Clark D. Cunningham
W. Lee Burge Chair in Law & Ethics
P.O. Box 4037
Atlanta, GA 30302-4037
Phone: 404/413-9168
Fax: 404/413-9225
Email: cdcunningham@gsu.edu
Home page: www.ClarkCunningham.org

GEORGIA STATE UNIVERSITY LAW

September 8, 2016

Dear President Obama,

The week of September 19 in two cases on opposite sides of the country the Department of Justice (DOJ) is expected to continue its efforts to prevent federal courts from being able to decide critical questions involving one of the most important legal issues of our era: what protections are provided by the Constitution for private information stored in cell phones and in the cloud? I write, not to ask you to weigh in on the substantive issues in these cases, but simply to consider in consultation with your Attorney General whether to exercise the executive discretion and judgment to allow the courts to reach the merits in these cases.

In Seattle Microsoft is asking the court to impose limits on the government's ability to use search warrants to read our email without our knowledge when we use Outlook and other cloud-based email systems. An example of such a search warrant is attached. DOJ moved to dismiss the lawsuit at the very outset, saying that Microsoft should not be allowed to raise the constitutional rights of its customers. DOJ also takes the position in the case that customers cannot sue unless they can prove their own email accounts are being seized, but the point of the lawsuit is that DOJ routinely gets orders preventing Americans from ever knowing the government has read their email. The inescapable logic of DOJ's position is that NO American can bring a lawsuit challenging secret warrants to search cloud-based email. The importance of having a decision on the merits is demonstrated by the many friend of the court briefs filed in support of Microsoft from such varied parties as the ACLU, the US Chamber of Commerce and Fox News. Remarkably three former U.S. Attorneys, who collectively served the Western District of Washington for every year from 1989 – 2009, and the retired Special Agent in Charge of the FBI's Seattle office have together filed an amicus brief in support of Microsoft's position. I respectfully suggest you give consideration to whether the administration should drop its opposition to allowing the court to consider Microsoft's request for a declaratory judgment on the merits. September 23 is the deadline for DOJ to file its reply brief.

In United States v. Ravelo, pending in Newark, DOJ has used a search warrant to download the entire contents of a lawyer's personal cell phone, over 90,000 items, and has taken the position it is entitled to look at everything (except for privileged lawyer-client communications) BEFORE the court decides whether the search complied with the Constitution. DOJ has further said there is no point to the court making a decision on the constitutional issues now, declaring even if the court decides that the search violated the Constitution it still has the power to keep and use all the downloaded data. I attach the two letters to the court from U.S. Attorney Fishman so stating. These positions seem

inconsistent with the values of your Administration and indeed of our constitutional form of government. The hearing on the constitutionality of the cell phone search is set for September 19. Once again, I do not ask you to consider the merits of whether the search was constitutional – only the opportunity for Ms. Ravelo, and other Americans subjected to a cell phone search warrant, to be heard by a court before all her private information is reviewed by the government.

I also attach a brief essay with further details about both cases scheduled to be published by the Yale Law Journal Forum next month. I have no relationship with any of the parties in either case.

Respectfully yours,

Clark D. Cunningham
W. Lee Burge Chair in Law & Ethics

cc:
Loretta E. Lynch, Attorney General
Counsel of record in Microsoft v Department of Justice, United States v. Ravelo (by email)

AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JCF
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013 4:30 pm

James C. Francis IV
Judge's signature

City and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT C

Particular Things To Be Seized

I. Information To Be Disclosed By MSN [redacted]:

To the extent that the information described in Attachment A for MSN, [redacted], is within the possession, custody, or control of MSN [redacted], then MSN [redacted] is required to disclose the following information to the Government for each account or identifier listed in Attachment A [redacted] (the "TARGET ACCOUNT") for the period of inception of the account to the present:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files,

and means and sources of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized By The Government

A variety of techniques may be employed to search the seized e-mails for evidence of the specified crimes, including but not limited to keyword searches for various names and terms including the TARGET SUBJECTS, and other search names and terms; and email-by-email review.

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 959, 960, and 963, Title 46, United States Code, Section 70503, and Title 18, United States Code, Section 1956, including, for each account or identifier listed on Attachment A [redacted], information pertaining to the following matters:

a. Any communications:

1. Pertaining to narcotics, narcotics trafficking, importation of narcotics into the United States, money laundering, or the movement or distribution of narcotics proceeds;

2. [redacted];

3. Pertaining to the use of ports or other places of entry to receive or ship narcotics or narcotics proceeds;

4. Related to the physical location of the TARGET SUBJECTS and their co-conspirators;

5. Constituting evidence of who uses the TARGET ACCOUNT, and where they live and work, and where they are using the TARGET ACCOUNT; and

6. Constituting information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

U.S. Department of Justice

United States Attorney
District of New Jersey

970 Broad Street, 7th floor
Newark, New Jersey 07102

973-645-2700

May 23, 2016

Honorable Kevin McNulty
United States District Judge
United States Post Office and Courthouse
Federal Square
Newark, New Jersey 07102

Re: United States v. Ravelo
Crim. No. 15-576 (KM)

Dear Judge McNulty:

Please accept this letter brief in lieu of a more formal brief in opposition to Keila Ravelo's ("Ms. Ravelo" or "the defendant") motion to suppress the evidence obtained from the seizure and search of Ms. Ravelo's cellular telephone ("the Phone"). The Government is in the process of determining whether it will use any evidence obtained from the Phone in its case-in-chief at trial. Until the Government makes this determination, the defendant's motion is not ripe. Thus, for the reasons set forth more fully below, the Government respectfully requests that the Court deny the defendant's motion without prejudice.

