of the document in question and represented the same to the court "in the matter of *United States v. Thomas A. Drake.*"

In examining the "What a Wonderful Success" document, I find that the NSA did not violate the Order's requirements for appropriately applying classification at document creation, nor did the agency violate the Order's expectation that information shall be declassified when it no longer meets the standards for classification. While my examination of the matter has led to my conclusion that the content and processing of the document fall within the standards and authority for classification under the Order and NSA regulations, that does not make them immune to opinions about how substantial the document's content may or may not be. I find, simply, that those opinions do not rise to the level of willful acts in violation of the Order. That said, such commentary on the culture of classification fits well in discussions of policy reform. In such fora, including the work of the Public Interest Declassification Board, your experience and observations would continue to be welcome.

Separate and apart from the specifics of the Drake matter, there are important aspects of the classification system worth noting in this larger discussion of the scope of classification guidance. As you are aware, section 1.1 of the Order grants both responsibility and latitude to Executive branch officials with original classification authority. These officials are the chief subject matter experts in government concerning information that could be damaging to national security if compromised or released in an unauthorized manner.

In light of this, section 2.2 of the Order directs officials with original classification authority to prepare classification guides to facilitate the proper and uniform classification of information. A well-constructed classification guide can foster consistency and accuracy throughout a very large agency, can impart direction concerning the duration of classification, and ensure that information is properly identified and afforded necessary

Roark V. U.S., Altachment 2

protections. Throughout the Executive branch, officials strive to impart proper classification guidance that is accurate, consistent, and easy to adopt in workforces that operates under tight time constraints. It seems quite clear, however, that the system would benefit from greater attention of senior officials in ensuring that their guidance applies classification only to information that clearly meets all classification standards in section 1.1 of the Order. For emphasis, I draw specific attention to language in Section 1.1 (a)(4) "... that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security..." and, 1.1 (b) "If there is significant doubt about the need to classify information, is shall not be classified."

I have a few observations about these matters in the context in which you raised them, namely, the matter of the *United States v Thomas A. Drake*. I have no basis to comment about the disposition of the case in the courts; that is not my purview. The conduct of the case did, however, bring to light actions and behaviors I will comment on briefly, for emphasis. The Order does not grant any individual the authority to safeguard classified information in a manner that is contrary to what the Order, its implementing directive, or an agency's security regulations require. The Order does not grant authorized holders of classified information the authority to make their own decisions concerning the classification status of that information. Furthermore, individuals are provided the means to challenge classification either formally or informally. Section 1.8 of the Order provides all authorized holders of classified information with the authority to issue challenges to classification actions. It explicitly states that individuals are "encouraged and expected" to challenge the classification status of the information through appropriate channels, and every agency is required to implement procedures whereby any authorized holder may issue a challenge without fear of retribution. I know, through the work of this Office, that the National Security Agency is well practiced in the Order's requirements concerning classification status of the information in question.

I note that neither version of the Order in force during the Drake case's time frame [Executive Order 13526 (29 December 2009) and its predecessor Executive Order 12958 (17 April 1995)] provides much in the way of guidance or direction, on its own, to influence the use of classified information in building prosecutions such as this. In general, the Department of Justice defers to the judgment of the "victim" agency as to what constitutes classified information. In building a case, victim agencies, for their part, tend to provide evidence that they deem sufficient to obtain a conviction with the hopes of protecting their most sensitive information and activities from release during court proceedings. The Directive (32 CFR 2001.48) requires only that agency heads "use established procedures to ensure coordination with" the Department of Justice and other counsel. All of this assumes that other influences will be at work to pursue only worthwhile prosecutions, but one interpretation of the Drake case outcome might suggest that this "coordination" was not sufficient. I would welcome your thoughts on whether there is role for policy to provide clearer, more effective guidance in the manner in which such cases are built.

I thank you for your diligent, care-filled observations and comments concerning classification matters. You continue to serve the public well by remaining engaged in the dialogue around the use of secrecy by the government. I can assure you that we take these viewpoints to heart.

Sincerely,

<Signed>

JOHN P. FITZPATRICK Director, Information Security Oversight Office



From: Bill Leonard

Date: December 31, 2012, 4:10:23 PM EST

To: John Fitzpatrick Subject: Re: Complaint

John:

Thanks very much for your <u>reply</u>. While I appreciate the time, effort and consideration you put into this matter, I am nonetheless disappointed in the substance of your reply. Some of my final thoughts on this matter include:

- 1. It took almost one and a half years to respond to a rather straightforward yet serious request. I recognize the need for coordination; nonetheless, irrespective of the nature of the reply, responsiveness is essential for a system to be able to be self-correcting.
- 2. As we discussed when we met in August 2011, I have never taken real issue with the classification of the "What a Success" document in the first instance, which although improper was, by all appearances, a reflexive rather than willful act. Nor did I take issue with its eventual "declassification," which I regarded as NSA simply coming to the proper conclusion, albeit belatedly. What I did and continue to take issue with is that in between those events, senior officials of both the NSA and DoJ made a number of deliberate decisions to use the supposed classified nature of that document as the basis for a criminal investigation of Thomas Drake as well as the basis for a subsequent felony indictment and criminal prosecution. Even after NSA recognized that the document did not meet the standards for continued classification and made the unprecedented decision to declassify an evidentiary document while an Espionage Act criminal prosecution was still pending, senior officials of both the NSA and DoJ still willfully persisted and made yet another deliberate decision to stand by the document's original classification status. I cannot imagine a clearer indication of willfulness on the part of senior government officials to "continue the classification of information in violation" of the governing order through numerous deliberate and collaborative decisions made over the course of years. Based upon my extensive experience, I find the provenance of this document's classification status to be unparalleled in the history of criminal prosecutions under the Espionage Act.
- 3. You ascribe the merits of my complaint as constituting a mere honest difference in opinion. However, this complaint is more than a question of the document failing to pass what I call the "guffaw test" (i.e. common sense). Rather, as I pointed out in my original complaint and yet you did not address, at the heart of this issue are matters of fact. In justifying the deliberate decision to represent during the Drake prosecution that the "What a Success" email was a legitimately classified document, NSA and DoJ officials did not cite some amorphous classification standard or classification guide rather they made factual representations which simply were not true and, in one instance, inherently contradictory (i.e. "information contained therein reveals ... a specific level (emphasis added) of effort ..."

Roark v. U.S., Altachment 2

Case 6:12-cv-01354-MC Document 100-1 Filed 02/02/15 Page 12 of 26 and that the same information "implied a level (emphasis added) of effort ..."). Keep in mind that these determinations were not made on the fly by NSA and DoJ but were in fact deliberate representations made over a period of time and subsequently further qualified but never disavowed. They were intended to demonstrate that the document met the standards of classification that require the original classification authority to identify or describe the damage to national security that could reasonably be expected to result from the unauthorized disclosure. A familiarity with classification standards is not required to determine that these official representations were on their face factually incorrect when compared with a plain text reading of the "What a Success" email. All too often, representatives of the Executive branch believe all they need to do is simply assert classification rather than adhere to the president's own standards, as apparently was the situation in the Drake case. That attitude must change and I will continue to do all I can to help make it foster change.

4. You comment on the fact that the Order does not grant any individual the authority to handle classified information in a manner contrary to the Order and other pertinent regulations. While reference to alleged actions taken or not taken by Mr. Drake are gratuitous and have no bearing on the merits of my complaint, I nonetheless agree with your sentiment. However, allow me to add my own observations, not only as one of your predecessors but also as the only individual who has played an integral role for both defense teams in the only two Espionage Act prosecutions (Drake and AIPAC) not to result in either a conviction or a plea of guilty. In both instances (in which I provided my services pro bono) my decision to get involved was not to defend the actions of the accused but rather to defend the integrity of the classification system, a highly critical national security tool. I have long held that when government agencies fail to adhere to their responsibilities under the governing order and implementing directive, they in turn compromise their ability to hold cleared individuals accountable for their actions. Accountability is crucial to any system of controls and the fact that your determination in this case preserves an unbroken record in which no government official has ever been held accountable for abusing the classification system does not bode well for the prospect of real reform of the system. This phenomenon, the readily apparent inclusion in the Order of a feckless provision which infers that accountability cuts both ways has once again been proven to be a major source of why most informed observers both inside and outside the government recognize that the classification system remains dysfunctional due to rampant and unchecked over-classification. It is disappointing to note that a genuine opportunity to instill an authentic balance to the system has been forfeited in this instance.

As to your request for my recommendations as to the potential for clearer guidance when the classification status of information is integral to a criminal prosecution, I would recommend requiring coordination with an independent body such as the Interagency Security Classification Appeals Panel. In the two cases I referenced above, the fact that the government did not obtain a criminal conviction under the Espionage Act actually bode well for the integrity of the classification system -- otherwise, the perceived wisdom in the reflexive over-classification of information would have been codified in case law.

Finally, I stand ready to share my experiences and observations with the Public Interest

Declassification Board and other fora as seen fit.

Thanks again for the reply, John. While I admire the job you do and the challenges you face, I obviously disagree with the content of your reply. Nonetheless, I am appreciative of the courtesy.

Best wishes for the New Year.

jwl

GENERAL AFFIDAVIT

State	ot	M	агу	and
Coun	ty	of	Cai	roll

Cheryl A. **BEFORE ME**, the undersigned Notary, on this 12th day of January 2015, personally appeared William E. Binney, known to me to be a credible person and of lawful age, who being by me first duly sworn, on his oath, deposes and says: In the matter of a 12 – 14 page document referred to as the THIN THREAD paper, the U.S.-Government, through its agent, the U.S. Department of Justice, and in the person of Assistant U.S. Attorney Thomas H. Barnard, District of Maryland, in a meeting held in July or August of 2012 at the District Court of Maryland, did state it had no interest in other copies of said document in the public domain, which is contrary to U.S. Government policy for the safeguarding and security of media and information the government deems classified. In a related matter, William E. Binney sent a copy of said document to Mr. James Picard of Robbins-Gioia, LLC in 2007. This document was not treated as sensitive information, despite the fact John K. Wiebe notified James Picard of the U.S. Government's claim the paper was sensitive. Mr. Picard notified his security staff at his company, but neither the document nor the hard drive on which he placed it was removed, according to a phone conversation John K. Wiebe had with Mr. Picard some weeks later. Such behavior is contrary to U.S. Government policy for the safeguarding and security of media and information the Government deems sensitive. I can only conclude that the Thin Thread paper was, in fact, not sensitive at all. This would be consistent with the evidence presented in Maryland district court in a 41G law suite against the government for return of property by Kirk Wiebe, William Binney, Edward Loomis and Thomas Drake. I hereby state that the information stated herein is true, to the best of my knowledge. I also state that the information put forth here is both accurate and complete. [signature of William E. Binney] William E. Binney 7800 Elberta Drive Severn, Md 21144 Subscribed and sworn to before me, this [day of month] day of January, 2015.

[Notary Seal:]

[signature of Nøtary]

Typed name of Notary

NOTARY PUBLIC

My commission expires: 10 v 13, 20 K

GENERAL AFFIDAVIT

State of Maryland County of Carroll

BEFORE ME, the undersigned Notary, ANNA MARKET M. PANDA—, on this 12th day of January 2015, personally appeared John K. Wiebe, known to me to be a credible person and of lawful age, who being by me first duly sworn, on his oath, deposes and says:

In the matter of a 12 – 14 page document referred to as "the THIN THREAD paper", the U.S. Government, through its agent, the U.S. Department of Justice, and in the person of Assistant U.S. Attorney Thomas H. Barnard, District of Maryland, in a meeting held in July or August of 2012 at the District Court of Maryland, did state it had no intent to retrieve all available copies of said document, which is contrary to U.S. Government policy for the safeguarding and security of media and information the government deems classified.

In a related matter, a copy of said document sent to Mr. James Picard of Robbins-Gioia, LLC by William E. Binney in 2007 was not treated as classified information, despite the fact I notified Mr. Picard of the U.S. Government's claim the paper was classified. Mr. Picard notified his security staff at his company, but neither the document nor the hard drive on which he placed it was removed from his computer, according to a phone conversation I had with Mr. Picard some weeks later. Such behavior is contrary to U.S. Government policy for the safeguarding and security of media and information the Government deems classified.

In addition, I certify that in the matter of the 26 July 2007 seizure by the FBI and subsequent return of personal information that had been stored on computer hard drives belonging to me, the Government did in fact return to me the very same document referred to as "the THIN THREAD paper" on two separate occasions. The first occasion occurred in 2009 when the FBI returned to me an external hard drive I used as a backup storage disc. The second occurred in 2013 when the FBI returned personal information that had been stored on the hard drives retained by the FBI. Return of the information was carried out subsequent to the ruling of Judge Richard D. Bennett in the case *John Wiebe*, *et al. v. National Security Agency* heard in the Maryland District Court, Baltimore, MD. Return of information the Government has claimed is classified or "sensitive" is contrary to U.S. Government policy for the safeguarding and security of classified and otherwise "sensitive" information. Perhaps more importantly, the return of the paper, including two copies at different times, indicates that the paper was neither classified nor "unclassified-but-sensitive" information.

I hereby state that the information stated herein is true, to the best of my knowledge. I also state that the information put forth here is both accurate and complete.

Roark v. 2.5. Affachment 3 John K. Wiebe

1390 Alison Court

Westminster, MD 21158-2741

Subscribed and sworn to before me, this 12th day of January, 2015.

[Notary Seal:]

[signature of Notary]

[typed name of Notary]

NOTARY PUBLIC

My commission expires: 4NVAM 8, 2018.

Affidavit for Diane Roark

from Thomas Drake

15 Jan 2015

RE: Return of Seized Property by the FBI

State of Maryland, County of Howard

Before the undersigned, an officer	duly commissioned by the laws of Maryland,	วท
this 15 day of January ,	2016, personally appeared	
Thomas A. Preke	who having first duly sworn and says:	

After the conclusion of my criminal case in July 2011, a civil lawsuit was filed by William Binney, J. Kirk Wiebe, Edward Loomis, and myself against the NSA, DoJ and FBI for the return of property seized by the FBI during raids of our residences within the period of July-November 2007.

Upon examination of the returned materials seized by the FBI from my residence in November 2007, I was unable to find any of the documents or related material from the charging or supporting documents in my criminal case, and was unable to find any correspondence related to the THINTHREAD (TT) paper from the period of April-July 2002 and Jan-April 2006 or the Diane Roark op-ed draft from July-October 2006, as all were apparently retained by the government as "protected information" from disclosure.

Prior to my indictment, the government focused on the TT paper for a long time as one of the key documents in their criminal investigation of me, but this same paper was not in the indictment, and instead they fabricated evidence by retroactively classifying 5 unclassified papers that formed the basis of the Espionage Act charges against me.

In summary I had copies of the Diane Roark OpEd (as well as the TT paper) but they were never raised as a classification issue (nor were the documents ever designated as charging or supporting documents, during my criminal case), after I was indicted by the Department of Justice in April 2010. And none of this material was ever provided as part of the criminal proceedings against me during the period of April 2010-July 2011.

Thomas A. Drake

Haron a Donbo

Subscribed and sworn to before me this 15 day of January, 20 15.

Notary Public

My Commission Expires on: Nov. 20, 2018

Roark v. 2.5.

Plan Aims to Ease Agencies' Sharing to Curb Attacks 12-15-09 agencies.

BY CAM SIMPSON AND SIOBHAN GORMAN

WASHINGTON-The Obama administration will announce Tuesday that it plans to make it easier for local, state and federal authorities to share clues that could thwart potential terrorist attacks.

At issue are the reams of reports, guidelines and advisories produced across the govern-4 ment every day that aren't sensitive enough to get classificaflons such as "top secret," but are still too sensitive to make immediately available to the

Right now, government agencies use a tangle of more than 100 categories for this sort of sensitive information. By one count, there are 117. Many of the categories have their own rules for how the information can be shared both inside and among

That red tape can contribute to keeping information from officials who could help connect dots and deter a terrorist attack. officials said.

President Barack Obama has ordered his staff to craft an executive order to consolidate those categories down to one. "Controlled Unclassified Information," according to a White House official involved in the

The executive order will also create a standardized set of rules for handling and sharing such data within all agencies, the official said.

The Obama administration also will announce that it is expanding a program that collects and analyzes potential terrorism tips from local police officers, so that, by 2014, all states will have the capability to analyze that data and share it with other



Attorney General Eric Holder testifies to Congress in November

states and the federal government, a senior homeland security official said.

The effort will take two to four years because it involves training analysts and setting up

technology in 50 states, officials

Mr. Obama in May asked Homeland Security Secretary Janet Napolitano and Attorney General Eric Holder to lead a task force to study barriers to sharing sensitive information that still exist more than eight years after the Sept. 11, 2001, terrorist attacks. The failure of agencies to share information about the Sept. 11 hijackers and the conspiracy was later seen as #The executive order will also a serious problem across the government.