Factual Basis and Procedural History

The defendant engaged in a fraudulent scheme from in or about 2008 through in or about July 2014 through which she and her husband, Melvin Feliz, obtained millions of dollars from one of the defendant's clients ("Client 1"). During that time, the defendant was a partner at one law firm from 2008 until approximately October 1, 2010. She then joined a second law firm as partner and remained there through the conspiracy. While at those law firms, Ms. Ravelo spent much of her time representing Client 1.

Ms. Ravelo used her position as a partner at both firms to fraudulently obtain more than $5,000,000. Specifically, Ms. Ravelo and her husband caused two entities to be formed. Both of the entities purported to be

companies that provided litigation support services. Ms. Ravelo and her husband caused those entities to submit invoices to the law firms where Ms. Ravelo was a partner. The invoices claimed that the entities were vendors, that they had performed work for the law firm as part of the law firm's representation of Client 1, and sought payment. In reality, the entities had not performed the work for which they sought payment. Ms. Ravelo then used her position as partner to authorize payment for many, if not all, of the submitted invoices.

The defendant and her husband reaped significant profits from their criminal activity. Indeed, records demonstrate that Ms. Ravelo and her husband caused the supposed vendors to transfer more than $4,000,000 into the couple's joint bank account. Ms. Ravelo and her husband then used the majority of this money to cover personal expenses and to fund investments. In addition, Ms. Ravelo and her husband made sure they kept all their fraudulently-obtained money by failing to report and pay taxes on this income.

On or about December 19, 2014, the Honorable Joseph A. Dickson, United States Magistrate Judge for the District of New Jersey, signed a Complaint charging Ms. Ravelo and her husband with conspiring to commit wire fraud and issued an arrest warrant for both individuals.

On or about December 22, 2014, law enforcement executed the warrants and arrested Ms. Ravelo and her husband. During the arrest law enforcement took possession of the Phone. On December 24, 2014, the Honorable Cathy L. Waldor, United States Magistrate Judge for the District of New Jersey, executed a warrant authorizing law enforcement to search the Phone.

The Government has told defense counsel that it will provide the search warrant affidavit for the Phone ("the Affidavit") if the Government determines that it intends to use evidence from the Phone in its case-in-chief at trial or if bound to do so by any other discovery obligations.

Following the issuance of the search warrant for the Phone, an AUSA not part of the trial team ("the filter AUSA") caused a copy of the contents of the Phone to be made and provided a copy of the Phone's contents to defense counsel. At or about that time, the filter AUSA and defense counsel agreed to a protocol whereby defense counsel would review the copy of the contents of the Phone and identify and notify the filter AUSA concerning any material that defense counsel alleged contained privileged material. It is the trial team's understanding that the protocol is currently ongoing.

Argument

The Court should defer on hearing the defendant's motion as it is not ripe for adjudication. A motion to suppress evidence is not ripe when the Government has stated that it does not intend to introduce the evidence. Cf. United States v. LeVasseur, 609 F.Supp.849 (D. Maine 1985) (in light of the Government indicating it would not use the evidence obtained during a search the Court dismissed the defendant's motion to suppress as moot because there was no justiciable issued before the Court); United States v. Martin, 2014 WL 3700917 (D. Minnesota, July 25, 2014) (the Court denied the defendant's motion to suppress as moot because the Government represented it would not use the evidence at issue in its case-in-chief at trial). Indeed, the Federal Rules of Criminal Procedure specifically permit the Court to take such action. Fed. R. Crim. Pro. 12(d) (Courts must decide every pretrial motion before trial unless it finds good cause to defer a ruling).

In this matter, the Government is in the process of determining whether it intends to introduce any of the contents of the Phone in its case-in-chief at trial. Specifically, the Government recognized in advance that the contents of the Phone may include privileged material. The Government, through the filter AUSA, therefore provided a copy of the contents of the Phone to defense counsel. It is the trial team's understanding that defense counsel is currently reviewing the Phone's contents to determine whether, in its view, any privileged materials exist. Once it is determined what, if any, evidence on the Phone is privileged, the trial team will receive the contents of the Phone minus the privileged items. The trial team will then conduct its review and determine if it intends to use any of the contents of the Phone in its case-in-chief at trial. If the trial team determines that it will indeed use any of the contents of the Phone in its case-in-chief at trial, it will provide the Affidavit to defense counsel and will address any motion to suppress at that time[1]. If the Government elects not to so use the contents of the Phone, however, Ms. Ravelo's motion would be moot. Thus, the defendant's motion is not ripe.

[1] As such, the Government is not presently seeking to have the defendant's motion dismissed with prejudice even though it is not supported by a sworn affidavit. Nor it the Government addressing what it believes to be factual inaccuracies in the defendant's submission.

Conclusion

Accordingly, the Government respectfully requests that the Court deny the defendant's motion without prejudice.

Thank you for your consideration.

Respectfully submitted,

PAUL J. FISHMAN
United States Attorney

By: Andrew Kogan
Assistant U.S. Attorney

cc: Lawrence S. Lustberg, Esq.
Steven Sadow, Esq.

U.S. Department of Justice

United States Attorney
District of New Jersey

970 Broad Street, 7th floor
Newark, New Jersey 07102

973-645-2700
Fax: 973-645-2702

July 12, 2016

By ECF and Electronic Mail
Hon. Kevin McNulty
United States Post Office & Courthouse
Federal Square
Newark, New Jersey 07101

Re: United States v. Keila Ravelo
Crim. No. 15-576 (KM)

Dear Judge McNulty:

Please accept this letter brief in response to your Honor's order for briefing on the issues of when the government must return suppressed evidence to a defendant and under what circumstances the government may use the suppressed evidence in a criminal case.

In summary, assuming *arguendo* that the Court granted Keila Ravelo's motion to suppress the contents of her cellular telephone ("the Phone") and a motion to return the Phone, the government would still be able to retain a copy of the Phone to be used lawfully, among other reasons, for impeachment purposes, at a sentencing hearing, filing an appeal, and/or in opposition to any *habeas* petition.

BACKGROUND

On or about December 22, 2014, law enforcement officers arrested Ms. Ravelo and her husband Melvin Feliz pursuant to a Complaint charging them with conspiracy to commit wire fraud. During the course of the arrest, law enforcement took possession of the Phone. On or about December 24, 2014, the Honorable Cathy L. Waldor, United States Magistrate Judge for the District of New Jersey, executed a warrant authorizing law enforcement to search the Phone.

Following the issuance of the search warrant, an AUSA not part of the trial team ("the filter AUSA") caused a copy of the contents of the Phone to be made. The filter AUSA then provided a copy of the Phone's contents to defense counsel. At or about that time, the filter AUSA and defense counsel agreed to a protocol whereby defense counsel would review the copy and identify and notify the filter AUSA concerning any material that defense counsel alleged contained privileged material.

On or about April 29, 2016, Ms. Ravelo filed a motion to suppress the evidence obtained from the seizure and search of the Phone. In response, on or about May 20, 2016, the government filed an opposition motion arguing that Ms. Ravelo's motion was not ripe for adjudication as the government's trial team had not reviewed the contents of the Phone because it was waiting for defense counsel and the filter AUSA to conduct a joint privilege review of the Phone.

At the status conference held on or about June 27, 2016, defense counsel appeared to reverse its earlier position, stating that it did not intend to conduct the joint privilege review of the Phone with the government's filter AUSA. Defense counsel explained that it believed the Court will order suppression of the Phone, thereby obviating defense counsel's need to review the Phone for privileged material. In response, the government argued that both defense counsel and the government's trial team will inevitably have to review the contents of the Phone regardless of whether or not the Court grants Ms. Ravelo's motion to suppress. Shortly thereafter, your Honor ordered the parties to brief the following issues, namely, if the Court were to suppress the evidence obtained from the Phone: (i) what is the government's obligation to return the suppressed evidence (that is, the Phone and its contents), and (ii) what are the government's permissible uses, if any, of the same suppressed evidence in its criminal case?

For the reasons set forth below, were the Court to suppress evidence obtained from the Phone, the government could not use any suppressed evidence from the Phone in its case-in-chief. However, the government could: (1) introduce such evidence to impeach the defendant's testimony and/or certain testimony of other witnesses; (2) use any relevant suppressed evidence from the Phone for sentencing purposes; (3) use relevant suppressed evidence from the Phone in opposition to any *habeas* petition that the defendant might file post-conviction; (4) retain copies of the contents of the Phone, as contemplated by the 1989 Amendments to Fed. R. Crim. P. 41, even if the court granted a motion to return the Phone. Additionally, the government would need to review the contents of the Phone to determine whether an appeal of the court's order to suppress would be appropriate.

PERMISSIBLE USES OF SUPPRESSED EVIDENCE

For over fifty years, the Supreme Court has permitted the government to admit suppressed evidence for certain purposes, regardless

of the exclusionary rule. In this case, if the court were to grant Ms. Ravelo's motion to suppress the contents of the Phone, the government might still try to admit the evidence to, among other reasons, impeach the defendant, prove relevant conduct at sentencing, or oppose a *habeas* petition by the defendant.

In *Weeks v. United States*, 232 U.S. 383 (1914), the Supreme Court initially prohibited the use of evidence seized in violation of the Fourth Amendment to secure a conviction. The Court later explained that the rule of exclusion was based on an effort to deter unlawful police activity and to recognize the judicial integrity in the admission of evidence. *Mapp v. Ohio*, 367 U.S. 643 (1961); *Elkins v. United States*, 364 U.S. 206 (1960). However, the Court also made clear that the exclusionary rule was a judicially created remedy, rather than a constitutional right, and that it did not "proscribe the use of illegally seized evidence in all proceedings or against all persons." *United States v. Calandra*, 414 U.S. 338, 348 (1974).

As such, the courts have allowed evidence obtained in violation of the Fourth Amendment to be used by the government for a variety of purposes. To name just a few examples relevant here, the government may impeach a defendant's false testimony with otherwise excludable evidence that is fruit of the poisonous tree. *Kansas v. Ventris*, 556 U.S. 586, 594 (2009) ("evidence whose very introduction does not constitute the constitutional violation, but whose obtaining was constitutionally invalid[,] is admissible for impeachment" of a testifying defendant); *Harris v. New York*, 401 U.S. 222, 225 (1971) ("Every criminal defendant is privileged to testify in his own defense, or refuse to do so. But that privilege cannot be construed to include the right to commit perjury"); *Walder v. United States*, 347 U.S. 62, 65 (1954) ("[T]here is hardly justification for letting the defendant affirmatively resort to perjurious testimony in reliance on the Government's disability to challenge his credibility"); *United States v. Torres*, 926 F.2d 321, 323 (3d Cir. 1991) (evidence obtained in violation of the Fourth Amendment is admissible for impeachment of defendant's testimony). Illegally obtained evidence can be used to impeach a defendant's testimony on either direct examination or on cross-examination as long as the government's questioning is reasonably suggested by the defendant's direct testimony. *United States v. Havens*, 446 U.S. 620, 627-28 (1980) (illegally seized t-shirt admissible to impeach statements by defendant on cross-examination denying knowledge of scheme using cut-up t-shirt to smuggle cocaine because questions reasonably suggested by direct examination). The government may also use suppressed evidence to impeach witnesses other than the defendant to the extent those witnesses are testifying about out-of-court statements of the defendant herself. *United States v. Rosales-Aguilar*, 818 F.3d 965, 969-70 (9th Cir. 2016).