The effort could become more urgent in the face of a spate of cases this year involving home-grown terrorist threats. The report, which has 40 recommendations, is scheduled to be released Tuesday, Key aspects are expected to serve as a basis for Mr. Obama's executive order.

One example of sensitive in-

formation: a Transportation Security Administration manual leaked last week that tells airport screeners across the nation what to look for when travelers pass through their security checkpoints.

Although not classified, the report was considered too sensitive to release publicly because it could give clues to anyone who wants to smuggle something dangerous onto an airliner.

more readily available to the public when it is no longer sensitive. the White House official said. Officials said they would announce Tuesday their intent to protect information "only where there is a compelling requirement to do

The most critical aspect of the new policy will be how the administration defines its new category, Controlled Unclassified Information, said Steven Aftergood, a government-secrecy specialist at the Federation of American Scientists.

Early drafts of the definition, he said, included loopholes that could allow agencies to restrict access to any information they chose just by rewriting agency

Another key issue will be implementation of the policy. One reason so many government documents have been labeled as sensitive is that employees felt their work was too important to share widely, and it isn't clear how the Obama administration's policy will change that, Mr. Aftergood

"I'm not sure that the problem that drove the creation of the 117 categories (of sensitive information] has been solved," he said, "but I admire the attempt."

Well St. Journal

the WHITE HOUSE PRESIDENT BARACK OBAMA

Contact Us ≱

BRIEFING ROOM

ISSUES

THE ADMINISTRATION

PARTICIPATE

1600 PENN

Search

Home · Briefing Room · Presidential Actions · Presidential Memoranda

THE WHITE HOUSE

Office of the Press Secretary

For immediate Release

May 27, 2009

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Classified Information and Controlled Unclassified Information

As outlined in my January 21, 2009, memoranda to the heads of executive departments and agencies on Transparency and Open Government and on the Freedom of Information Act, my Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.

To these ends, I hereby direct the following:

Section 1. Review of Executive Order 12958. (a) Within 90 days of the date of this memorandum, and after consulting with the relevant executive departments and agencies (agencies), the Assistant to the President for National Security Affairs shall review Executive Order 12958, as amended (Classified National Security Information), and submit to me recommendations and proposed revisions to the order.

- (b) The recommendations and proposed revisions shall address:
- (i) Establishment of a <u>National Declassification Center</u> to bring appropriate agency officials together to perform collaborative declassification review under the <u>administration of the Archivist</u> of the United States;
- (ii) Effective measures to address the problem of over classification, including the possible restoration of the presumption against classification, which would preclude classification of information where there is significant doubt about the need for such classification, and the implementation of increased accountability for classification decisions:
- (iii) Changes needed to facilitate greater sharing of classified information among appropriate parties;
- (iv) Appropriate <u>prohibition of reclassification</u> of material that has been declassified and released to the public under proper authority,
- (v) Appropriate classification, safeguarding, accessibility, and declassification of information in the electronic environment, as recommended by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and others; and
- (vi) Any other measures appropriate to provide for <u>greater openness and transparency</u> in the Government's security classification and declassification program while also affording necessary protection to the Government's legitimate interests.
- Sec. 2. Review of Procedures for Controlled Unclassified Information. (a) Background. There has been a recognized need in recent years to enhance national security by establishing an information sharing environment that facilitates the sharing of terrorism-related information among government personnel addressing common problems across agencies and levels of government. The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able rapidly to share sensitive but unclassified information so that those who must act have the information they need.

To this end, efforts have been made to <u>standardize procedures for designating, marking, and handling</u> information that had been known collectively as "Sensitive But Unclassified" (SBU) information. Sensitive But Unclassified refers collectively to the various designations used within the Federal Government for documents



LATEST BLOG POSTS

January 12, 2015 6:01 PM EST

The President Announces New Actions to Protect Americans' Privacy and Identity President Obama stops by the Federal Trade. Commission offices to talk about how we can better protect consumers from identity theft and safeguard everyone's privacy, including our children.

January 12, 2015 5:45 PM EST

Email from Dan Pfeiffer: "Your Memo for the President"

White House Senior Advisor Dan Pfeiffer announces an opportunity for the public to voice their concerns for the 2015's "Citizens Memo." The merno will be constructed from comments sent through the online form listed and will outline goals for the end of the Obama administration.

January 12, 2015 2:08 PM EST
2015 SelectUSA Investment Summit Is
Now Open for Business
At the 2015 SelectUSA Investment Summit,
economic development organizations (EDOs)
from across the United States will once again
gather to showcase investment opportunities to
companies from around the world.

VIEW ALL RELATED BLOG POSTS

Facebook YouTube

Twitter Vimeo

Flickr iTunes

Google+ Linkedin

Roack V. 24-S.

Allachaeart 4

and information that are sufficiently sensitive to warrant some level of protection, but that do not meet the standards for national security classification. Because each agency has implemented its own protections for categorizing and handling SBU, there are more than 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information.

A Presidential <u>Memorandum of December 16, 2005</u>, created a process for establishing a single, standardized, comprehensive designation within the executive branch for most SBU information. A related Presidential <u>Memorandum of May 9, 2008</u> (hereafter the "May 2008 Presidential Memorandum"), adopted the phrase "Controlled Unclassified Information" (CUI) to refer to such information. That memorandum adopted, instituted, and defined CUI as the single designation for information within the scope of the CUI definition, including terrorism-related information previously designated SBU. The memorandum also established a CUI Framework for designating, marking, safeguarding, and disseminating CUI terrorism-related information; designated the National Archives and Records Administration as the Executive Agent responsible for overseeing and managing implementation of the CUI Framework, and created a CUI Council to perform an advisory and coordinating role.

The May 2008 Presidential Memorandum had the salutary effect of establishing a framework for standardizing agency-specific approaches to designating terrorism-related information that is sensitive but not classified. As anticipated, the process of implementing the new CUI Framework is still ongoing and is not expected to be completed until 2013. Moreover, the scope of the May 2008 Presidential Memorandum is limited to terrorism-related information within the information sharing environment. In the absence of a single, comprehensive framework that is fully implemented, the persistence of multiple categories of SBU, together with institutional and perceived technological obstacles to moving toward an information sharing culture, continue to impede collaboration and the otherwise authorized sharing of SBU information among agencies, as well as between the Federal Government and its partners in State, local, and tribal governments and the private sector.

Agencies and other relevant actors should continue their efforts toward implementing the CUI framework. At the same time, new measures should be considered to further and expedite agencies' implementation of appropriate frameworks for standardized treatment of SBU information and information sharing.

(b) Interagency Task Force on CUI.

- (i) The Attorney General and the Secretary of Homeland Security, in consultation with the Secretary of State, the Archivist of the United States, the Director of the Office of Management and Budget, the Director of National Intelligence, the Program Manager, Information Sharing Environment (established in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (6 U.S.C. 485)), and the CUI Council (established in the May 2008 Presidential Memorandum), shall lead an Interagency Task Force on CUI (Task Force). The Task Force shall be composed of senior representatives from a broad range of agencies from both inside and outside the information sharing environment.
- (ii) The objective of the Task Force shall be to review current procedures for categorizing and sharing SBU information in order to determine whether such procedures strike the proper balance among the relevant imperatives. These imperatives include protecting legitimate security, law enforcement, and privacy interests as well as civil liberties, providing clear rules to those who handle SBU information, and ensuring that the handling and dissemination of information is not restricted unless there is a compelling need. The Task Force shall also consider measures to track agencies' progress with implementing the CUI Framework, other measures to enhance implementation of an effective information sharing environment across agencies and levels of government, and whether the scope of the CUI Framework should remain limited to terrorism-related information within the information sharing environment or be expanded to apply to all SBU information.
- (iii) Within 90 days of the date of this memorandum, the Task Force shall submit to me recommendations regarding how the executive branch should proceed with respect to the CUI Framework and the information sharing environment. The recommendations shall recognize and reflect a balancing of the following principles:
- (A) <u>A presumption in favor of openness</u> in accordance with my memoranda of January 21, 2009, on Transparency and Open Government and on the Freedom of Information Act;
- (B) The value of standardizing the procedures for designating, marking, and handling all SBU information; and
- (C) The need to prevent the public disclosure of information where disclosure would compromise privacy or other legitimate interests.
- Sec. 3. General Provisions. (a) The heads of agencies shall assist and provide information to the Task Force, consistent with applicable law, as may be necessary to carry out the functions of their activities under this memorandum. Each agency shall bear its own expense for participating in the Task Force.
- (b) Nothing in this memorandum shall be construed to impair or otherwise affect:
- (i) Authority granted by law or Executive Order to an agency, or the head thereof;
- (ii) Functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.
- (c) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (d) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.
- <u>Sec. 4.</u> <u>Publication</u>. The Attorney General is hereby authorized and directed to publish this memorandum in the Federal Register.

the WHITE HOUSE PRESIDENT BARACK OBAMA

BRIEFING ROOM

THE ADMINISTRATION

PARTICIPATE

1600 PENN

Search

Home · Briefing Room · Presidential Actions · Executive Orders

The White House

Office of the Press Secretary

For Immediate Release

November 04, 2010

Executive Order 13556 -- Controlled Unclassified Information

ISSUES

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

<u>Section 1. Purpose</u>. This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employed hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as <u>Controlled Unclassified Information</u>, that emphasizes the <u>openness and uniformity</u> of Government-wide practice.

Sec. 2. Controlled Unclassified Information (CUI).

- (a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.
- (b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.
- (c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. Review of Current Designations.

- (a) Each agency head shall, within 180 days of the date of this order:
- (1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and
- (2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.
- (b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.



ASY-TO-NAVIGATE PAGE

LATEST BLOG POSTS

Contact Us >

January 12, 2015 6:01 PM EST

The President Announces New Actions to Protect Americans' Privacy and Identity President Obama stops by the Federal Trade Commission offices to talk about how we can better protect consumers from identity theft and safeguard everyone's privacy, including our children

CONTENT IN ONE

January 12, 2015 5:45 PM EST

Email from Dan Pfeiffer: "Your Memo for the President"

White House Senior Advisor Dan Pfeiffer announces an opportunity for the public to voice their concerns for the 2015's "Citizens Memo." The memo will be constructed from comments sent through the online form listed and will outline goals for the end of the Obama administration.

January 12, 2015 2:08 PM EST

2015 SelectUSA Investment Summit Is Now Open for Business
At the 2015 SelectUSA Investment Summit, economic development organizations (EDOs) from across the United States will once again gather to showcase investment opportunities to companies from around the world.

VIEW ALL RELATED BLOG POSTS

Facebook YouTube
Twitter Vimeo
Flickr iTunes
Google+ LinkedIn

Sec. 4. Development of CUI Categories and Policies.

Roark v. 2.5. Affachment 4

- (a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.
- (b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, <u>safeguarding</u> dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency <u>Task Force on Controlled Unclassified Information published in August 2009</u>. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.
- (c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.
- (d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public <u>CUI registry</u> reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.
- (e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.
- (f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. Implementation.

- (a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.
- (b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.
- (c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. General Provisions.

- (a) This order shall be implemented in a manner consistent with:
 - (1) applicable law, including protections of confidentiality and privacy rights;
- (2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government, and
- (3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.
- (b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.
- (c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.
- (d) This order is not intended to, and does not create any right or benefit, substantive or procedural, enforceable

- (a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.
- (b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.
- (c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.
- (d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public <u>CUI registry</u> reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.
- (e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.
- (f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. Implementation.

- (a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.
- (b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.
- (c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. General Provisions.

- (a) This order shall be implemented in a manner consistent with:
 - (1) applicable law, including protections of confidentiality and privacy rights;
- (2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and
- (3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.
- (b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.
- (c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.
- (d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable

at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

- (e) This order shall be implemented subject to the availability of appropriations.
- (f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.
- (g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

BARACK OBAMA

THE WHITE HOUSE, November 4, 2010. Case 6:12-cv-01354-MC Document 100-1 Filed 02/02/15 Page 26 of 26

at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

- (e) This order shall be implemented subject to the availability of appropriations.
- (f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.
- (g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby residned.

BARACK OBAMA

THE WHITE HOUSE, November 4, 2010. Diane Roark 2000 N. Scenic View Dr. Stayton OR 97383 gardenofeden@wvi.com Telephone: (503) 767-2490

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

v.

Case No.: 6:12-CV-01354-MC

Plaintiff,

PLAINTIFF'S RESPONSE TO DEFENDANT'S BRIEF IN SUPPORT OF DEFENDANT'S

MOTION FOR SUMMARY

JUDGMENT

Piailillii

UNITED STATES OF AMERICA

Defendant.

Plaintiff Diane Roark, *pro se*, submits this response in opposition to Defendant's Motion for Summary Judgment.

INTRODUCTION

As there is a great deal of duplication between Defendant's two briefs, one in support of the Government's own motion and one opposing Plaintiff's cross-motion, Plaintiff presents herein a more in-depth look at some of the issues on which Plaintiff and Defendant disagree. Responses to other individual Defendant positions are provided in Plaintiff's other brief regarding their response to Plaintiff's cross-motion.

Page 1 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Judicial Review

In response to Plaintiff's request for judicial review of proposed Government withholdings of unclassified or allegedly classified papers, the Government stated briefly that only the Executive Branch can determine classification. (p. 16).

Under separation of powers within the U.S. Constitution, there is almost nothing that the Executive Branch can do with total independence and impunity, and there is no executive power beyond the law. Like the Judiciary, Congress has its own powers over classification when it chooses to exert them for oversight or other purposes.¹

In the Judicial Branch, Title III courts can review allegedly classified information. Since *Marbury v. Madison*. 5 U.S. 137 in 1803, the general principle of judicial review has been well established.

Courts have devised methods to protect military or foreign policy secrets within the judicial process.² Title III judges are cleared for access to classified information, although their assistants are not. Federal detailees from a Department of Justice team are available to help with classified storage or other security issues should the need arise.

Page 2 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

¹ Because of its oversight responsibilities, Congress can override Administration classification decisions and publicize information that the Executive wants to keep classified. The House Intelligence Committee itself therein also confers clearances on its members and staff (Rule 11(b)(3)(B) so the Executive may not use clearances to infringe on Congressional powers or influence its oversight.

Congress also exerts oversight over the classification system. For example, it has for decades complained about over-classification and about leaks historically originating primarily at a high level in the Executive Branch. Congress funds the Intelligence Community, including its expensive classification infrastructure. It passes laws pertaining to classification, such as the Foreign Intelligence Surveillance Act and the Classified Information Protection Act. It has considered measures under the National Defense Authorization Act to punish Executive Branch leakers. Recently, Congress considered demanding notification of information that is to be or has been "unofficially" declassified by Administration officials, I.e. leaked on "background" but in the past probably never officially acknowledged as declassified.

² Robert Timothy Reagan, Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers, Federal Judicial Center, 2007. A copy is at **Attachment 1**.

Closed hearings, private *in camera* judicial review, issuance of protective orders, sealing of court records containing classified information, redactions or unclassified summaries, assistance from national security experts with clearances, and other ways to protect sensitive information have been developed for both civil and criminal cases.

In this case almost all disputed documents are expected to be deemed Unclassified/For Official Use Only due to inclusion of personnel last names, as the Government itself has stated. Because it is Unclassified, FOUO **does not** require security clearances, merely protection from public dissemination. Confidential and Secret documents may be double-wrapped and mailed and do not require expensive couriers or storage facilities.

Criminal cases are governed by the Classified Information Protection Act (CIPA). In the case of Plaintiff's associate Thomas Drake, the Maryland District Court determined in preliminary closed hearings on CIPA issues that five unmarked documents that NSA swore in court were classified were in fact unclassified. The Government was then forced to drop all ten felony charges entailing a potential 35 years in prison. Plaintiff pointed this out previously and the Government did not deny it.

In civil cases, although security precautions similar to those in a criminal case are available, consideration of classified information has been affected by a 1953 Supreme Court case, *United States v. Reynolds*, 345 U.S. 1 (1953), that developed what is now termed a "State Secrets privilege." The privilege derived from English common law applying to royalty, and had sparse and tangential US history before the decision.

Page 3 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Justices Black, Frankfurter and Jackson dissented "substantially," in agreement with the reasoning of a prior appeals court decision. The Supreme Court has never again considered the issue, although *Reynolds* lacked clear guidelines. There has been no legislative clarification, unlike with the CIPA legislation for criminal cases. The result is a confused and inconsistent civil court legacy.