Evidence obtained in violation of the Fourth Amendment may also be used at sentencing. *United States v. Carlos Torres*, 926 F.2d 321 (3d Cir. 1991) (holding that cocaine that had been suppressed because it was illegally seized could be considered in determining the amount of cocaine involved in the offense for sentencing purposes); *United States v. Tejada,* 956 F.2d 1256, 1262 (2d Cir. 1992) (proper for court to considered suppressed evidence at sentencing despite being illegally obtained because it was not gathered for the express purpose of improperly influencing the sentencing judge). In the post-sentencing context, the government may introduce tainted evidence in *habeas* proceedings. *Stone v. Powell*, 428 U.S. 465, 493 (1976).

In this case, if the court were to grant Ms. Ravelo's motion to suppress evidence obtained from the Phone, Ms. Ravelo would likely file a subsequent motion under Fed. R. Crim. P. 41(g) for the return of the Phone. Were the Court to grant the defendant's Rule 41 motion, the government would likely retain copies of the contents of the Phone. These copies would be necessary so that the government would be able to: (1) impeach any false testimony of the defendant at trial; (2) use any evidence of relevant conduct for sentencing purposes; (3) use the evidence in opposition to a *habeas* petition; and(4) review the evidence so that the U.S. Attorney may certify that the suppressed evidence constitutes "substantial proof of a fact material in the proceeding" to warrant an appeal under 18 U.S.C. § 3731 of the court's grant of Ms. Ravelo's motion to suppress the Phone.

RETURN OF UNLAWFULLY SEIZED PROPERTY

A motion to return property seized by law enforcement is governed by Fed. R. Crim. P. 41(g). Specifically, the rule provides:

> A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. 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, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

If a motion for return of property is made while a criminal prosecution is pending, the burden is on the movant to show that he or she is entitled to the property. *United States v. Chambers*, 192 F.3d 374, 377 (3d Cir. 1999). A Rule 41(g) motion is often properly denied "if the defendant is not entitled to lawful possession of the seized property, the property is contraband or subject to forfeiture, or the government's need for the property as evidence continues." *Id.* (quoting *United States v. Van Cauwenberghe,* 934 F.2d ,1048, 1061 (9th Cir.

1991).

For the same rationale stated in the above case law, Rule 41(g) contemplates that the return of illegally seized property to the defendant does not automatically prohibit the government from retaining copies or making use of the seized property in the future. In 1989, the current provision of Rule 41(g) (then Rule 41(e)) added the language: "If [the court] grants the motion, the court must return the property to the movant, but may impose *reasonable conditions to protect access to the property and its use in later proceedings*." (emphasis added).

The Advisory Committee Note to the 1989 amendment of Rule 41(g) further provides:

> As amended, Rule 41[(g)] avoids an all or nothing approach whereby the [G]overnment must either return records and make no copies or keep originals notwithstanding the hardship to their owner. The amended rule recognizes that reasonable accommodations might protect both the law enforcement interests of the United States and the property rights of property owners and holders. In many instances documents and records that are relevant to ongoing or contemplated investigations and prosecutions may be returned to their owner as long as the [G]overnment preserves a copy for future use.... The amended rule contemplates judicial action that will respect both possessory and law enforcement interests.

"Accordingly, Rule 41[(g)] provides a balance whereby the property interests of the aggrieved party are protected and the legitimate law enforcement interests are not impaired." *Johnson v. United States,* 971 F. Supp. 862, 869 (D.N.J. 1997) (collecting cases). Thus, even in cases where the Government improperly seizes evidence and where the aggrieved party's Rule 41(g) motion is granted, courts have allowed the Government to retain copies of the evidence. *Ramsden v. United States*, 2 F.3d 322 (9thCir. 1993) (allowing the Government to retain copies of the documents at issue in the case despite the Government's violation of the petitioners' constitutional rights). This is so because property that is inadmissible for one purpose may be admissible for another purpose under the Fourth Amendment.

Therefore, even if the Court were to grant Ms. Ravelo's motion to suppress evidence from the Phone and a subsequent Rule 41(g) motion for the return of the Phone, the government would still be permitted to retain a copy of the contents of the Phone "as a reasonable condition" for "its use in later proceedings" and to protect legitimate "law enforcement interests"

as detailed above.

CONCLUSION

In summary, if the Court granted Ms. Ravelo's motions to suppress and to return the Phone, the parties would still have to review the contents of the Phone because the government would still be able to use the Phone's contents for certain lawful purposes.

Respectfully submitted,

PAUL J. FISHMAN
United States Attorney

/s/ Brian Urbano
By: Brian Urbano
Assistant U.S. Attorney

Cc: Lawrence S. Lustberg, Esq.
Steven H. Sadow, Esq.

Apple and the American Revolution:
Remembering Why We Have the Fourth Amendment

Yale Law Journal Company, Incorporated
126 YALE LAW JOURNAL FORUM (forthcoming October 2016)
Clark D. Cunningham[1]
cdcunningham@gsu.edu
www.ClarkCunningham.org

On February 16, 2016, the U.S. Department of Justice (DOJ) obtained an unprecedented court order in the San Bernardino shooting case that would have forced Apple to design and deliver to it software capable of destroying the encryption and passcode protections built into the iPhone.[2] The DOJ asserted that this order was simply the extension of a warrant obtained by the Federal Bureau of Investigation (FBI) to search the shooter's iPhone, which had been locked with a standard passcode.

The FBI's litigation strategy backfired when Apple decided to commit all its resources to getting the order vacated. The Fourth Amendment's guarantee that "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated"[3] was not technically at issue in the San Bernardino case. Nonetheless, when Apple CEO Tim Cook said, "we fear that this demand would undermine the very freedoms and liberty our government is meant to protect,"[4] perhaps for the first time since the era of the Revolution Americans in general began to feel that they needed protection against search warrants.

Apple assembled a team of legal luminaries to challenge the San Bernardino order, including former Solicitor General Ted Olson, who told the media that a loss for Apple would "lead to a police state."[5] The day before the highly anticipated hearing, the DOJ unexpectedly requested an adjournment; a week later the DOJ asked that the order be vacated as no longer necessary, saying that an unnamed "third party" had broken the passcode for the FBI.[6] The DOJ similarly backed off in a later case in New York.[7]

What happened? The FBI took a beating in the media, public opinion, and Congress. As the story of FBI v. Apple received tremendous national media coverage,[8] public opinion shifted to

---

[1] Clark D. Cunningham is the W. Lee Burge Chair in Law & Ethics at Georgia State University College of Law in Atlanta. Thanks to Ryan Bozarth, Tosha Dunn, and reference librarians Pamela C. Brannon, Margaret Elizabeth Butler, and Jonathan Edward Germann for research assistance. The thinking that underlies this essay owes much to teaching and guidance received from James Boyd White and the late Joseph Grano. This is the second line-edit version of this essay; the final edited and formatted version is scheduled for on-line publication in early October. An earlier version, currently available at www.yalelawjournal.org/forum/apple-and-the-american-revolution-remembering-why-we-have-the-fourth-amendment, will be replaced when the final version is published

[2] In the Matter of the Search of an Apple iPhone (C.D. Cal. Feb. 16, 2016), *Order Compelling Apple Inc. to Assist Agents in Search* (No. CM-16-10). Cited case materials and other information are available at: http://clarkcunningham.org/Apple/Cases/SanBernardino.html

[3] U.S. CONST., amend IV.

[4] Tim Cook, *A Message to Our Customers* (Feb. 16, 2016),, http://www.apple.com/customer-letter/

[5] David Goldman & Laurie Segall, *Apple's lawyer: If we lose, it will lead to a 'police state'*, CNN (Feb. 26, 2016), http://money.cnn.com/2016/02/26/technology/ted-olson-apple/.

[6] For further details *see* http://clarkcunningham.org/Apple/Cases/SanBernardino.html

[7] For further details *see* http://clarkcunningham.org/Apple/Cases/EDNY.html.

[8] *See* http://www.nytimes.com/news-event/apple-fbi-case (indexing more than 30 New York Times articles, including four on the front page); http://www.npr.org/series/469827708/the-apple-fbi-debate-over-encryption

support Apple's position.[9] The editorial board of the New York Times opined "Apple is Right to Challenge an Order to Help the FBI";[10] the Wall Street Journal said in an editorial that "more secure phones are a major advance for human freedom";[11] and Pulitzer Prize-winning columnist Clarence Page concluded that the "future of . . . personal liberties . . . is at stake."[12]

The clash between Apple and the FBI/DOJ quickly made its way to Congress's doorstep. Within days of the San Bernardino order, congressional committees commenced hearings in which FBI Director James Comey came under considerable criticism.[13] Two Senators proposed legislation that would force companies to comply with court decryption orders, but the idea drew a filibuster threat, failed to gain support (even from the White House), and was never introduced.[14] The House Homeland Security Committee dismissed the idea of a statute that would authorize "law enforcement access to obtain encrypted data with a court order" as "riddled with unintended consequences," and concluded that "the best way for Congress and the nation to proceed at this juncture is to formally convene a commission of experts to thoughtfully examine not just the matter of encryption and law enforcement, but law enforcement's duty in a world of rapidly evolving digital technology."[15] Legislation to create a Congressionally led expert commission was introduced with broad bipartisan support only two weeks after the San Bernardino order was entered, and a Bipartisan Encryption Working Group has been established jointly by the House Judiciary Committee and the House Energy and Commerce Committee.[16]

The need for legislative action initially prompted by FBI v Apple has become even more compelling as the result of two lawsuits brought by Microsoft. On April 14, 2016 Microsoft sued DOJ alleging that its pervasive use of the "delayed notice" provisions in 18 U.S.C. § 2705 violated the Fourth Amendment by preventing Microsoft from notifying its customers when it was served with search warrants for email stored "in the cloud" on Microsoft servers.[17] In July the U.S. Court of Appeals for the Second Circuit ordered that Microsoft's motion to quash such a warrant in a different case be granted because the statute used by the DOJ did not authorize warrants for email stored outside the United States.[18]

(indexing more than 50 National Public Radio stories); Lev Grossman, *Apple CEO Tim Cook on his Fight with the FBI and Why He Won't Back Down*, TIME (Mar. 28, 2016) (cover story), http://time.com/magazine/us/4262476/march-28th-2016-vol-187-no-11-u-s/.

[9] Michael D. Shear, David E. Sanger & Katie Benner, *Apple Battle Strikes Nerve*, NY TIMES (March 13, 2016) at A1, http://www.nytimes.com/2016/03/14/technology/in-the-apple-case-a-debate-over-data-hits-home.html .

[10] *Why Apple is Right to Challenge an Order to Help the FBI*, N.Y.TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/opinion/why-apple-is-right-to-challenge-an-order-to-help-the-fbi.html

[11] *The FBI vs. Apple: The White House should have avoided this legal and security showdown*, WALL STREET JOURNAL (Feb. 19, 2016), https://homeland.house.gov/wp-content/uploads/2016/03/WSJeditorial.pdf.

[12] Clarence Page, *Apple's standoff with FBI is about more than one iPhone*, CHICAGO TRIBUNE (Feb. 26, 2016), http://www.chicagotribune.com/news/opinion/page/ct-apple-fbi-marco-rubio-iphone-page-perspec-0228-20160226-story.html.

[13] For details *see* http://clarkcunningham.org/Apple/CongressionalAction.html.

[14] *Id.*

[15] STAFF OF H. COMM. ON HOMELAND SECURITY, 114TH CONG., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE 3, https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

[16] For details *see* http://clarkcunningham.org/Apple/CongressionalAction.html.

[17] Microsoft Corp. v. United States Department of Justice (W.D. Wash. June 17, 2016), *First Amended Complaint for Declaratory Judgment* (16-cv-00538-JLR).