Some judges are reluctant to require verification that information pertinent to a civil case is properly and wholly classified. They may also skip the process of deciding whether the case is critically dependent upon that information, or whether the case could be tried using measures such as an unclassified description of withheld material.³

District of Columbia District Court Judge Royce Lamberth, who formerly presided over the Foreign Intelligence Surveillance Court, addressed this issue during a May 2013 conference.⁴ He said fellow jurists usually rubber-stamp agency claims that disclosing information would jeopardize national security. "It bothers me that judges, in general, are far too deferential to [FOIA] Exemption 1 claims, he said. "Most judges give almost blind deference on Exemption 1 claims." He wrote that judges are supposed to make a "de novo" determination whether information is "in fact properly classified." However, most check only whether the mechanics of the classification process were followed, not looking at whether the reasons for classification were legitimate, or

³ Justin Florence and Matthew Gerke, "National Security Issues in Civil Litigation: A Blueprint for Reform," *Working Paper of the Series on Counterterrorism and American Statutory Law, a joint project of the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution,* November 17, 2008.

⁴ Josh Gerstein, "Judge: Courts too deferential on classified information," *Politico*, May 13, 2013 (online news site). http://www.politico.com/blogs/under-the-radar/2013/05/judge-courts-too-deferential-on-classified-information-163826.html

Page 4 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

accepting any plausible reason. This is also true of appeals courts, he indicated. However, there are exceptions.

Lamberth said his views were informed by "a couple of really horrible examples" of intelligence agency misconduct that might have been more quickly exposed and addressed if courts held a more "robust" interpretation of FOIA rights.⁵ "The next COINTELPRO [FBI surveillance of dissenters such as Martin Luther King] may not be that far away. The next intelligence scandal may just not be that far away," he warned. Three weeks later, the press began revealing massive domestic surveillance programs, citing NSA documents provided by Edward Snowden.

The State Secrets privilege is an evidentiary rule, as was clearly repeated in the *Reynolds* opinion. However, the *Reynolds* majority decided that it was in that particular case unnecessary to review the classified evidence to verify the grounds for invoking the privilege, stating that "circumstances" should determine how far the court should go in this regard. Some courts have since interpreted the privilege as a justiciability rather than evidentiary rule, 6 dismissing at the outset cases involving significant classified information. Others have cited *Reynolds* respecting the discretionary rather than absolute nature of executive privilege and the judicial need for specific information in order to

Lamberth presided over one State Secrets case that he may have had in mind: Richard A. Horn v. Franklin Huddle, Jr., et al., Civil Action 94-1756-RCL (D.D.C. 2010), h. It is discussed in another Josh Gershwin column, "Judge prods Holder in secrets case," Politico, March 30, 2010, http://www.politico.com/blogs/joshgerstein/0310/Judge prods Holder in secrets case.html. The article notes that Lamberth referenced another D.C. District Court case involving government misconduct in the investigation of anthrax sent to government offices that resulted in a \$6 million payout.

⁶ Florence and Gerke, id.

Page 5 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

evaluate circumstances and balance the interests involved.⁷

Following the 9/11 attacks, the government greatly raised the profile of the State Secrets privilege by repeatedly using it to argue against justiciability, in order to avoid court scrutiny of controversial post-9/11 intelligence activities involving domestic civil liberties and other issues. In civil cases the government is more likely to be the defendant than in criminal cases, and usually has an interest in the outcome. Thus it may be tempted to hide information that is embarrassing or creates liability. Blind judicial deference to executive classifications therefore risks misuse of the classification system, injustice toward civil litigants, failure to uphold the Constitution and erosion of citizens' trust in government.

As noted in Plaintiff's last submission, the D.C. appeals court encouraged a district court to investigate *in* camera NSA's claimed right under the NSA Act to protect specific information that was sought in a FOIA case. Other courts have also upheld the right of a judge presiding over a civil case to review classified information *in camera*.⁸ The Supreme Court ruled in *Reynolds* that the "court itself must determine whether the circumstances are appropriate for the claim of privilege," although its overall discussion

Page 6 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

⁷ Black v. Sheraton Corp. of America, 371 F. Supp. 97 (D.D.C. 1974), 100-101. See also the reviews of government classification claims in Center for International Environmental Law v. Office of the United States Trade Representative, et al. Civil Action No. 01-498 (RWR) (D.D.C., 2012), www.fas.org/sgp/jud/ciel041211.pdf; International Counsel Bureau and Pillsbury, Winthrop, Shwaw, Pittman, LLP v. United States Department of Defense, Civil Action No 08-1063 (JDB), (D.D.C. 2010).

⁸ *The Founding Church of Scientology of Washington, D.C. Inc. v. National Security Agency,* 610 F.2d 824 (D.C. Cir. 1979) pp. 5 and 8. *Weatherhead v. U.S.*, No. 95-519, slip op. At 5-6 (E.D. Wash. Mar. 29, 996) reconsideration granted in pertinent part (E.D. Wash. Sept. 9, 1996) (upholding classification upon in camera inspection), rev'd 157 F. 3d 735 (9th Cir. 1998) vacated and case remanded for dismissal, 528 U.S. 1042 (1999).

⁹ United States v. Reynolds, 345 U. S. 1 (1953) at 7-8.

shed little light on the proper standards for such deliberations, other than the need to maintain security for classified documents. Ultimately, when the facts emerged some 40 years later, history proved that the *Reynolds* majority erred in its confidence that the circumstances in that case did not require judicial review of the classified material.

Declassification revealed that the Supreme Court had been misled. The birth of the State Secrets privilege was triggered by sworn Air Force affidavits at the height of the Cold War. The affidavits used the excuse of a classified mission and electronic equipment to hide, from relatives of civilians who died in a military airplane crash after an engine caught fire, evidence of government culpability due to substandard aircraft maintenance. There was a classified mission and equipment, but they did not cause the fire; information about them could have been redacted from the investigation report that the Air Force refused to turn over to the court or to surviving relatives.

Reynolds is presented herein because Plaintiff seeks judicial review of documents that the Government proposes to retain. The Defendant's response does not directly invoke this privilege. It does briefly state an exclusive Executive Branch right to classify. The Government also comments that the appeals case precedent for judicial review of NSA documents previously cited by Plaintiff, the *Scientology*¹¹ case cited in a prior brief,

¹⁰ The investigation report was quietly declassified and found by a relative of one of the deceased civilians in 2000. Its contents have generated considerable commentary, e.g., Louis Fisher, IN THE NAME OF NATIONAL SECURITY: UNCHECKED PRESIDENTIAL POWER AND THE REYNOLDS CASE, 140-5 (2006); Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1292 n.251 (2007).

¹¹ The Founding Church of Scientology of Washington, D.C. Inc. v. National Security Agency, 610 F.2d 824 (D.C. Cir. 1979) pp. 5 and 8. See also American Civil Liberties Union and American Civil Liberties Union Foundation v. Central Intelligence Agency, Court of Appeals for the D.C. Circuit, No. 11-5320, 2013, (rejects the applicability of a Glomar "judicial construct" for FOIA exemptions (neither confirming nor denying the existence of records that might show the CIA was involved in or interested in drone strikes) as being stretched too far in a manner that no reasonable person would regard as

Page 7 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

involved "extended" interpretation of the NSA Act beyond use of personnel last names; regardless, it serves as an appeals court precedent for judicial review of national security information and State Secrets privilege. However, Defendant does not commit to restricting future seizures of Plaintiff's unclassified property to redaction of employee last names in her documents.

In any case, it appears that judicial review could theoretically be opposed by Defendant for only a small percentage of of the documents at issue. As of now, the Government alleges that only two disputed documents are classified and thus potentially might be claimed as privileged under Reynolds. However, NSA and HPSCI have not yet reviewed the great majority of records considered of potential interest, those that were culled from over 10,000 emails via two separate key word searches. NSA has not revealed how many such documents await further review, and it may be alleged that some are classified. Assuming that virtually all disputed documents in this case will be Unclassified/FOUO, and thus by definition their revelation would not threaten national security, the Reynolds precedent regarding classified information is irrelevant to this larger category, and judicial review of such papers should not be subject to Government dispute. The allegedly classified documents will be minimal, perhaps only two, and will not subject the Court to an undue burden of security or time. However, if the Government is permitted to withhold unclassified items other than last names or to withhold entire documents rather than simply redacting names, Plaintiff will request

plausible (p.14). Citing *Judicial Watch*, *Inc. v. FDA*, 449 F. 3d 146, the Court suggests possible *in camera* review of some or all of the documents if they are deemed too sensitive to list publicly (p. 16). Hereafter cited as *ACLU v. CIA*.

Page 8 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

judicial review of such items as well.

Judicial review has sometimes been avoided in national security cases because judges are not comfortable with their knowledge of the intelligence and national security and especially with the bases for classification decisions. However, the educated layman can spot information that specifically may NOT be classified, such as embarrassing facts, errors, fraud, waste, illegality, etc. Another common-sense criterion that can be applied by those lacking deep expertise is whether the information is widely available in public and thus is improperly classified or over-classified.

E.O. 13526 specifies that information is not automatically declassified merely because it has leaked, but it offers no other guidelines in this respect. Typically, with one-time or limited revelation, the administration may refuse to confirm or deny the leak's accuracy, hoping that adversaries do not see it or may not act upon it, and that the revelation eventually will largely fade into oblivion. When the leak appears authoritative and/or there is widespread or even prolonged publicity, the calculus arguably should change. If it is no longer by any stretch a secret from legitimate adversaries, normally foreign intelligence agencies in particular, it could be argued that normally the information should not remain classified, and if there is persuasive reason for it to remain classified, this should probably be at a lower level than originally.

A long string of administration studies and official statements and policies have verified that the classification system suffers disrepute from widespread over-classification and classification of far too many records. The current administration's

Page 9 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Executive Order on classification and its guidance on FOIA transparency were specifically intended to address over-classification.¹²

Refusing to declassify information that is readily available to an ordinary citizen further undermines the credibility of, respect for and adherence to standards that already are suspect. Classification for political purposes, including to hide potentially illegal domestic activities, greatly aggravates this situation. The Administration and NSA repeatedly have admitted that documents provided to the press by NSA subcontractor Edward Snowden and published worldwide were authentic NSA documents and admitted the existence of some specific programs initially publicized. Yet it is now claiming that all this information remains highly classified and that military and civilian employees may not visit web sites containing it, even as the entire world has been in a furor over the revelations, with often a majority polled in numerous countries being aware of the material. Further, the Administration continues to seek to block court consideration of the programs' constitutional implications. This strengthens the appearance that its main aim has been to keep American citizens and courts in the dark over infringements on liberty and to protect themselves legally, not to deny knowledge to target countries. This example relates directly to the seized papers, because Plaintiff and four associates were in constant email discussion about partial press revelations and their distress over the program. The topic would have been unclear to an ordinary citizen before December 2005 press revelations, and vastly more expansive and detailed discussion has taken place openly since then. In short, these discussions never were classified, and certainly they

12 See information on overclassification and FOIA at Attachment 2.

Page 10 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

are not at this point, nor are they "sensitive."

Martin Peck's database containing published information on NSA affords the Court an opportunity to compare published data against NSA claims that that related emails or papers are classified or sensitive. Its ability to compare various text passages would also help automate retrieval of relevant data and improve quality control among Original Classification Authorities at NSA and elsewhere. There were long delays in the NSA review process during the Maryland case due to an alleged shortage of assigned personnel. Plaintiff has documented vast differences in classification decisions over time and between the Maryland and instant cases. And improper classification decisions are a matter of record in the Drake prosecution¹³ as well as being documented in this case. There was also a 2-year delay in processing the Maryland documents, that ended only because the judge lost patience and imposed a firm deadline. Moreover, President Obama has encouraged development of electronic solutions to improve classification and expedite declassification. However, NSA responded that it does not lack resources and neither needs nor wants to use Mr. Peck's free software and database (p. 16).

This small case nevertheless could be a manageable initial test of the software's

Page 11 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

The Maryland District Court overturned classifications on all five documents used to indict Drake. Four of these remain under seal because NSA alleged they all remained sensitive. Mr. William Leonard, a former director of the Information Security Oversight Office (ISOO) responsible for overall classification policy in the Executive Branch, was so upset by the blatant nature of the misclassifications that he persuaded Judge Bennett to remove a protective order on one document and conducted an open dialogue with one of his successors over the document's content. He also protested the lack of punishment or change, although egregious misclassification with extremely serious consequences had been proven. Two court documents contain Mr. Leonard's request to the Court and the Court's approval. More importantly, two letters from Mr. Leonard to ISOO discuss the attendant policy issues and problems. These are the top four documents listed as of 1/27/15 at http://www.fas.org/sgp/jud/drake/ and copies of the letters are at **Attachment 3**.

utility for court judicial reviews and to help prevent any undue burden on the Court. The Court could enlist the assistance of cleared DOJ security experts available to the courts from the Department of Justice Litigation Security Group (see footnote 7). They could assist cleared IT specialists, perhaps without travel to Oregon, in a software search investigating whether allegedly classified information in one or two documents already has been released by NSA or whether the information is otherwise widely available. For unclassified information, the great bulk of this material, the Court's own local IT expert could probably assist. Mr. Peck could offer these operators technical advice if any problems are encountered. Use of neutral parties would in any case be preferable to NSA assistance.

The database attempts to avoid excessive duplication or repetition of such sources in the interest of efficient storage, retrieval and use of customer time; however, if the Court sought more information on how extensively the information has been republished or otherwise spread, it could follow up with a simple search using a commercial browser.

Finally, Plaintiff prays that the Court consider allowing Plaintiff to participate in judicial *in camera* review of the disputed documents in this case, allowing a meaningful adversarial proceeding. Only a few of these documents are allegedly classified. Plaintiff did consulting work and maintained TS/SCI clearances continuously for about 28 years, the last five doing consulting work, until she was raided. She has been proven innocent of wrongdoing and has been investigated far more extensively than the normal clearance holder. There is ample precedent, in that Maryland associates Thomas Drake and Edward

Page 12 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Loomis have been read back into needed classifications and then read out again as needed, the former on numerous occasions to prepare for his aborted trial and the latter during NSA's pre-publication review of a book he wrote.¹⁴

Descriptions of documents that the Government seeks to withhold

The Government claims that "for the two documents identified to date as classified, the Government has met its burden by providing detailed evidence describing the documents and the classification basis" (p. 2). The government has provided no description whatsoever of what is considered classified within those documents.

NSA did not supply in the Maryland case, evidence sufficient for Plaintiffs to identify the content or often even the title of almost all withheld electronic documents, which usually were identified by a number. The exception was Thomas Drake, who was last in line and who secured an agreement for better identification during a conference call involving the magistrate judge. However, many documents returned to the others were withheld in his case, including, e.g., nearly everything involving ThinThread. This was yet another example of discriminatory and inconsistent classification.

In Plaintiff's case, the two high-profile and allegedly classified documents referenced above were readily identified and the agenda book and telephone logs were obvious, but others often were not. In some cases, Plaintiff's only real insight came from HPSCI descriptions. A very large portion of the total to be reviewed is emails — drawn from over 10,000 messages. Virtually all of those pertaining to NSA were exchanged with one or more other persons, most often a group of four or five. It will be difficult

Page 13 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

¹⁴ See Drake's affidavit at Attachment 4.

under the very best of circumstances for Plaintiff to have any idea of the contents in order to object substantively to allegations that an individual record is sensitive or classified. It is now 7-1/2 years since the documents were seized and as long as 13 years since they were written or received.

The only email currently individually listed as withheld is a printout, document HC1 at page 7 in the Declaration of Miriam P. The information provided is: Email strings "Re: suggestions tonight?," 9 pages. The index lists no date, authors, recipients or summary description of content. It is impossible even to guess what the content is, much less why it might be objectionable. Thus it is impossible to refute the government's retention of the document, although it is unclassified. Records returned in the Maryland case often were identified only by a number.

These are hardly the "detailed" descriptions claimed by Defendant. HPSCI's descriptions of some of the same documents are somewhat more helpful in identifying the record and the Committee's objection to content, but are uneven in quality and hardly are specific about objections to their content.

Given that by far the largest percentage of documents is electronic, it is easy for NSA to generate automatically almost all the information needed, except the need for a content description in the frequent event that the title or "subject" is ambiguous or does not relate to the objection. NSA should provide an unclassified description of content to which it objects. Other information should include document type, length in kilobytes or pages, author, and "from," to," "bcc," and "subject" lines in emails. In short, paper and

Page 14 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

email metadata should be supplied. Since the *New York Times* revelations of December 2005 and the Snowden revelations from June 2013 to the present, we know that NSA has a great deal of experience at autoatically collecting, storing and handling metadata, in massive bulk. NSA has consistently argued that metadata is not an invasion of privacy or too revelatory and that citizens should not be upset about its collection, therefore the Agency can have no objection.

There is court precedent requiring a proper index identifying material for which some form of executive privilege is alleged, *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1982). The requirements and precedents for a *Vaughn* index are discussed in the D.C. Circuit's consideration of ACLU v. CIA, with the Court noting that "in the usual case the index is public and relatively specific in describing the documents the agency is withholding." Particularly since almost all material is unclassified, this should be considered a "usual case."

Illegal Search

In its response, the Government argues that the lawfulness and efficiency of NSA programs are not material (p. 3). This argument presumably applies to Plaintiff's allegations of apparent illegal search. The Government also argues that the Court dismissed charges of illegal search in Plaintiff's constitutional case.

A material fact is anything needed to prove one party's case, or tending to establish a point that is crucial to a person's position. A material issue is a question that is in dispute and that must be answered in order for the conflict to be resolved. Materiality ACLU v. CIA, id., 15-19.

Page 15 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

requires that the facts or issues be logically connected to the case, significant, substantial and sufficiently important to affect case outcome.¹⁶

The Government should explain its logic in claiming that an illegal FBI/NSA search is immaterial to this Rule 41(g) case, given that the Rule itself provides for return of property seized pursuant to such a search. "A person aggrieved by an unlawful search and seizure of property...may move for the property's return....The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant." In this case, that applies to all of Plaintiff's property remaining in Government hands.

As discussed in the introduction to today's companion paper, two Government searches of Plaintiff's property after Drake's criminal trial, looking for items different from those that prompted the investigation and warrant, are illegal. Further warrants were required, but the searches were conducted without them in violation of the particularity clause of the Fourth Amendment.

The Ninth Circuit in 1982 established guidelines for searches of mainly paper documents in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982). As the Court later observed, The point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases. But problems developed

The Free Dictionary by Farlax, http://thelawdictionary.org/material-evidence/; http://www.businessdictionary.com/definition/material-evidence.html.

Page 16 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

when federal agents exploited the "plain view" doctrine when sorting through computers to gather information far beyond the original warrant, then act upon it. This came to a head in *U.S. v. Consolidated Drug Testing* (CDC).

The original *U.S. v. CDC* (579 F.3d 989 (9th Cir. 2009)) case laid down mandatory guidelines meant to ensure that even otherwise lawful warrants authorizing the search and seizure of computer do not give officers too much access to private data that might be intermingled with evidence of a crime. Although the Ninth Circuit still aimed "to avoid turning a limited search for particular information into a general search of office file systems and computer databases," it fell back on Tamura rather than updating it. In a subsequent reconsideration, the original CDC guidelines were eliminated from the majority opinion and included in a 5-judge concurring opinion recommending them as "a useful tool for the future." This removed their mandatory nature when considered by magistrate judges, on whose "good sense and vigilance" the court relied.¹⁷ Those guidelines are:

(1) the government must waive the "plain view" rule, meaning it must agree to only use evidence of the crime or crimes that led to obtaining the warrant, and not to use evidence of other crimes; (2) the government must wall off the forensic experts who search the hard drive from the agents investigating the case; (3) the government must explain the "actual risks of destruction of information" they would face if they weren't allowed to seize entire computers; (4) the government must use a search protocol to designate what information they can give to the investigating agents; and (5) the government must destroy or return non-responsive data. ¹⁸

¹⁷ Musetta Durkee, "Ninth Circuit relaxes electronicsearch procedures in U.S. v. Comprehensive Drug Testing rehearing," Sep. 28, 2010, *berkley technology law journal*, .

¹⁸ Lee Tien, "Revised Opinion in Privacy Case Blurs Clear Limits to Digital Search and Seizure, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2010/09/revised-opinion-privacy-case-blurs-clear-limits.

Page 17 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

A recent circuit decision re-emphasized that the burden of proof is on the government when it fails to return property, and that mere assertion, without evidence, that it was too difficult or costly to separate contraband from his computer files, was insufficient. *U.S. v. Gladding*, 12-10544 (Jan. 2015). In *U.S. v. Cervantes*, (2012 U.S. A the court ruled that except for some very limited exceptions, a search without a warrant is unreasonable and the evidence must be suppressed.

Plaintiff argues that it is clear from these cases that the Court would not approve additional warrantless computer searches exceeding the original warrant's intent, since it strongly advocates segregating any information not applying to the original warrant and has strongly opposed expeditions beyond the original warrant. It also strongly advocates return of property to the owner, especially when presented with assertions rather than detailed evidence. The Government's claim of a continuing interest in unclassified documents is ineffectual given that the Ninth Circuit has ruled that property seized illegally must be returned, in some cases even if it arguably was used or remains usable for illegal purposes.

If electronic or other material is seized and retained in violation of the Farticularity clause in the Fourth Amendment, it must be returned.¹⁹ The Fourth amendment protects citizens from unreasonable seizures as well as unreasonable searches.²⁰ The Government must also return *copies* (emphasis added) of records where

¹⁹ United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1173 (9th Cir. 2010).

²⁰ United States v. Place, 462 U.S. 696, 701 (1983).

Page 18 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

the originals were illegally seized.²¹

The Government's argument that NSA can seize the unclassified, private, unpublished writings, opinions or communications of citizens violates Plaintiff's First Amendment rights²² as well as the reasonableness requirement for Fourth Amendment seizure under Rule 41g). Plaintiff's nondisclosure agreement does not cover unclassified information and does not apply to material that is not made public and is shared only among persons with clearances for classified information. The Government's argument that allegedly sensitive unclassified material constitutes contraband under Rule 41c) was rejected in the Maryland case, *Wiebe et al. v. NSA et al.*, the results of which the Government has embraced.

The Court dismissed Plaintiff's constitutional case without prejudice, meaning that none of the rights or privileges of the individual involved are considered to be lost or waived. This ordinarily indicates the absence of a decision on the merits and leaves the parties free to litigate the matter in a subsequent action, as though the dismissed action had not been started. It is unnecessary for the court to determine whether that action is based on the same cause as the original action and the defendant is prohibited from using the doctrine of Res Judicata in any later action on the subject matter by the same plaintiff. That is, dismissal without prejudice leaves the plaintiff free to bring another suit based on the same grounds.²³

Page 19 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

²¹ United States v. Wallace & Tiernan Co., 336 U.S. 793, 801 (1948); Goodman v. United States, 369 F.2d 166 (9th Cir. 1966); Paton v. LaPrade, 524 F.2d 862, 867–69 (3rd Cir. 1975).

²² See **Attachment 5** for a brief review of case law regarding standing and political speech under the First Amendment, as presented in the constitutional portion of this lawsuit.

²³ The Free Dictionary by Farlax, http://legal-dictionary.thefreedictionary.com/without+prejudice; Nolo's

Plaintiff's argument that apparent illegal searches were within the two-year

Oregon statute of limitations on the basis of a continuing conspiracy against her by the

Government was rejected by the Court in the constitutional portion of this case.

However, as contemplated under dismissal without prejudice, additional evidence may

change the Court's prior judgment. Plaintiff now has evidence of possible continuous or

resumed, as well as new, Government electronic searches related to her case. It appears

that a Government conspiracy by NSA and/or FBI still continues and involves illegal

searches that target Plaintiff.

Overt downloads from Plaintiff's computer did not end until at least November 2011, shortly after Plaintiff and associates filed the Maryland 41g) lawsuit. At this time, tracking of Thomas Drake also ended (it had continued although sentencing for a misdemeanor had occurred about four months earlier). While the more overt monitoring techniques were not observed thereafter, Plaintiff was well aware that software caching most non-junk deleted emails remained on her computer. For this and other reasons, she suspected it was possible that the Government had transitioned from semi-overt and coercive pressure and harrassment to covert monitoring, in continued violation of her Fourth Amendment rights.

On November 26, 2014, the day before Thanksgiving weekend, Plaintiff submitted her first response to the Government's motion for summary judgment. On December 1, the following Monday, at 3 a.m. additional software code was improperly

Page 20 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Plain-English Law Dictionary, http://www.nolo.com/dictionary/dismissal-without-prejudice-term.html.

"pushed" without permission onto a telephone owned by Martin Peck, an expert witness who had offered free software to help determine whether a document is properly classified. The number of this telephone had been submitted to the Court along with his testimony on November 26.²⁴

Plaintiff's computer was working in the early morning of December 1, but when she attempted to log on early that afternoon, the screen froze and the computer could not be operated. Plaintiff took the computer to a local repair shop. With electronic scanning, a Trojan Horse was found on the computer and removed, along with other adware and malware. The shop was quite surprised, saying that insertion of a Trojan Horse is extremely rare. An employee informed me that this was a full-scale Trojan, not, e.g. a lesser "root kit" type of capability. Therefore, he said it could probably notify the Trojan operator every time I logged on, extract any information it wanted from my computer, take pictures of the screen, and likely included a keylogger to capture information such as passwords. Because it was found through the scan, it was a previously discovered and known threat.

At the shop, the computer appeared to be repaired. But it immediately froze on two more occasions, and could not be relied upon to meet legal deadlines, so Plaintiff replaced it.

Page 21 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

²⁴ Oddly, Peck's submission of testimony at the courthouse in Portland had not been entered into the Court record for **some** days. Eventually he drove to Eugene to re-submit it, and it appeared on Pacer by the time he got back to his car.

²⁵ For diagnoses and receipts, see **Attachment 6**.

For more information on Trojan Horse types and capabilities, see the Internet Security Center at Kaspersky Lab, http://usa.kaspersky.com/internet-security-center/threats/trojans.

Snowden documents and other analyses demonstrate that NSA has used known attack software, either to disguise the identity of the attacker (a common tactic), because NSA and its allies use it so extensively that it becomes known, or because NSA computer attacks have been discovered and used by others such as malicious commercial or other state hackers.²⁷

These incidents provide more evidence of a "continuing conspiracy," including intrusive searches, that should permit extension of a two-year statute of limitations to the present day and also justify discovery.

Plaintiff is proposing herein not a Bivens or tort claim but a civil action in equity to recover the *entirety* of her property that was seized pursuant to illegal search, while simultaneously finding and exposing the truth about Government breaking and entering activities and lengthy electronic searches. The Government has misinterpreted her statement in objecting that the property return is not an objective. It is.

A Rule 41g) case is a civil action in equity.²⁸ The statute of limitations for a 41g)

²⁷ See, e.g., a *Der Spiegel* article featuring analysis of source code that was provided by Edward Snowden. It confirms previous suspicions that the notorious Trojan Horse dubbed "Regin" was probably developed at least partially by NSA's U.K. partner, GCHQ, and also is used by NSA, where it was named Qwerty. "The new analysis provides clear proof that Regin is in fact the cyber-attack platform belonging to the Five Eyes alliance..." Marcel Rosenbach, Hilmar Schmundt and Christian Stocker, "Source Code Similarities: Experts Unmask 'Regin' Trojan as NSA Tool," http://m.spiegel.de/international/world/a-1015255.html#spRedirectedFrom=www&referrrer=. In this case, it appears that the Five-Eyes English-speaking countries used Regin so frequently that it became known within the Information Technology community, with some developing an ability to spot it and perhaps even protect against it.

²⁸ United States v. Machado, 465 F.3d 1301, 1307 (11th Cir. 2006), overruled on other grounds, as recognized in United States v. Lopez, 562 F.3d 1309, 1311-13 (11th Cir. 2009). Other claims under section 2401a) are considered in: Young v. United States, 907 F.2d 156 (9th Cir. 1990) para. 10, (claims that NASA used his invention without paying him are barred by, inter alia, the 6-year statute of limitations); Sisseton-Wahpeton Sioux Tribe v. United States, 895 F.2d 588, 592 (9th Cir.1990) (quoting 28 U.S.C. Sec. 2401(a) to uphold the District

Page 22 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

lawsuit commenced after completion of trial and/or investigation is six years after the right of action first accrues, under 28 U.S.C. section 2401(a): "[E]very civil action commenced against the United States shall be barred unless the complaint is filed within six years after the right of action first accrues." (Baxter v. U.S., Court of Appeals for the Eleventh Circuit, No. 11-12216, 2012, pp. 3-4). Six years is the general statute of limitations for non-tort actions against the federal government, with tort actions subject instead to limitations in the companion 28 U.S.C. section 2401(b).

As Plaintiff's case wore on and she was not indicted, retention of property being held by the government could be justified by the related pending trial of Thomas Drake. Trial preparations were halted in June 2011 and followed by sentencing for a misdemeanor plea in July 2011. When the Government did not reply to her four associates' repeated requests for return of their seized property, Plaintiff joined a Maryland 41g) lawsuit in November 2011, from which she later was removed, then in July 2012 filed a 41g) lawsuit in Oregon, where her property was seized. Thus Plaintiff filed timely, at most one year after Drake's case ended and nine months after it became clear that the Government had no intention of returning the property, thus provoking the Maryland lawsuit -- well within the six-year limitation.

If the Rule 41g) case is filed timely, Plaintiff assumes it covers all the search and

Court finding that Sioux tribes may not sue the U.S. in 1987 to challenge a law passed in 1972); United States v. Mottaz.476 U.S.8324(1986) (Ruling that suit against the US re title to Indian lands is barred not by the general 6-year statute of limitations but by a 12-year limitations period under the Quiet Title Act of 1972).

²⁹ Baxter v. U.S., Court of Appeals for the Eleventh Circuit, No. 11-12216, 2012, pp. 3-4.

Page 23 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

seizure issues that occurred during the investigation and throughout long legal proceedings, so the issue of tolling over the prolonged period that may be involved would not normally arise as it would in a tort claim.³⁰

Plaintiff submits that there is clearly enough information about a pattern of apparent illegal searches, that form a continuing conspiracy since 2006, to justify discovery. Discovery should also be justified under the Rule 41g) statute of limitations.

CONCLUSION

For the foregoing and other reasons, Plaintiff opposes the Government's motion for summary judgment. She respectfully requests that the Court grant her cross-motion for summary judgment and discovery regarding illegal searches.

DATED this 30th day of January 2015.

Respectfully submitted,

Diane Hoark

30Alternatively, the permitted six-year statute of limitations for a non-tort action against the Government is a span that covers almost all the relevant history of her complaints against the Defendant, were the limitation counted backward from the date of filing rather than forward from the conclusion of Drake's case.

Therefore, it would seem that a 6-year statute of limitations also would apply from the date of those individual government activities to the time of filing, unless this would require two separate actions. The initial telephone and electronic searches probably began in 2006, an unnotified sneak and peak search occurred in July 2007, and subsequent or continuing electronic/phone searches occurred to the present time. A sixyear statute of limitations from the time of the these suspect activities forward until filing should cover searches back to July 2006 and possibly even to November 2005, six years before the first attempt to recover property in a Maryland lawsuit.

Page 24 Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment, Roark v. U.S., 6:12-CV-01354-MC.

Diane Roark, pro se

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Plaintiff's Response to Defendant's Brief in Support of Defendant's Motion for Summary Judgment was emailed to James E. Cox, Jr. on January 30, 2015 to the following email address: jim.cox@usdoj.gov.

It was then sent by United States Mail from Stayton, Oregon to:

James E. Cox, Jr., Esq. 1000 SW Third Ave., Suite 600 Portland OR 97204-2902

ATTACHMENTS

Attachment 1 Keeping Government Secrets: A Pocket Guide for Judges...

Attachment 2 Overclassification and the Freedom of Information Act

FOIA slides, Department of Defense

Text of amended FOIA

Attachment 3 William Leonard correspondence with ISOO re classification errors

Attachment 4 Drake affidavit re temporary clearances

Attachment 5 First Amendment case law overview

Attachment 6 Computer repair receipts

Roark V. U.S., Plainfiff Response, Summary, Judgment

Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers

Robert Timothy Reagan

Federal Judicial Center 2007

This Federal Judicial Center publication was undertaken in furtherance of the Center's statutory mission to develop and conduct education programs for the judicial branch. The views expressed are those of the author and not necessarily those of the Federal Judicial Center.

Roark v. U.S., Mountiff Response, Summerer Judgment

Contents

Preface v

Introduction 1

- I. Classified Information 1
- II. The State-Secrets Privilege 3
 - A. Invocation of the Privilege 4
 - B. Secrecy Validity 5
 - C. Disposition of the Case 6
 - D. Covert Espionage Agreements 7
- III. The Classified Information Procedures Act 8
- IV. Bringing Classified Information to the Court's Attention 8
 - A. Classified Information Held by the Government 9
 - B. Classified Information Held by a Defendant 9
- V. Protective Procedures 10
 - A. CIPA Hearing 10
 - B. Protective Orders 11
 - C. Classification Designations 12
 - D. Withholding Discovery 12
 - E. Ex Parte Presentation 13
 - F. Limited Presentation at Trial 14
 - G. Declassification 15
 - H. Jury Instructions 16
 - I. Dismissal 16
- Vl. Flexibility 16
- VII. Interlocutory Appeal 17
- VIII. Court Security Officers 17
- IX. Sensitive Compartmented Information Facilities 19
- X. Conclusion 19

Appendix A: Classified Information Procedures Act 21

Appendix B: Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information 31

Preface

Most federal judges come into contact with classified information infrequently, if at all, but when they do, they are faced with the dilemma of how to protect government secrets in the context of an otherwise public proceeding.