[18] Microsoft Corp. v. United States, __ F.3d __, 2016 WL 3770056 (2d Cir. July 14, 2016). Materials on both Microsoft cases available at http://clarkcunningham.org/Apple/Cases/Microsoft.html.

Over twenty years ago Akhil Amar claimed that prevalent thinking of the Fourth Amendment as just a tool of criminal procedure had caused both courts and the public to view the Amendment as little more than "criminals getting off on … technicalities."[19] However, his call for a "return to first principles" by reading carefully the words of the Amendment and the history that gave rise to those words[20] fell largely on deaf ears. But the last nine months, in which two of the three most valuable companies in America[21] have taken the offensive against the federal government to assert the Fourth Amendment rights of everyone, may be a complete game changer, generating momentum for a much-needed and long-overdue reassessment of the use of warrants to seize and search electronically stored information (ESI), whether stored in cell phones, conventional computers or in the cloud. This recent use of high-profile litigation to challenge the power of search warrants is a striking parallel to a series of lawsuits from the 1760s, and the ensuing public debate they caused, that were among the critical events leading to the American Revolution and which established the following bedrock principles underlying the Fourth Amendment:

- The right to keep private papers secure from government surveillance is essential to liberty.
- Search warrants are a grave threat to the security of private papers.
- General warrants to seize and search all of a person's private papers must be absolutely prohibited.

After reviewing the history giving rise to these principles, this essay will show how the DOJ's current practices in using ESI search warrants violate these fundamental principles and concludes by proposing new legislation to restore Fourth Amendment protections to our "private papers" stored in digital form.

I. Why We Have the Fourth Amendment

No less an authority than John Adams has told us "the child Independence was born" in 1761[22] when James Otis filed a petition pro bono on behalf of a group of Boston citizens[23] opposing reissuance of "writs of assistance," which ordered "all Subjects" of the king to assist customs officials so they could enter private homes and "break open" any locked door or chest in search of goods imported without payment of custom duties.[24] According to Adams' eyewitness account, after Otis told the court that the writ of assistance was "the worst instrument of arbitrary power, the most destructive of English liberty,"[25] "[e]very man of an [immense] crowded Audience appeared to me to go away, as I did, ready to take up Arms against Writts of Assistants [sic]. Then and there was the first scene of the first Act of Opposition to the arbitrary Claims of Great Britain."[26]

---

[19] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758-59, 799 (1994)
[20] *Id*. at 759.
[21] Stephen Gandel, *These Are the 10 Most Valuable Companies in the Fortune 500*, FORTUNE (Feb. 4. 2016) (Apple #1, Microsoft #3), http://fortune.com/2016/02/04/most-valuable-companies-fortune-500-apple/.
[22] John Adams, *Letter to William Tudor* (March 29, 1817), 1 LEGAL PAPERS OF JOHN ADAMS 107 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).
[23] Adams, *Petition of Lechmere (Argument on Writs of Assistance) 1761, id.* at 139-41.
[24] Adams, *Thomas Hutchinson's Draft of a Writ of Assistance, id*. at 144-47.
[25] Adams, *Writs of Assistance, id.* at 140.
[26] Adams, *Letter to Tudor, id.* at 107.

Just two years after Otis's passionate speech, a group of political pamphleteers in England struck back against royal oppression by filing a number of successful damage actions challenging the use of general warrants to seize and search their private papers. In the most famous of these cases the British Secretary of State, Lord Halifax, had issued a general warrant "to make strict and diligent search for the . . . authors, printers and publishers of a seditious and treasonable paper, entitled the North Briton, Number 45 . . . and . . . any of them having found, to apprehend and seize, together with their papers."[27] The dragnet search led to the arrest of John Wilkes, a member of Parliament, for being the suspected author. When officers searched Wilkes' London home and encountered a table with a locked drawer, they sent to Halifax for directions, who replied that the drawer must be opened and all manuscripts seized.[28] A locksmith was summoned and the officers took "all the papers in those drawers and a pocket-book of Mr. Wilkes's," put them in a sack, and carried them away.[29]