This pocket guide is designed to familiarize federal judges with statutes and procedures established to help public courts protect government secrets when courts are called upon to do so. The guide provides information about the Classified Information Procedures Act (CIPA), information security officers, and secure storage facilities.

I hope you will find this guide useful in meeting the challenge of protecting government secrets in a public forum.

Barbara Jacobs Rothstein Director, Federal Judicial Center

Introduction

As courts adjudicate cases involving classified information, they must protect government secrets. The Classified Information Procedures Act (CIPA) provides procedures for protecting classified information in criminal prosecutions. Similar procedures are used in civil cases. The courts are assisted in their protection of government secrets by court security officers provided by a small office in the Department of Justice's Management Division called the Litigation Security Group.

According to an executive order of President Clinton, "Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security."

I. Classified Information

Classified information is information designated by the executive branch as not subject to public discussion.

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.²

The Classified Information Procedures Act defines "classified information" as

information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of

^{1.} Exec. Order No. 12.968, 60 Fed. Reg. 40,245 (Aug. 7, 1995).

^{2.} *Id*.

section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).³

Other laws define classified information similarly.⁴ The act, in turn, defines "national security" as "the national defense and foreign relations of the United States."⁵ Other laws define national security similarly.⁶

There are three levels of classification: (1) confidential. (2) secret, and (3) top secret. Information is classified by an "original classification authority," who is "an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance." Confidential information is "information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."8 Secret information is "information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."9 Top secret information is "information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe."10

- 3. 18 U.S.C. app. 3 § 1(a) (2000).
- 4. Exec. Order No. 13,292 § 6.1(h), 68 Fed. Reg. 15,315 (Mar. 28, 2003) ("Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."); Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 7, 1995) ("Classified information" means information that has been determined pursuant to Executive Order No. 12958 [superseded by Executive Order No. 13292], or any successor order, Executive Order No. 12951 [concerning Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems], or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.").
 - 5. 18 U.S.C. app. 3 § 1(b) (2000).
- 6. Exec. Order No. 13,292 \S 6.1(y), 68 Fed. Reg. 15,315 (Mar. 28, 2003) ("the national defense or foreign relations of the United States").
 - 7. Id. § 6.1(cc).
 - 8. Id. § 1.2(a)(3).
 - 9. Id. § 1.2(a)(2) (emphasis added).
 - $10. \, \mathit{Id}. \, \S \, 1.2(a)(1)$ (emphasis added).

Generally, access to classified information requires a security clearance.¹¹ Article III judges are automatically entitled to access to classified information necessary to resolve issues before them, but their law clerks must obtain security clearances to have access to classified information.¹²

Compartmentation can provide an additional layer of security. "Sensitive compartmented information" is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." Usually sensitive compartmented information is top secret information, access to which is restricted to a limited set of individuals on a need-to-know basis specific to the information.

Courts do not have authority to overrule classification determinations.¹⁴

II. The State-Secrets Privilege

The government has a common-law right to keep state secrets secret. The modern articulation of the privilege is a 1952 Supreme Court case.

Three civilian observers were among those killed when a B-29 bomber crashed on October 6, 1948, during a flight to test secret electronic equipment.¹⁵ The observers' widows sued the government and sought to discover the Air Force's official accident investigation report and investigative statements of the three surviving crew members.¹⁶ The Supreme Court determined, in *United States*

^{11.} E.g., United States v. Bin Laden, 58 F. Supp. 2d 113, 118 (S.D.N.Y. 1999).

^{12.} Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information ¶ 4, 18 U.S.C. app. 3 § 9 note, issued Feb. 12, 1981 [hereinafter Courts' Security Procedures]; United States v. Smith, 899 F.2d 564 (6th Cir. 1990) (holding that executive branch investigations of court staff for security clearances do not violate the constitutional separation of powers).

^{13. 28} C.F.R. § 17.18(a) (2007).

^{14.} United States v. Fernandez, 913 F.2d 148, 154 (4th Cir. 1990); United States v. Musa, 833 F. Supp. 752, 755 (E.D. Mo. 1993).

^{15.} United States v. Reynolds, 345 U.S. 1, 2-3 (1952).

^{16.} Id. at 3.

v. Reynolds, that the evidence was subject to a privilege against revealing military secrets. 17

The district court had ordered production and awarded the plaintiffs damages as a sanction for the government's failure to produce the evidence and refusal to allow ex parte in camera inspection by the court. ¹⁸ The Secretary of the Air Force filed a formal claim of privilege in response to the production order, and the Air Force's judge advocate general filed an affidavit declaring that production of the evidence would seriously hamper national security. ¹⁹ The government offered as a substitute production of the surviving crew members for examination as witnesses. ²⁰ The Supreme Court, which did not examine the classified evidence, determined that the proposed substitute was adequate. ²¹

The privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party. It is not to be lightly invoked. There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer. The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.²²

A. Invocation of the Privilege

There are three steps to invocation of the state-secrets privilege.²³ First, the privilege must be (1) invoked by the United States government²⁴ (2) by formal claim made by the head of the department

```
17. Id. at 6.
```

^{18.} Id. at 4-5.

^{19.} Id.

^{20.} Id. at 5.

^{21.} Id. at 11.

^{22.} Id. at 7-8 (footnotes omitted).

^{23.} El-Masri v. United States, 479 F.3d 296, 304 (4th Cir. 2007).

^{24.} *El-Masri*, 479 F.3d at 304; Bareford v. Gen. Dynamics Corp., 973 F.2d 1138, 1141 (5th Cir. 1992); Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 546 (2d Cir. 1991); Fitzgerald v. Penthouse Int'l Ltd., 776 F.2d 1236, 1239 n.4 (4th Cir. 1985); Ellsberg v. Mitchell, 709 F.2d 51, 56 (D.C. Cir. 1983).

controlling the secret²⁵ (3) after personal review of the matter.²⁶ Second, the court must determine that the secret information is legitimately secret, in which case it is absolutely protected.²⁷ Third, the court must determine how protection of the secret affects the case.²⁸

B. Secrecy Validity

The court does not determine what information should be secret, but it does have the responsibility to determine what information legitimately has the status of a state secret.

Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers. Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case. It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.²³

The court's review of classified evidence or arguments is not necessary if the public record sufficiently establishes the need to

25. El-Masri, 479 F.3d at 304; Sterling v. Tenet, 416 F.3d 338, 345 (4th Cir. 2005); McDonnell Douglas Corp. v. United States, 323 F.3d 1006, 1022 (Fed. Cir. 2003); Kasza v. Browner, 133 F.3d 1159, 1169 (9th Cir. 1998); Bareford, 973 F.2d at 1141; Zuckerbraun, 935 F.2d at 546; Halkin v. Helms, 690 F.2d 977, 991 (D.C. Cir. 1982); Fitzgerald, 776 F.2d at 1242; Halpern v. United States, 258 F.2d 36, 38 (2d Cir. 1958).

26. El-Masri, 479 E.3d at 304; Sterling, 416 E.3d at 345; Kasza, 133 E.3d at 1169; Bareford, 973 E.2d at 1141–42; Zuckerbraun, 935 E.2d at 546; Halkin, 690 E.2d at 991; Halpern, 258 E.2d at 38.

27. El-Masri, 479 F.3d at 304–06; Sterling, 416 F.3d at 343; McDonnell Douglas Corp., 323 F.3d at 1021; Kasza, 133 F.3d at 1166; Black v. United States, 62 F.3d 1115, 1119 (8th Cir. 1995); Zuckerbraun, 935 F.2d at 546–47; Fitzgerald, 776 F.2d at 1243; Halkin, 690 F.2d at 990, 992–94.

28. El-Masri, 479 F.3d at 304, 306–13; Kasza, 133 F.3d at 1166; Bareford, 973 F.2d at 1141–44; Halkin, 690 F.2d at 990, 997–99; Fitzgerald. 776 F.2d at 1243; Halpern. 258 F.2d at 43–44.

29. United States v. Reynolds, 345 U.S. 1, 10 (1952).

keep the evidence secret.³⁰ Whether or not the court reviews classified evidence or arguments also depends upon a balancing of how necessary the evidence is to a party's case and how imperative it is that the evidence remain secret.³¹

C. Disposition of the Case

A case may be dismissed if it cannot be litigated without compromising state secrets.³² If a plaintiff is denied access to state secrets that are essential to the plaintiff's claim, then the claim may be dismissed.³³ If a defendant is denied access to, or prevented from entering into evidence, state secrets that are essential to a defense, then also the claim may be dismissed.³⁴ But unavailability of material evidence does not necessarily result in dismissal; sometimes the case is simply litigated without the unavailable evidence.²⁵

If both the plaintiff and the defendant have access to statesecrets evidence, the court may be able to use various protective procedures to litigate the case without exposing state secrets to

- 30. Sterling, 416 F.3d at 343-45; Halkin, 690 at 992-94.
- 31. Sterling, 416 F.3d at 343; Ellsberg v. Mitchell, 709 F.2d 51, 58–59 (D.C. Cir. 1983).
- 32. Sterling, 416 F.3d at 345–48; McDonnell Douglas Corp., 323 F.3d at 1021; Kasza, 133 F.3d at 166; Fitzgerald, 776 F.2d at 1243.
- 33. McDonnell Douglas Corp., 323 F.3d at 1024; Monarch Assurance P.L.C. v. United States, 244 F.3d 1356, 1361 (Fed. Cir. 2001); Kasza, 133 F.3d at 166; Black v. United States, 62 F.3d 1115, 1119 (8th Cir. 1995); Bareford, 973 F.2d at 1142; Zuckerbraun, 935 F.2d at 547–48
- 34. *In re* Sealed Case, 494 F.3d 139, 149 (D.C. Cir. 2007); *Sterling*, 416 F.3d at 344; Tenenbaum v. Simonini, 372 F.3d 776, 777 (6th Cir. 2004); *Kasza*, 133 F.3d at 166; Molerio v. FBI, 749 F.2d 815, 825 (D.C. Cir. 1984).
- 35. In re Sealed Case, 494 F.3d at 148 ("even after evidence relating to covert operatives, organizational structure and functions, and intelligence-gathering sources, methods, and capabilities is stricken from the proceedings under the state secrets privilege, [the plaintiff] has alleged sufficient facts to survive a motion to dismiss"); Kasza, 133 F.3d at 166; In re United States, 872 F.2d 472, 480 (D.C. Cir. 1989) ("We share the district court's confidence that it can police the litigation so as not to compromise national security."); Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268, 270–71 (4th Cir. 1980) ("When the government is not a party and successfully resists disclosure sought by a party, the result is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence.") (quoting McCormick's Handbook of the Law of Evidence § 109, at 233 (1972)).

the public.³⁶ The case may also proceed if evidence is available that suitably substitutes for state-secrets evidence.³⁷

D. Covert Espionage Agreements

Courts may not hear suits premised on covert espionage agreements.³⁸

It may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated. On this principle, suits cannot be maintained which would require a disclosure of the confidences of the confessional, or those between husband and wife, or of communications by a client to his counsel for professional advice, or of a patient to his physician for a similar purpose. Much greater reason exists for the application of the principle to cases of contract for secret services with the government, as the existence of a contract of that kind is itself a fact not to be disclosed.³⁹

The Supreme Court determined in *Totten v. United States* that the survivor of an alleged Civil War spy could not recover from the government unpaid compensation for the spying.⁴⁰ Chief Justice William Rehnquist determined for the Court in *Tenet v. Doe* that *Totten's* absolute bar is not just an example of the state-secrets privilege.⁴¹

^{36.} Loral Corp. v. McDonnell Douglas Corp., 558 F.2d 1130, 1132 (2d Cir. 1977) ("[A] large amount of material properly classified confidential and secret must be submitted to the trier of fact in the case. We are persuaded that this circumstance is enough to make it inappropriate for jury trial."); Halpern v. United States, 258 F.2d 36, 43 (2d Cir. 1958) ("Under the circumstances of this case, we are not convinced that a trial *in camera* is either undesirable or unfeasible.").

^{37.} United States v. Reynolds, 345 U.S. 1, 11 (1952) ("Here, necessity was greatly minimized by an available alternative, which might have given respondents the evidence to make out their case without forcing a showdown on the claim of privilege.").

^{38.} Tenet v. Doe, 544 U.S. 1 (2005).

^{39.} Totten v. United States, 92 U.S. 105, 107 (1876).

^{40.} Totten, 92 U.S. 105.

^{41.} Tenet, 544 U.S. at 10.

III. The Classified Information Procedures Act

The Classified Information Procedures Act (CIPA) was enacted on October 15, 1980, and it is codified as the third appendix to Title 18 of the U.S. Code, the title concerning crimes and criminal procedures.⁴²

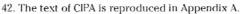
CIPA, by its terms, covers only criminal cases; in civil cases, courts and the government follow procedures similar to those provided by CIPA.⁴³

If either the government or the defendant believes that classified information will come into play in a criminal case, then that party must bring the matter to the court's attention, and the court must establish and implement procedures to keep classified information secret.⁴⁴

IV. Bringing Classified Information to the Court's Attention

The court should receive prompt notice if classified information will be at play in a prosecution, and the court should promptly establish procedures to protect the information:

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Follow-





44. United States v. Mejia, 448 F.3d 436, 455 (D.C. Cir. 2006) ("CIPA is a procedural statute that does not itself create a privilege against discovery of classified information."); United States v. O'Hara, 301 F.3d 563, 568 (7th Cir. 2002) ("CIPA's fundamental purpose [is] protecting and restricting the discovery of classified information in a way that does not impair the defendant's right to a fair trial."); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("Congress intended CIPA to clarify the court's power to restrict discovery of classified information."); United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir. 1989) ("CIPA was enacted by Congress in an effort to combat the growing problem of greymail, a practice whereby a criminal defendant threatens to reveal classified information during the course of his trial in the hope of forcing the government to drop the criminal charge against him.").

ing such motion, or on its own motion, the court shall promptly hold a pretrial conference....⁴⁵

A. Classified Information Held by the Government

The government may bring concerns about classified information to the court's attention ex parte: "The court may permit the United States to make a request for [authorization to withhold classified information from the defendant] in the form of a written statement to be inspected by the court alone."46

If the court is to implement procedures to protect classified information, the government should provide the defendant with notice that classified information is at issue.⁴⁷

Before any [CIPA hearing], the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.*





A court of appeals held that it was improper for a government agency to initiate secret proceedings, without the knowledge of either the defense or the prosecution, to determine whether certain classified information had to be disclosed to the defendant.⁴⁹

B. Classified Information Held by a Defendant

If a criminal defendant contemplates use of classified information, the defendant must notify both the court and the government of its intentions.

^{45. 18} U.S.C. app. 3 § 2 (2000).

^{46.} Id. § 4.

^{47.} United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363 (11th Cir. 1994).

^{48. 18} U.S.C. app. 3 § 6(a)(1) (2000).

^{49.} Mejia, 448 F.3d at 453–54 (concerning a district court finding in a drug-crime prosecution that classified evidence presented ex parte and in camera by the Drug Intelligence Unit of the Justice Department's Narcotic and Dangerous Drug Section would not be helpful to the defense).

If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information.⁵⁰

A court of appeals held that "a brief description of the classified information," as prescribed in the text of the statute, is sufficient, overruling a trial court holding that the defendant's notice must include justifications of relevance.⁵¹ But the notice must contain sufficient detail so that the government can determine how presentation of the evidence might damage national security.⁵²

Evidence preclusion is the statutory remedy for failure to comply with the notice requirement.⁵³ When a defendant identified virtually every classified document that the government had produced in discovery as reasonably expected to be used at trial, the court determined that the vastly overinclusive notice was in bad faith, and so the court required the defendant to identify for use at trial approximately the same number of classified documents as the government had identified its intent to use.⁵⁴

V. Protective Procedures

A. CIPA Hearing

Protective procedures generally are established through a CIPA hearing. Both parties are present, but the hearing may be conduct-

^{50. 18} U.S.C. app. 3 § 5(a) (2000).

^{51.} United States v. Miller, 874 F.2d 1255, 1276 (9th Cir. 1989).

^{52.} United States v. Collins, 720 F.2d 1195, 1200 (11th Cir. 1983).

^{53. 18} U.S.C. app. 3 § 5(b) (2000); United States v. Badia, 827 F.2d 1458, 1464–66 (11th Cir. 1987).

^{54.} United States v. North, 708 F. Supp. 389 (D.D.C. 1988).

ed in camera if the government certifies that an in camera hearing is necessary to protect classified information.

Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information.⁵⁵

The record of a hearing concerning classified information should be preserved for use in an appeal, but should be sealed to prevent unauthorized disclosure of the classified information.

If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.⁵⁶

B. Protective Orders

A key tool in protecting classified information is the protective order. "Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States." ⁵⁷

^{55. 18} U.S.C. app. 3 § 6(a) (2000); see also id. § 6(c)(1) ("The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.").

^{56.} Id. § 6(d).

^{57.} Id. § 3.

C. Classification Designations

In the prosecution of Admiral John Poindexter for obstruction of Congress in the Iran-Contra scandal, the government produced in discovery hundreds of thousands of pages of documents, many of which were classified. 58 But the practices of the agencies who supplied the documents did not always result in the documents' being marked to reflect their level of classification or precisely what parts of the documents were classified.⁵⁹ On the one hand, a full classification review of all of the documents would have been too burdensome for the government; but on the other hand, the defendant needed to know the classification status of documents he wanted to use for trial.⁶⁰ The parties negotiated a procedure, which was approved by the court, in which the defendant would identify documents he wanted to share with witnesses or use for trial, and an interagency group of government security officers would perform a full classification review on those documents, but the group would not disclose to the attorneys representing the government which documents were reviewed.61

D. Withholding Discovery

Classified information may be withheld from the defendant. The act provides for three ways of withholding discovery: (1) deletion, (2) summarization, and (3) admission.

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information, from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. 62

In a prosecution for conspiracy to bomb the Los Angeles International Airport in December 1999, the court reviewed classified intelligence information potentially discoverable by the defendant

^{58.} United States v. Poindexter, 727 F. Supp. 1470, 1472, 1486 (D.D.C. 1989).

^{59.} Id. at 1486 & n.33.

^{60.} Id. at 1486.

^{61.} Id.

^{62. 18} U.S.C. app. 3 § 4 (2000).

and, after determining what was discoverable, authorized the government to provide the defendant with unclassified summaries.63

The government must, however, provide the defendant with such information as is relevant and helpful to the defense.64

E. Ex Parte Presentation

To resolve discovery issues and pretrial motions, the government can present to the court in exparte proceedings classified evidence to which neither the defendant nor defense counsel has access. 65

During the discovery phase of an obstruction-of-justice prosecution of Vice President Dick Cheney's chief of staff, the court permitted the government to submit ex parte potentially discoverable classified material for the court's review so long as the government explained why the material was classified and why defense counsel with security clearances could not see it.66 The court also allowed defense counsel to submit ex parte to the court their defense needs so that the court could better evaluate whether the government's classified submissions were discoverable.67

In a prosecution for helping to fund Hamas, the defendant sought to suppress confession statements that he claimed were obtained with torture by Israeli secret police officers. 68 The governments of the United States and Israel waived the classification designation regarding all evidence presented at the suppression hearing, except for a small amount of evidence that concerned the credibility of the Israeli witnesses but not the defendant's treatment or guilt.69 The court heard this evidence in camera and ex

^{63.} United States v. Ressam, 221 F. Supp. 2d 1252, 1256 (W.D. Wash. 2002).

^{64.} United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("In order to determine whether the government must disclose classified information, the court must determine whether the information is 'relevant and helpful to the defense of an accused.""); United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998) ("[1]f some portion or aspect of a document is classified, a defendant is entitled to receive it only if it may be helpful to his defense. A court applying this rule should, of course, err on the side of protecting the interests of the defendant.")

^{65.} Klimavicius-Viloria, 144 F.3d at 1261; United States v. Pringle, 751 F.2d 419, 427 (1st Cir. 1984).

^{66.} United States v. Libby, 429 F. Supp. 2d 18, 25, 27 (D.D.C. 2006).

^{67.} Id. at 26-27; see also United States v. North, 708 F. Supp. 389, 391 (D.D.C. 1988) (noting that the court obtained ex parte information about the intended defense before ordering extensive discovery on the government).

^{68.} United States v. Marzook, 435 F. Supp. 2d 708 (N.D. III. 2006).

^{69.} ld. at 745-47.

parte.⁷⁰ Because the defense did not have access to this evidence, the court drew "adverse inferences" against the government, which the court explained were like a thumb on the scale in favor of the defendant—not drawing any inferences from the evidence in the government's favor.⁷¹

F. Limited Presentation at Trial

The court may authorize the presentation of classified information at trial by summary or authorize admissions that would render the presentation of classified information unnecessary. But the defendant must retain "substantially the same ability to make his defense as would disclosure of the specific classified information."

If the evidence would be admissible at trial, the burden shifts to the government to offer in lieu of the classified evidence either a statement admitting relevant facts that the classified information would tend to prove or a summary of the specific classified information. . . .



... [But] the district court may not take into account the fact that evidence is classified when determining its use, relevance, or admissibility.⁷⁴

Some courts have held that normal evidentiary principles govern the admissibility of classified evidence. To For example, a district court ruled that classified evidence was admissible as part of a hijacking defendant's argument that the hijacking was a CIA operation. Other courts require a balancing of the public interest in protecting secrets against the right to a defense.

Classified information may be presented to a jury without requiring security clearances for the jurors, but jurors may be cautioned not to disclose the classified information to others.⁷⁸

```
70. Id. at 746.
```

^{71.} Id. at 750.

^{72. 18} U.S.C. app. 3 § 6(c)(1) (2000).

^{73.} Id.

^{74.} United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363–64 (11th Cir. 1994) (quotation marks omitted).

^{75.} United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir. 1989); United States v. Wilson, 750 F.2d 7, 9 (2d Cir. 1984).

^{76.} United States v. Lopez-Lima, 738 F. Supp. 1404 (S.D. Fla. 1990).

^{77.} United States v. Smith, 780 F.2d 1102, 1105 (4th Cir. 1985).

^{78.} Courts' Security Procedures, supra note 12, ¶ 6.

When a defendant sought to prove that his confession was obtained with torture by Israeli secret police officers, the court permitted the government to make several admissions to obviate presentation of classified evidence. For example, the government admitted that Israeli secret police officers were authorized to use hoods, handcuffs, and shackles during interrogations. The defendant was able to question the police officers at trial about their treatment of him and pursue extensive cross examination except in the limited areas that would elicit classified information.

Courts will sometimes permit narrowly tailored procedures that present classified evidence to the judge, the parties, and the jury, but not to the public.⁸²

However, in a trial for conspiracy to communicate national defense information to unauthorized persons, the government sought to use a "silent witness" procedure extensively.⁸³ Using this procedure, the court, the witness, the parties, and the jury would have access to classified documents, but the public would not. Testimony concerning classified information would be in code, such as by referring to persons as X, Y, and Z, and by referring to countries as A, B, and C. The trial judge ruled that extensive use of this procedure would impair the defendant's statutory right to make his defense and his constitutional right to a public trial.⁸⁴

G. Declassification

Once the court determines what classified evidence must be admitted to ensure the defendant a fair trial, the government may decide to declassify the information.⁸⁵

^{79.} United States v. Salah, 462 F. Supp. 2d 915, 917-18, 925 (N.D. III. 2006).

^{80.} Id. at 917.

^{81.} Id. at 923, 925.

^{82.} E.g., United States v. Pelton, 696 F. Supp. 156 (D. Md. 1986) (allowing the playing of audio tapes containing "secret" information through headphones).

^{83.} United States v. Rosen, 487 F. Supp. 2d 703, 705–09 (E.D. Va. 2007); see also United States v. Zettl, 835 F.2d 1059, 1063 (4th Cir. 1987) (describing the silent witness rule).

^{84.} Rosen, 487 F. Supp. 2d at 714, 720.

^{85.} United States v. O'Hara, 301 E.3d 563, 568 (7th Cir. 2002).

H. Jury Instructions

It may be helpful to instruct the jury on why trial proceedings appear to be skirting relevant information. One judge developed the following instruction:

This case involves certain classified information. Classified information is information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure. In lieu of disclosing specific classified information, I anticipate that you will hear certain substitutions for the classified information during this trial. These substitutions are admissions of relevant facts by the United States for purposes of this trial. The witnesses in this case as well as attorneys are prohibited from disclosing classified information and, in the case of the attorneys, are prohibited from asking questions to any witness which if answered would disclose classified information. Defendants may not cross examine a particular witness regarding the underlying classified matters set forth in these admissions. You must decide what weight, if any, to give to these admissions.86

I. Dismissal

If the government's secrets cannot be protected adequately while affording the defendant a fair trial, then ordinarily the indictment is dismissed.⁸⁷

VI. Flexibility

At the conclusion of the trial of Colonel Oliver North for his involvement in the Iran–Contra scandal, Judge Gerhard Gesell observed that the court and the attorneys served the purposes of CIPA, although they did not always conform to CIPA precisely.

CIPA was ill-suited to a case of this type and amendments are needed to recognize practical difficulties. For some instances, the Court followed procedures which

^{86.} United States v. Salah, 462 F. Supp. 2d 915, 924 (N.D. III. 2006).

^{87.} United States v. Moussaoui, 382 E3d 453, 466 n.18, 474-76 (4th Cir. 2004).

were not in strict accord with the statutory framework to expedite resolution of unusual problems that arose. Fortunately, CIPA is a procedural statute, and the legislative history of it shows that Congress expected trial judges to fashion creative solutions in the interests of justice for classified information problems. The Executive cooperated with the Court by liberally waiving classification objections when to do otherwise might have halted the proceeding and interfered with a fair trial.⁸⁸

VII. Interlocutory Appeal

The government has a statutory right to an expedited interlocutory appeal of an order "authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information."89

VIII. Court Security Officers

The Department of Justice employs security specialists whose job it is to assist the courts in protecting the secrecy of classified information.

There are ten security specialists employed by the Department of Justice's Security and Emergency Planning Staff (SEPS). They, plus an associate director of SEPS and a secretary, constitute the Litigation Security Group, which is approximately one eighth of SEPS's personnel. The director of SEPS reports to the deputy assistant attorney general for Human Resources and Administration, a unit of the Department of Justice's Management Division, which is headed by an assistant attorney general. This assistant attorney general is designated by regulation as the Justice Department's manager of information classification and access to classified information.⁹⁰

The security specialists are not lawyers, and they are organizationally quite separate from the government's representatives in

^{88.} United States v. North, 713 F. Supp. 1452, 1452–53 (D.D.C. 1989).

^{89. 18} U.S.C. app. 3 § 7(a) (2000).

^{90.} Id. § 17.11(a).

court. Their obligation is to help the court protect classified information, not to assist the government's representatives in court. ⁹¹ In fact, they often provide assistance to parties opposing the government.

Formally, in criminal cases, when the court needs assistance in protecting classified information, the director of SEPS submits to the presiding judge a nomination letter recommending a security specialist as the court's security officer. This nomination letter complies with procedures established by Chief Justice Warren Burger on February 12, 1981, 32 as required by the act:

Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of Central Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.⁹³

Chief Justice Burger's procedures provide that the court security officer *shall* be selected from among the persons listed in the nomination letter.⁹⁴ The director of SEPS customarily recommends one security specialist as the court security officer for the case and recommends all others as alternates (including the SEPS associate director for the Litigation Security Group but excluding a security specialist whose job is largely administrative).

^{91.} United States v. Yunis, 867 F.2d 617, 621 n.8 (D.C. Cir. 1989); United States v. Musa, 833 F. Supp. 752, 756 (E.D. Mo. 1993).

^{92.} Courts' Security Procedures, supra note 12. The procedures are reproduced in Appendix B.

^{93. 18} U.S.C. app. 3 § 9(a) (2000) (as enacted Oct. 15, 1980). The phrase "Director of Central Intelligence" was changed to "Director of National Intelligence" when the latter position was created in 2004. P.L. 108-458 (Dec. 17, 2004), 118 Stat. 3691.

^{94.} Courts' Security Procedures, supra note 12, \P 2.

IX. Sensitive Compartmented Information Facilities

The court security officer will assist the court in determining how to physically secure classified documents. Sometimes a safe in the judge's chambers is enough. Sometimes classified documents must be stored in a "Sensitive Compartmented Information Facility," or SCIF.

A SCIF (which usually is pronounced like "skiff") is a secure room—or building—that meets certain construction and access requirements. Courthouses where cases implicating classified information arise frequently—such as the Southern District of New York and the Eastern District of Virginia—have one or more SCIFs. Safes and locked file cabinets may be stored in a SCIF, and different judges may have access to different parts of a SCIF.

When a SCIF is required for a court to hear a case, the government will either construct a SCIF for the court or arrange for the court to have access to an existing SCIF.⁹⁵ It is even possible to "SCIF" a judge's bathroom.

Attorneys—and their clients if they have sufficient security clearances—may be required to review classified information within a SCIF. Sometimes secure computers are provided for attorneys' exclusive use within the SCIF.

X. Conclusion

The executive branch decides what information is classified as state secrets, and the judicial branch decides how to protect the rights of parties in civil and criminal cases while keeping government secrets. The Classified Information Procedures Act and court security officers help the courts meet their obligations to the parties and the government.

^{95. &}quot;Expenses of the United States Government which arise in connection with the implementation of these procedures shall be borne by the Department of Justice or other appropriate Executive Branch agency." *Id.* ¶ 12.

FOIA Exemption 1 & E.O. 13526 Classified National Security Information

Defense Freedom of Information Policy Office (703) 696-4689 DFOIPO@whs.mil

www.dod.mil/pubs/dfoipo/docs/EO_13526.ppt

Roank v. U.S., Placetof Kesponse, Summary Judgment

Background

- May 27, 2009 Presidential Memorandum, "Classified Information and Controlled Unclassified Information"
 - Directed a review of E.O. 12958, to include proposals concerning:
 - i. Establishment of a National Declassification Center;
 - ii. Effective measures to address the problem of over classification and increase accountability for classification decisions;
 - iii. Facilitate greater sharing of classified information;
 - iv. Prohibition of reclassification of material that has been declassified and released to the public under proper authority;
 - v. Consideration of the electronic environment; and
 - vi. Greater openness and transparency while also affording necessary protection to the Government's legitimate interests.

E.O. 13526 – Tier I (Information less than 25 years old)

- Under Section 1.4 of the Order, information shall not be considered for original classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security, and it pertains to one or more of the following:
 - a) Military plans, weapons, or operations;
 - b) Foreign government information;
 - ✓ c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
 - d) Foreign relations or foreign activities of the U.S., including confidential sources;
 - e) Scientific, technological, or economic matters relating to the national security;

E.O. 13526 – Tier I (Continued)

- f) U.S. Government programs for safeguarding nuclear materials or facilities;
- g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security; or
- The development, production or use of weapons of mass destruction.

FOIA UPDATE: THE FREEDOM OF INFORMATION ACT, 5 U.S.C. SECT. 552, AS AMENDED BY PUBLIC LAW NO. 104-231, 110 STAT. 3048

January 1, 1996

FOIA Update Vol. XVII, No. 4 1996

THE FREEDOM OF INFORMATION ACT 5 U.S.C. § 552, AS AMENDED BY PUBLIC LAW NO. 104-231, 110 STAT. 3048

Below is the full text of the Freedom of Information Act in a form showing all amendments to the statute made by the "Electronic Freedom of Information Act Amendments of 1996." All newly enacted provisions are in boldface type.

- § 552. Public information; agency rules, opinions, orders, records, and proceedings
- (a) Each agency shall make available to the public information as follows:
- (1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public--
 - (A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;
 - (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;
 - (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;
 - (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and
 - (E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

- (2) Each agency, in accordance with published rules, shall make available for public inspection and copying--
 - (A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

Roark v. U.S., Plaintiff Response, Summary Sudgment

- (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; and
- (C) administrative staff manuals and instructions to staff that affect a member of the public;
- (D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and
- (E) a general index of the records referred to under subparagraph (D);

unless the materials are promptly published and copies offered for sale. For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction, staff manual. instruction, or copies of records referred to in subparagraph (D). However, in each case the justification for the deletion shall be explained fully in writing, and the extent of such deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of an index on request at a cost not to exceed the direct cost of duplication. Each agency shall make the index referred to in subparagraph (E) available by computer telecommunications by December 31, 1999. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if-

- (i) it has been indexed and either made available or published as provided by this paragraph; or
- (ii) the party has actual and timely notice of the terms thereof.
- (3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon request for records which (A) (i) reasonably describes such records and (B) (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.
 - (B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.
 - (C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

- (D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.
- (4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.
 - (ii) Such agency regulations shall provide that--
 - (I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use:
 - (II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and
 - (III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.
 - (iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.
 - (iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section--
 - (I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or
 - (II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.
 - (v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed \$250.
 - (vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

- (vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo, provided that the court's review of the matter shall be limited to the record before the agency.
- (B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).
- (C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.
- [(D) Except as to cases the court considers of greater importance, proceedings before the district court, as authorized by this subsection, and appeals therefrom, take precedence on the docket over all cases and shall be assigned for hearing and trial or for argument at the earliest practicable date and expedited in every way. Repealed by Pub. L. 98-620, Title IV, 402(2), Nov. 8, 1984, 98 Stat. 3335, 3357.]
- (E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.
- (F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.
- (G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.
- (5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.
- (6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--

Case 6:12-cv-01354-MC Document 101-1 Filed 02/02/15 Page 32 of 55

- (i) determine within ten days twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and
- (ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.
- (B) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days. As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular request—
 - (i) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;
 - (ii) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or
 - (iii) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.
- (B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days, except as provided in clause (ii) of this subparagraph.
 - (ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C).
 - (iii) As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular requests--
 - (I) the need to search for and collect the requested records from field

facilities or other establishments that are separate from the office processing the request;

- (II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or
- (III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.
- (iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.
- (C)(i) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.
 - (ii) For purposes of this subparagraph, the term "exceptional circumstances" does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.
 - (iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing the request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.
- (D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.
 - (ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.
 - (iii) This subparagraph shall not be considered to affect the requirement under

subparagraph (C) to exercise due diligence.