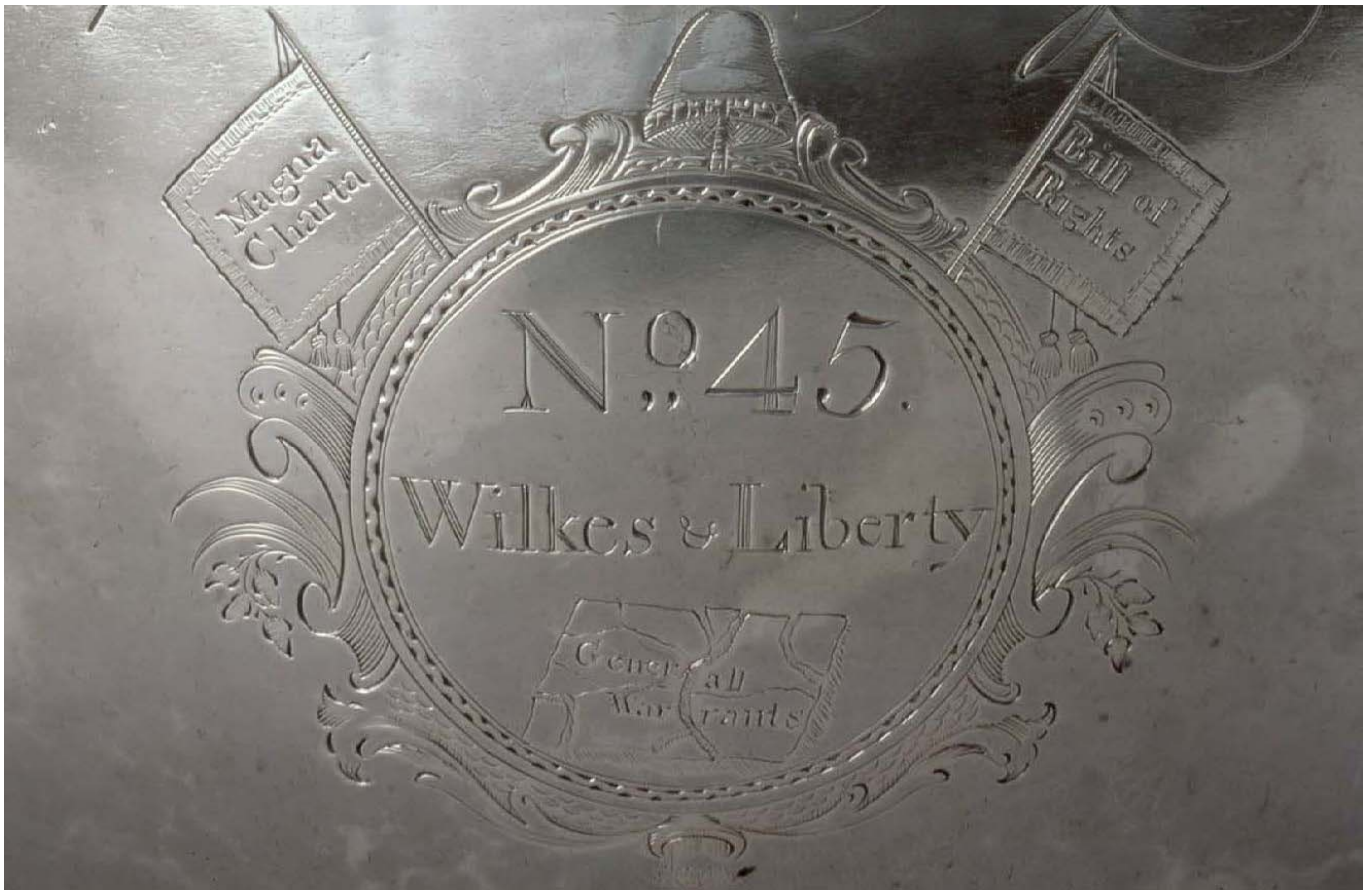
Chief Justice Charles Pratt told the *Wilkes* jury that the defendant's claim to be acting under a legal warrant "was a point of the greatest consequence he had ever met with in his whole practice." He went on, "If such a power is truly invested in a Secretary of State … it … is totally subversive of … liberty".[30]

In another pamphleteer lawsuit, the plaintiff's lawyer told the jury: "Ransacking a man's secret drawers and boxes to come at evidence against him is like racking his body to come at his secret thoughts. Has a Secretary of State right to see all a man's private letters of correspondence, family concerns, trade and business? This would be monstrous indeed; and if it were lawful, no man could endure to live in this country."[31] Affirming the jury's verdict on appeal two years later, Chief Justice Pratt (recently given the title, Lord Camden) authored one of the most widely-cited[32] judicial decisions in Fourth Amendment jurisprudence, declaring: "Papers are … [our] dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection".[33] Asking, "Where is the written law that gives any magistrate such a power?", Lord Camden concluded, "I can safely answer, there is none."[34]

Colonists understood that resistance to writs of assistance in Boston and opposition in England to the use of general warrants to search private papers were all part of a unified struggle for liberty.[35] The famous silver bowl designed in 1768 by Paul Revere for the Boston Sons of Liberty says it all: the image of a general warrant torn in half is paired with the words "No. 45" and "Wilkes & Liberty" and topped by flags labeled "Magna Carta" and "Bill of Rights."[36]

---

[27] Money v. Leach, 97 Eng. Rep. 1075, 1076 (1765). This and subsequently cited English cases challenging general warrants are available at http://clarkcunningham.org/Apple/History/English.html.
[28] Wilkes v. Wood, 98 Eng. Rep. 489, 491, 496 (1763).
[29] *Id.*
[30] *Id.* at 498.
[31] Entick v. Carrington, 19 Howell's State Trials 1030, 95 Eng. Rep. 807, 812 (1765).
[32] *See, e.g.*, Boyd v United States, 116 U.S. 524, 530 (1886)
[33] *Id.*, 19 Howell's State Trials at 1066.
[34] *Id.*
[35] Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 912-14 (1985) (One member of the Sons of Liberty . . . wrote that "The fate of Wilkes and America must stand or fall together.").
[36] *The Sons of Liberty Bowl*, Museum of Fine Arts, Boston, http://www.mfa.org/collections/object/sons-of-liberty-bowl-39072



Otis gave early articulation[37] to "the right of the people to be secure in their … houses" recognized in the first clause of the Fourth Amendment; the pamphleteer lawsuits in England similarly contribute to our understanding the guarantee in the first clause of "the right of the people to be secure in their … papers".[38] What is known as the "particularity requirement" in the second clause --"*no* Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing* the *place to be searched*, and the persons or *things to be seized*"[39] -- can also be traced back to these cases. Otis argued that if a house must be searched, as for stolen goods, only a "special warrant" was lawful: issued "upon oath by the person, who asks, that he suspects such goods to be concealed in THOSE VERY PLACES HE DESIRES TO SEARCH."[40] In the *Wilkes* case, Chief Justice Pratt denied that the defendants had the right "to break open escrutories, seize their papers, etc upon a general warrant, where no inventory is made of the things thus taken away … and … a discretionary power given … to search wherever their suspicions may chance to fall."[41]

---

[37] Adams, *Writs of Assistance*, *supra* note __, at 142 ("Now one of the most essential branches of English liberty, is the freedom of one's house. … This writ, if it should be declared legal, would totally annihilate this privilege.")
[38] U.S. CONST., amend IV. The inclusion of "papers" in the "right to be secure" also expands the potential meaning of "searches." Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541 (1988).
[39] U.S. CONST., amend IV (emphasis added).
[40] *Id*. at 125-26, 141 (capitalization in original).
[41] *Wilkes*, *supra* note __, at 498.