- (E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records--
 - (i) in cases in which the person requesting the records demonstrates a compelling need; and
 - (II) in other cases determined by the agency.
 - (ii) Notwithstanding clause (i), regulations under this subparagraph must ensure--
 - (I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and
 - (II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.
 - (iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.
 - (iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.
 - (v) For purposes of this subparagraph, the term "compelling need" means--
 - (I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or
 - (II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.
 - (vi) A demonstration of a compelling need by a person making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person's knowledge and belief.
- (F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.
- (b) This section does not apply to matters that are--
- (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

- (2) related solely to the internal personnel rules and practices of an agency;
- (3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made.

- (c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and--
 - (A) the investigation or proceeding involves a possible violation of criminal law; and
 - (B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.
- (2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

- (3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.
- (d) This section does not authorize the withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.
- (e) On or before March 1 of each calendar year, each agency shall submit a report covering the preceding calendar year to the Speaker of the House of Representatives and President of the Senate for referral to the appropriate committees of the Congress. The report shall include--
- (1) the number of determinations made by such agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;
- (2) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information;
- (3) the names and titles or positions of each person responsible for the denial of records requested under this section, and the number of instances of participation for each;
- (4) the results of each proceeding conducted pursuant to subsection (a)(4)(F), including a report of the disciplinary action taken against the officer or employee who was primarily responsible for improperly withholding records or an explanation of why disciplinary action was not taken;
- (5) a copy of every rule made by such agency regarding this section;
- (6) a copy of the fee schedule and the total amount of fees collected by the agency for making records available under this section; and
- (7) such other information as indicates efforts to administer fully this section.

The Attorney General shall submit an annual report on or before March 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subsections (a)(4)(E), (F), and (G). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

- (e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States a report which shall cover the preceding fiscal year and which shall include—
 - (A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;
 - (B)(i) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and
 - (ii) a complete list of all statutes that the agency relies upon to authorize the agency to withhold information under subsection (b)(3), a description of

whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;

- (C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median number of days that such requests had been pending before the agency as of that date;
- (D) the number of requests for records received by the agency and the number of requests which the agency processed;
- (E) the median number of days taken by the agency to process different types of requests;
- (F) the total amount of fees collected by the agency for processing requests; and
- (G) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests.
- (2) Each agency shall make each such report available to the public including by computer telecommunications, or if computer telecommunications means have not been established by the agency, by other electronic means.
- (3) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Government Reform and Oversight of the House of Representatives and the Chairman and ranking minority member of the Committees on Governmental Affairs and the Judiciary of the Senate, no later than April 1 of the year in which each such report is issued, that such reports are available by electronic means.
- (4) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.
- (5) The Attorney General of the United States shall submit an annual report on or before April 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.
- (f) For purposes of this section, the term "agency" as defined in section 551(1) of this title includes any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.
- (f) For purposes of this section, the term--
 - (1) "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

- (2) "record" and any other term used in this section in reference to information includes any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.
- (g) The head of each agency shall prepare and make publicly available upon request, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including--
- (1) an index of all major information systems of the agency;
- (2) a description of major information and record locator systems maintained by the agency; and
- (3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

* * * * *

Section 12. Effective Date [not to be codified].

- (a) Except as provided in subsection (b), this Act shall take effect 180 days after the date of the enactment of this Act [March 31, 1997].
- (b) Sections 7 and 8 shall take effect one year after the date of the enactment of this Act [October 2, 1997].

Below is the full text of the statement issued by President Clinton upon signing the 1996 FOIA amendments into law on October 2, 1996:

I am pleased to sign into law today H.R. 3802, the "Electronic Freedom of Information Act Amendments of 1996."

This bill represents the culmination of several years of leadership by Senator Patrick Leahy to bring this important law up to date. Enacted in 1966, the Freedom of Information Act (FOIA) was the first law to establish an effective legal right of access to government information, underscoring the crucial need in a democracy for open access to government information by citizens. In the last 30 years, citizens, scholars, and reporters have used FOIA to obtain vital and valuable government information.

Since 1966, the world has changed a great deal. Records are no longer principally maintained in paper format. Now, they are maintained in a variety of technologies, including CD ROM and computer tapes and diskettes, making it easier to put more information on-line.

My Administration has launched numerous initiatives to bring more government information to the public. We have established World Wide Web pages, which identify and link information resources throughout the Federal Government. An enormous range of documents and data, including the Federal budget, is now available on-line or in electronic format, making government more accessible than ever. And in the last year, we have declassified unprecedented amounts of national security material, including information on nuclear testing.

The legislation I sign today brings FOIA into the information and electronic age by clarifying that it applies to records maintained in electronic format. This law also broadens public access to government information by placing more material on-line and expanding the role of the agency reading room. As the Government actively disseminates more information, I hope that there will be less need to use FOIA to obtain government information.

This legislation not only affirms the importance, but also the challenge of maintaining openness in government. In a period of government downsizing, the numbers of requests continue to rise. In addition, growing numbers of requests are for information that must be reviewed for declassification, or in which there is a proprietary interest or a privacy concern. The result in many agencies is huge backlogs of requests.

In this Act, the Congress recognized that with today's limited resources, it is frequently difficult to respond to a FOIA request within the 10 days formerly required in the law. This legislation extends the legal response period to 20 days.

More importantly, it recognizes that many FOIA requests are so broad and complex that they cannot possibly be completed even within this longer period, and the time spent processing them only delays other requests. Accordingly, H.R. 3802 establishes procedures for an agency to discuss with requesters ways of tailoring large requests to improve responsiveness. This approach explicitly recognizes that FOIA works best when agencies and requesters work together.

Our country was founded on democratic principles of openness and accountability, and for 30 years, FOIA has supported these principles. Today, the "Electronic Freedom of Information Act Amendments of 1996" reforges an important link between the United States Government and the American people.

Go to: FOIA Update Home Page

Topic(s): FOIA Update

Posted in:

Office of Information Policy

Updated August 13, 2014

INFORMATION SECURITY OVERSIGHT OFFICE

NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE. NW. ROOM 100 WASHINGTON. DC 20408-0001

www.archives.gov/isoo



December 26, 2012

J. William Leonard P.O. Box 2355 Leonardtown, MD 20650 VIA E-MAIL

Dear Mr. Leonard,

I am responding to your letter of July 30, 2011, in which you asked that I, in accordance with my assigned duties under Executive Order 13526, "Classified National Security Information" ("the Order"), consider and take action with regard to what you viewed as a violation of the Order. Specifically, you requested I "ascertain if employees of the United States Government, to include the National Security Agency (NSA) and the Department of Justice (DOJ), have willfully classified or continued the classification of information in violation of the Order" in the matter of *United States v. Thomas A. Drake*. I have concluded my inquiries into this matter, having consulted with the above-mentioned agencies, drawn upon the Order, its implementing Directive, and examined relevant portions of each agency's security regulations, and now share with you my findings and observations.

With regard to your complaint, I conclude that neither employees of the Department of Justice nor of the National Security Agency willfully classified or continued the classification of the "What a Wonderful Success" document in violation of the Order. I wish to note that your complaint suggests this was done "in the matter of *United States v. Thomas A. Drake.*" I think it is important to point out that my process in addressing your complaint examined (and distinguished between) the classification of the document in its first instance and any continuation of its classification "in the matter of *United States v. Thomas A. Drake.*" I find no violation in either case. In fact, as materials you provided with your complaint make clear, NSA discontinued the classification of the document in question and represented the same to the court "in the matter of *United States v. Thomas A. Drake.*"

In examining the "What a Wonderful Success" document, I find that the NSA did not violate the Order's requirements for appropriately applying classification at document creation, nor did the agency violate the Order's expectation that information shall be declassified when it no longer meets the standards for classification. While my examination of the matter has led to my conclusion that the content and processing of the document fall within the standards and authority for classification under the Order and NSA regulations, that does not make them immune to opinions about how substantial the document's content may or may not be. I find, simply, that those opinions do not rise to the level of willful acts in violation of the Order. That said, such commentary on the culture of classification fits well in discussions of policy reform. In such fora, including the work of the Public Interest Declassification Board, your experience and observations would continue to be welcome.

Separate and apart from the specifics of the Drake matter, there are important aspects of the classification system worth noting in this larger discussion of the scope of classification guidance. As you are aware, section 1.1 of the Order grants both responsibility and latitude to Executive branch officials with original classification authority. These officials are the chief subject matter experts in government concerning information that could be damaging to national security if compromised or released in an unauthorized manner.

In light of this, section 2.2 of the Order directs officials with original classification authority to prepare classification guides to facilitate the proper and uniform classification of information. A well-constructed classification guide can foster consistency and accuracy throughout a very large agency, can impart direction concerning the duration of classification, and ensure that information is properly identified and afforded necessary

Roack v. U.S., Phintiff Regonse, Summary Judgment

protections. Throughout the Executive branch, officials strive to impart proper classification guidance that is accurate, consistent, and easy to adopt in workforces that operates under tight time constraints. It seems quite clear, however, that the system would benefit from greater attention of senior officials in ensuring that their guidance applies classification only to information that clearly meets all classification standards in section 1.1 of the Order. For emphasis, I draw specific attention to language in Section 1.1 (a)(4) "... that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security..." and, 1.1 (b) "If there is significant doubt about the need to classify information, is shall not be classified."

I have a few observations about these matters in the context in which you raised them, namely, the matter of the *United States v Thomas A. Drake*. I have no basis to comment about the disposition of the case in the courts; that is not my purview. The conduct of the case did, however, bring to light actions and behaviors I will comment on briefly, for emphasis. The Order does not grant any individual the authority to safeguard classified information in a manner that is contrary to what the Order, its implementing directive, or an agency's security regulations require. The Order does not grant authorized holders of classified information the authority to make their own decisions concerning the classification status of that information. Furthermore, individuals are provided the means to challenge classification either formally or informally. Section 1.8 of the Order provides all authorized holders of classified information with the authority to issue challenges to classification actions. It explicitly states that individuals are "encouraged and expected" to challenge the classification status of the information through appropriate channels, and every agency is required to implement procedures whereby any authorized holder may issue a challenge without fear of retribution. I know, through the work of this Office, that the National Security Agency is well practiced in the Order's requirements concerning classification status of the information in question.

I note that neither version of the Order in force during the Drake case's time frame [Executive Order 13526 (29 December 2009) and its predecessor Executive Order 12958 (17 April 1995)] provides much in the way of guidance or direction, on its own, to influence the use of classified information in building prosecutions such as this. In general, the Department of Justice defers to the judgment of the "victim" agency as to what constitutes classified information. In building a case, victim agencies, for their part, tend to provide evidence that they deem sufficient to obtain a conviction with the hopes of protecting their most sensitive information and activities from release during court proceedings. The Directive (32 CFR 2001.48) requires only that agency heads "use established procedures to ensure coordination with" the Department of Justice and other counsel. All of this assumes that other influences will be at work to pursue only worthwhile prosecutions, but one interpretation of the Drake case outcome might suggest that this "coordination" was not sufficient. I would welcome your thoughts on whether there is role for policy to provide clearer, more effective guidance in the manner in which such cases are built.

I thank you for your diligent, care-filled observations and comments concerning classification matters. You continue to serve the public well by remaining engaged in the dialogue around the use of secrecy by the government. I can assure you that we take these viewpoints to heart.

Sincerely,

<Signed>

JOHN P. FITZPATRICK Director, Information Security Oversight Office



From: Bill Leonard

Date: December 31, 2012, 4:10:23 PM EST

To: John Fitzpatrick Subject: Re: Complaint

John:

Thanks very much for your <u>reply</u>. While I appreciate the time, effort and consideration you put into this matter, I am nonetheless disappointed in the substance of your reply. Some of my final thoughts on this matter include:

- 1. It took almost one and a half years to respond to a rather straightforward yet serious request. I recognize the need for coordination; nonetheless, irrespective of the nature of the reply, responsiveness is essential for a system to be able to be self-correcting.
- 2. As we discussed when we met in August 2011, I have never taken real issue with the classification of the "What a Success" document in the first instance, which although improper was, by all appearances, a reflexive rather than willful act. Nor did I take issue with its eventual "declassification," which I regarded as NSA simply coming to the proper conclusion, albeit belatedly. What I did and continue to take issue with is that in between those events, senior officials of both the NSA and DoJ made a number of deliberate decisions to use the supposed classified nature of that document as the basis for a criminal investigation of Thomas Drake as well as the basis for a subsequent felony indictment and criminal prosecution. Even after NSA recognized that the document did not meet the standards for continued classification and made the unprecedented decision to declassify an evidentiary document while an Espionage Act criminal prosecution was still pending, senior officials of both the NSA and DoJ still willfully persisted and made yet another deliberate decision to stand by the document's original classification status. I cannot imagine a clearer indication of willfulness on the part of senior government officials to "continue the classification of information in violation" of the governing order through numerous deliberate and collaborative decisions made over the course of years. Based upon my extensive experience, I find the provenance of this document's classification status to be unparalleled in the history of criminal prosecutions under the Espionage Act.
- 3. You ascribe the merits of my complaint as constituting a mere honest difference in opinion. However, this complaint is more than a question of the document failing to pass what I call the "guffaw test" (i.e. common sense). Rather, as I pointed out in my original complaint and yet you did not address, at the heart of this issue are matters of fact. In justifying the deliberate decision to represent during the Drake prosecution that the "What a Success" email was a legitimately classified document, NSA and DoJ officials did not cite some amorphous classification standard or classification guide rather they made factual representations which simply were not true and, in one instance, inherently contradictory (i.e. "information contained therein **reveals ... a specific level** (emphasis added) of effort ..."

and that the same information "implied a level (emphasis added) of effort ..."). Keep in mind that these determinations were not made on the fly by NSA and DoJ but were in fact deliberate representations made over a period of time and subsequently further qualified but never disavowed. They were intended to demonstrate that the document met the standards of classification that require the original classification authority to identify or describe the damage to national security that could reasonably be expected to result from the unauthorized disclosure. A familiarity with classification standards is not required to determine that these official representations were on their face factually incorrect when compared with a plain text reading of the "What a Success" email. All too often, representatives of the Executive branch believe all they need to do is simply assert classification rather than adhere to the president's own standards, as apparently was the situation in the Drake case. That attitude must change and I will continue to do all I can to help make it foster change.

4. You comment on the fact that the Order does not grant any individual the authority to handle classified information in a manner contrary to the Order and other pertinent regulations. While reference to alleged actions taken or not taken by Mr. Drake are gratuitous and have no bearing on the merits of my complaint, I nonetheless agree with your sentiment. However, allow me to add my own observations, not only as one of your predecessors but also as the only individual who has played an integral role for both defense teams in the only two Espionage Act prosecutions (Drake and AIPAC) not to result in either a conviction or a plea of guilty. In both instances (in which I provided my services pro bono) my decision to get involved was not to defend the actions of the accused but rather to defend the integrity of the classification system, a highly critical national security tool. I have long held that when government agencies fail to adhere to their responsibilities under the governing order and implementing directive, they in turn compromise their ability to hold cleared individuals accountable for their actions. Accountability is crucial to any system of controls and the fact that your determination in this case preserves an unbroken record in which no government official has ever been held accountable for abusing the classification system does not bode well for the prospect of real reform of the system. This phenomenon, the readily apparent inclusion in the Order of a feckless provision which infers that accountability cuts both ways has once again been proven to be a major source of why most informed observers both inside and outside the government recognize that the classification system remains dysfunctional due to rampant and unchecked over-classification. It is disappointing to note that a genuine opportunity to instill an authentic balance to the system has been forfeited in this instance.

As to your request for my recommendations as to the potential for clearer guidance when the classification status of information is integral to a criminal prosecution, I would recommend requiring coordination with an independent body such as the Interagency Security Classification Appeals Panel. In the two cases I referenced above, the fact that the government did not obtain a criminal conviction under the Espionage Act actually bode well for the integrity of the classification system -- otherwise, the perceived wisdom in the reflexive over-classification of information would have been codified in case law.

Finally, I stand ready to share my experiences and observations with the Public Interest

Declassification Board and other fora as seen fit.

Thanks again for the reply, John. While I admire the job you do and the challenges you face, I obviously disagree with the content of your reply. Nonetheless, I am appreciative of the courtesy.

Best wishes for the New Year.

jwl



From: Bill Leonard

Date: December 31, 2012, 4:10:23 PM EST

To: John Fitzpatrick Subject: Re: Complaint

John:

Thanks very much for your <u>reply</u>. While I appreciate the time, effort and consideration you put into this matter, I am nonetheless disappointed in the substance of your reply. Some of my final thoughts on this matter include:

- 1. It took almost one and a half years to respond to a rather straightforward yet serious request. I recognize the need for coordination; nonetheless, irrespective of the nature of the reply, responsiveness is essential for a system to be able to be self-correcting.
- 2. As we discussed when we met in August 2011, I have never taken real issue with the classification of the "What a Success" document in the first instance, which although improper was, by all appearances, a reflexive rather than willful act. Nor did I take issue with its eventual "declassification," which I regarded as NSA simply coming to the proper conclusion, albeit belatedly. What I did and continue to take issue with is that in between those events, senior officials of both the NSA and DoJ made a number of deliberate decisions to use the supposed classified nature of that document as the basis for a criminal investigation of Thomas Drake as well as the basis for a subsequent felony indictment and criminal prosecution. Even after NSA recognized that the document did not meet the standards for continued classification and made the unprecedented decision to declassify an evidentiary document while an Espionage Act criminal prosecution was still pending, senior officials of both the NSA and DoJ still willfully persisted and made yet another deliberate decision to stand by the document's original classification status. I cannot imagine a clearer indication of willfulness on the part of senior government officials to "continue the classification of information in violation" of the governing order through numerous deliberate and collaborative decisions made over the course of years. Based upon my extensive experience, I find the provenance of this document's classification status to be unparalleled in the history of criminal prosecutions under the Espionage Act.
- 3. You ascribe the merits of my complaint as constituting a mere honest difference in opinion. However, this complaint is more than a question of the document failing to pass what I call the "guffaw test" (i.e. common sense). Rather, as I pointed out in my original complaint and yet you did not address, at the heart of this issue are matters of fact. In justifying the deliberate decision to represent during the Drake prosecution that the "What a Success" email was a legitimately classified document, NSA and DoJ officials did not cite some amorphous classification standard or classification guide rather they made factual representations which simply were not true and, in one instance, inherently contradictory (i.e. "information contained therein reveals ... a specific level (emphasis added) of effort ..."

Roark V. U.S., Plaintiff Responce, Summery Judgment

Case 6:12-cv-01354-MC Document 101-1 Filed 02/02/15 Page 46 of 55 and that the same information "implied a level (emphasis added) of effort ..."). Keep in mind that these determinations were not made on the fly by NSA and DoJ but were in fact deliberate representations made over a period of time and subsequently further qualified but never disavowed. They were intended to demonstrate that the document met the standards of classification that require the original classification authority to identify or describe the damage to national security that could reasonably be expected to result from the unauthorized disclosure. A familiarity with classification standards is not required to determine that these official representations were on their face factually incorrect when compared with a plain text reading of the "What a Success" email. All too often, representatives of the Executive branch believe all they need to do is simply assert classification rather than adhere to the president's own standards, as apparently was the situation in the Drake case. That attitude must change and I will continue to do all I can to

help make it foster change.

4. You comment on the fact that the Order does not grant any individual the authority to handle classified information in a manner contrary to the Order and other pertinent regulations. While reference to alleged actions taken or not taken by Mr. Drake are gratuitous and have no bearing on the merits of my complaint. I nonetheless agree with your sentiment. However, allow me to add my own observations, not only as one of your predecessors but also as the only individual who has played an integral role for both defense teams in the only two Espionage Act prosecutions (Drake and AIPAC) not to result in either a conviction or a plea of guilty. In both instances (in which I provided my services pro bono) my decision to get involved was not to defend the actions of the accused but rather to defend the integrity of the classification system, a highly critical national security tool. I have long held that when government agencies fail to adhere to their responsibilities under the governing order and implementing directive, they in turn compromise their ability to hold cleared individuals accountable for their actions. Accountability is crucial to any system of controls and the fact that your determination in this case preserves an unbroken record in which no government official has ever been held accountable for abusing the classification system does not bode well for the prospect of real reform of the system. This phenomenon, the readily apparent inclusion in the Order of a feckless provision which infers that accountability cuts both ways has once again been proven to be a major source of why most informed observers both inside and outside the government recognize that the classification system remains dysfunctional due to rampant and unchecked over-classification. It is disappointing to note that a genuine opportunity to instill an authentic balance to the system has been forfeited in this instance.

As to your request for my recommendations as to the potential for clearer guidance when the classification status of information is integral to a criminal prosecution, I would recommend requiring coordination with an independent body such as the Interagency Security Classification Appeals Panel. In the two cases I referenced above, the fact that the government did not obtain a criminal conviction under the Espionage Act actually bode well for the integrity of the classification system -- otherwise, the perceived wisdom in the reflexive over-classification of information would have been codified in case law.

Finally, I stand ready to share my experiences and observations with the Public Interest

Declassification Board and other fora as seen fit.

Thanks again for the reply, John. While I admire the job you do and the challenges you face, I obviously disagree with the content of your reply. Nonetheless, I am appreciative of the courtesy.

Best wishes for the New Year.

jwl

Affidavit for Diane Roark

from Thomas Drake

15 Jan 2015

RE: Access to Gov't Protected Information

State of Maryland, County of Howard

Before the	e undersigned, an officer	duly commissioned by the laws of	Maryland, on
this 15	day of January ,	20 <u>15</u> , personally appeared	/
Thomas	A. Druke	who having first duly sworn an	d says:

During the period of January 2009-April 2009 while under investigation by the US government, I was read in for access to government information deemed "protected information" (including classified information) and then read out of access to "protected information" (including classified information) when appearing multiple times with my private attorney at the National Security Agency at Ft. Meade, Maryland for the purpose of reviewing documents and related material seized from my residence on 28 November 2007 by the FBI, that also included information and documents regarding the THINTHREAD program.

During the criminal proceedings in my case within the period of approximately August 2010 through July 2011 after I was indicted in April 2010, I was given access to a Sensitive Compartmented Information Facility specially built at the Federal District Courthouse in Baltimore, Maryland for the purpose of reviewing information deemed protected information (including classified information) with my public defenders.

Thomas A. Drake

Subscribed and sworn to before me this 6 day of January, 20 15.

VhMCY

·

My Commission Expires on: Nov. 20, 2018

Roark v. U.S., Plaintiff Response, Summary Judgment

Legal Standing and the First Amendment Roark v. U.S.

Attachment 5

Political speech is the most fundamental and most fully protected of all types of speech falling under the First Amendment. Robert H. Bork describes it as "absolute protection for all verbal expression," and "the core of the first amendment, speech that is explicitly political:"

I mean by that criticisms of public officials and policies, proposals for the adoption or repeal of legislation or constitutional provisions and speech addressed to the conduct of any governmental unit in the country." ¹

Political speech is so closely guarded because the framers realized that a representative democracy is "a form of government that is meaningless without open and vigorous debate about officials and their policies." Professor Alexander Meiklejohn said:

The First Amendment does not protect a "freedom to speak." It protects the freedom of those activities of thought and communication by which we "govern." It is concerned, not with a private right, but with a public power, a governmental responsibility.³

By seeking to ban unclassified speech about NSA by employees or former employees, NSA seeks to avoid democratic accountability.

The courts use "strict scrutiny" criteria for restriction of political speech, and most government restrictions do not survive this scrutiny.⁴ There must be a compelling state 1Robert H. Bork, "Neutral Principles and Some First Amendment Problems, *Indiana Law Journal*, Vol. 47, Fall 1971, No. 1, pp. 28,29. 2*Id.*, 26.

3Meiklejohn, *The First Amendment is an Absolute*, 1961 Sup.Ct.Rev., 245, 255.

4See a statistical analysis by Adam Winkler, "Fatal In Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts," *Vanderbilt Law Review*, Vol. 59, p. 793, 2006.

P. 1 First Amendment and Standing Roark v. U.S., Plaintiff Response, Summary Judgment

interest (that NSA has not proven or even asserted), the policy must be narrowly tailored to achieve that interest, and it must be the least restrictive means for achieving the interest, even if there is another means that is similarly restrictive. It is obvious that Section 6a of the NSAA does not meet these criteria.

NSA's enforcement of its alleged right to seize *private* communications and thus prohibit and punish unclassified communications by its employees or former employees amounts to a "prior restraint" on speech that invokes even higher court scrutiny. The prior restraint doctrine was first developed in *Near v. Minnesota (283 U.S. 697,1931)* for attempted closure of a pesky local newspaper, and the Court still uses the *Near* test in evaluating prior restraints. A follow-on 1971 case, *New York Times Co. v. United States*, rejected the Nixon administration's attempt to enjoin publication of the Pentagon Papers. The government must demonstrate that grave harm will result from a publication or utterance before a court will enjoin the speech.⁵ In *Near*, the Supreme Court held that, except in rare cases, censorship is unconstitutional.

For these reasons we hold the statute, so far as it authorized the proceedings in this action...to be an infringement of the liberty of the press guaranteed by the Fourteenth Amendment. We should add that this decision rests upon the operation and effect of the statute, without regard to the question of the truth of the charges contained ...The fact that the public officers named in this case, and those associated with the charges of official dereliction, may be deemed to be impeccable cannot affect the conclusion that the statute imposes an unconstitutional restraint upon publication.

Other cases closed off censorship of the press by constraining grounds for public officials to sue for libel and by excluding parodies, extending beyond merely defamation suits to

⁵See First Amendment Problem Solving Flowchart, "Fully Protected Speech," http://classes.lls.edu/archive/manheimk/114d3/echarts/speech3.htm.

P. 2 First Amendment and Standing Roark v. U.S.

other torts such as intentional infliction of emotional distress.

Standards are similarly stringent for statutes imposing a prior restraint on speech.

The test most frequently employed is whether the prohibited activity poses a clear and present danger of damage to a legitimate government interest, usually national security.

The courts also expect statutes with precise standards so there is notice of what speech is proscribed. Section 6a of the NSAAh hardly qualifies in this respect. Precision also satisfies due process concerns and avoids inviting arbitrary and subjective application. Vague or overbroad laws tend to suppress speech arbitrarily, so the courts expect narrowly tailored law to meet legitimate state interests. Because First Amendment rights are so easily chilled, courts even allow *jus tertii*, or third party standing, to assert others' rights against an overbroad law. A statute may be characterized by "standing overbreadth" meaning it deters highly valued speech and a large quantity of it.⁶

Freedom of association is the individual right to come together with other individuals and collectively express, promote, pursue and defend common interests.⁷

Again, in the U.S. political associations, notably political parties, are highly protected.

Political association is essential both to establish a genuine democracy and to ensure that it remains healthy, and the right to come together to achieve one's political objectives is an integral part of First Amendment freedom. Law upholding freedom of association as a First Amendment right connected to free speech developed with seminal racial civil rights cases protecting the NAACP in the 1950s and 1960s, then progressed to other groups such as labor unions. A major expansion in protection for political groups also

⁶See First Amendment Problem Solving Flowchart, "Vagueness and Overbreadth." 7(Jeremy McBride, Foredoom of Association, The Essentials of Human Rights, Hodder Arnold, London, 2005, pg. 18.

P. 3 First Amendment and Standing Roark v. U.S.

occurred. *Kusper v. Pontikes*, 414 U.S. 51, 56 -57 (1973) declared that "There can no longer be any doubt that freedom to associate with others for the common advancement of political beliefs and ideas is a form of 'orderly group activity' protected by the First and Fourteenth Amendments." The Fourteenth Amendment, which applied the Bill of Rights to all states of the Union, is considered integral to freedom of association because it is the states that normally impose rules infringing upon it and that must protect the right, notably for organizing the election process.

All About Computers

915 Main St. Aumsville, OR 97325

(503)749-4030 Help@allaboutpcs.us	
Bill To	
Roark, Diane 2000 n scenic view dr stayton or 97383	

Invoice

Date	Invoice #
12/5/2014	5197

Rep	Terms	Customer Phone		
DPM	Due on receipt			

		Di ivi		
Quantity	Description		Rate	Amount
	Flat-Fee Shop Labor. Virus Removal, Malware, Adware & Spyware. Red Flag: Trojan Horse(Or backdoor for remote access Active on Computer. It's been removed as well as varispyware apps.	s) Installed & ous adware and	85	85.00

Payments/Credits

\$-85.00

We are not responsible for lost data, or data loss due to bad or failing hardware. Though rarely we cannot salvage data, we make every attempt to recover lost or over written data & offer many data recovery service options.

Total

\$85.00

Balance Due

\$0.00

Roark v. U.S., Response to Summary Judgement



	Threats			. 7902	
	Select the required action for each result and click 'Aj	oply*.	Trojan (led)		
	File name	Severity	Status	Action	Result
1	C:\\>Intuit_Order_N4849169.htm#882488080	High	Threat: JS:Redirector-SU [Trj]	Delete	ŵ Action successful
***	C:\Users\Diane\\Chrome_Update (1).exe	Low	PUP: Win32:Adware CAH [PUP]	Delete \	Kak Action successful
	C:\Users\Diane\\Chrome_Update (2).exe	Low	PUP: Win32:Adware-CAH [PUP]	Delete	🗱 Action sucreasful
	C:\Users\Diane\\Chrome_Update.exe	Low	PUP: Win32:Adware-CAH [PUP	Delete	🕼 Action successful
	C:\Users\Diane\\Crossword Puzzle.exe	Low	PUP: Win32:PUP-gen [PUP]	Delete	📞 Action successful
	C:\AdwCleaner\\ChromeModule.dll.vir	Low	PUP: Win32:Conduit-D [PUP]	Delete	Action successful
	C:\AdwCleaner\Quarantine\C\\cltmng.exe.vir	Low	PUP: Win32:Conduit-D [PUP]	Delete	Kalaman surcessful
	$C: \label{lem:condition} C: \label{lem:condition} C: \label{lem:condition} Adw Cleaner \label{lem:condition} Quarantine \label{lem:condition} Like \label{lem:condition} Adw Cleaner \label{lem:condition} Quarantine \label{lem:condition} Like \label{lem:condition}$	Low	PUP: Win32:Conduit-D [PUP]	Delete	Action successful
	$C: \label{local-condition} C: \label{local-condition} C: \label{local-condition} Adw Cleaner \mbox{λ. \label{local-condition} $$ E = (1, 1) \mbox{λ. \label{local-condition} $$ E $	Low	PUP: Win32:Conduit-D [PUP]	Delete	🚧 Action suncessful
	C: VAdw Cleaner V VInternet Explorer Module. dll. vir	Low	PUP: Win32:Conduit-D [PUP]	Delete	Gar Action successful
	$C: \label{lem:condition} C: \label{lem:condition} Adw Cleaner \label{lem:condition} Quarantine \label{lem:condition} Like \label{lem:condition} Adw Cleaner \label{lem:condition} Quarantine \label{lem:condition} Like lem:conditio$	Low	PUP: Win32:Conduit-D [PUP]	Delete	Co Action successful
	C:\Basic Software\\ComboFix.exe	High	Threat: Win32:Malware-gen	Delete	🕼 Action successful

Apply this action for all: Fix automatically

Note: the automatic fix tries to repair the file first if repair is not possible, it proceeds to move the file to the Chest. If that fails as well, the file is deleted

2014-12-04 21:04:52 . 2014-12-04 21:04:52 534 ----a-w-C:\Qoobox\Quarantine\Registry backups\\BafeBoot-WudfRd.reg.dat\ 2014-12-04 21:04:52 . 2014-12-04 21:04:52 534 ----a-w-C:\Qoobox\Quarantine\Registry backups\SafeBoot-WudfPf.reg.dat 2014-12-04 20:58:06 . 2014-12-04 20:58:06 3,923 ----a-w-C:\Qoobox\Quarantine\Registry_backups\tcpip.reg _ 2014-12-04 20:49:18 . 2014-12-04 20:49:18 512 ----a-w-C:\Qoobox\Quarantine\MBR_HardDisk0.mbr 2014-12-04 20:46:01 . 2014-12-04 20:49:23 62 ----a-w--C:\Qoobox\Quarantine\catchme.log - Keystrokes 2010-05-14 21:13:07 . 2010-05-14 21:13:07 258 ----a-w-C:\Qoobox\Quarantine\C\ProgramData\ntuser.pol.vir

Agorars to be kenjoy file