After Independence, many revolutionaries raised the concern that a federal government would, like the vanquished British, abuse the power of the search warrant. At the Virginia ratifying convention for the proposed Constitution Patrick Henry declared: "unless the general government be restrained by a bill of rights [it may] go into your cellars and rooms and search, ransack and measure every thing you eat, drink and wear. Everything the most sacred may be searched and ransacked by the strong hand of power."[42] Ultimately both Virginia and New York conditioned approval on adoption of a Bill of Rights that included a search warrant provision closely modeled on Article 14 of the Massachusetts Constitution of 1780; Article 14 incorporated key points from the 1761 Otis argument and was written by John Adams.[43]

II. Unconstitutional Search Warrant Practices

The FBI's efforts to break iPhone encryption is only the latest chapter in a very troubling story: far from recognizing the special protection the Fourth Amendment is intended to give private papers, the DOJ is almost literally re-enacting the procedures used by Lord Halifax and applying them to seizing and searching electronically stored information, whether maintained on a conventional computer, in the cloud, or on a cell phone. The DOJ standard operating procedure is to obtain warrants that authorize copying the entire data base. Although the DOJ may then choose to use keyword searches and other techniques to look for items of information for which it actually has probable cause to search, it writes into the warrant discretion to look at everything if it chooses.[44]

In 2009 a new section was added to Federal Rule of Criminal Procedure 41 (Search and Seizure) on "Warrant[s] Seeking Electronically Stored Information" that codified the already prevailing DOJ practice of requesting ESI warrants that authorized a "two-step process": (1) seizing either an entire computer hard drive or creating a mirror "image" of the drive and then (2) "later review," typically by an expert in computer forensics, "to determine what [ESI on the drive] falls within the scope of the warrant."[45] Codification of the two-step process coincided with the rise of web-based email service, and the DOJ quickly adapted this procedure, designed for computer hardware, to obtain mirror images of entire email accounts stored in the cloud. The warrant quashed by the Second Circuit last July is illustrative. It ordered Microsoft to turn over "for the period of the inception of the account to the present the contents of all emails stored in the account . . . [and] [a]ll records or other information . . . including address books, contact and buddy lists, pictures, and files . . . ."[46] The warrant further stated: "A variety of techniques may be employed to search the seized emails for evidence of the specified crimes including . . . email-by-email review."[47]

---

[42] Cunningham, *Meanings of Search*, supra note ___, at 554-55.
[43] Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 INDIANA L.J. 979, 1031-51 (2011).
[44] SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATION (3rd ed., U.S. Department of Justice) 79, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. ("Do Not Place Limitations on the Forensic Techniques That May Be Used to Search").
[45] Fed. R. Crim. P. 41(e)(2)(B), Cttee Notes – 2009 Amendment, subdivision (e)(2).
[46] *Search and Seizure Warrant, Attachment C* (S.D. N. Y. Dec. 4, 2013), Joint Appendix A44, 46, *Microsoft v. DOJ*, *supra* note . Warrant available at http://clarkcunningham.org/Apple/Cases/Microsoft.html.
[47] *Id.* at A47.

The DOJ has now brought the two-step process to cell phone searches, with such troubling results as demonstrated in the currently pending case of *United States v. Ravelo*. In this prosecution for alleged white collar crime the government downloaded all "the user-generated content" from the iPhone of a prominent attorney including "emails, text messages, contact list, and user-generated photographs,"[48] more than 90,000 separate items of information.[49] The U.S. Attorney has written a letter remarkably similar to the letter Lord Halifax sent to Wilkes:

May 7, 1763 Mr. Wilkes Sir, In answer to your letter of yesterday, we acquaint you, that your papers were seized in consequence of the heavy charge brought against you, for being the author of an infamous and seditious libel, for which, notwithstanding your discharge from your commitment to the Tower, his Majesty has ordered you to be prosecuted by his Attorney-general. Such of your papers as do not lead to a proof of your guilt, shall be restored to you. Such as are necessary for that purpose, it was our duty to turn over to those, whose office it is to collect the evidence, and manage the prosecution against you. We are Your humble Servants Egremont Dunk Halifax[50]	May 23, 2016 Dear Judge McNulty, . . . [T]he Government is in the process of determining whether it intends to introduce any of the contents of the Phone in its case-in-chief at trial. . . . Once it is determined what, if any, evidence on the Phone is privileged, the trial team will receive the contents of the Phone minus the privileged items. The trial team will then conduct its review and determine if it intends to use any of the contents of the Phone in its case-in-chief at trial. If the trial team determines that it will indeed use any of the contents of the Phone in its case-in-chief at trial, it will provide the [Search Warrant] Affidavit to defense counsel and will address any motion to suppress at that time. . . . Respectfully submitted, Paul J. Fishman, United States Attorney By: Andrew Kogan, Assistant U.S. Attorney[51]

U.S. Attorney Fishman has further taken the position that, even if the court grants pending motions to suppress all evidence from the phone and to return the phone to Ravelo, thus ruling that the cell phone was seized and searched in violation of the Fourth Amendment, "the government would likely retain copies of the contents of the Phone" and could still use that digital data against Ravelo in a variety of ways.[52]

It has not escaped judicial notice that warrants authorizing the two-step procedure risk becoming general warrants prohibited by the Fourth Amendment, but to date the DOJ has resisted court attempts to address the problem, defending step one by saying that effective computer forensics

---

[48] United States v Ravelo (D.N.J. Feb 19, 2016), *Letter from "Filter" Assistant United States Attorney* (15-CR-576). Cited material and other information about this case available at: http://www.clarkcunningham.org/Apple/Cases/USvRavelo.html

[49] *Id., Letter in Support of Motion to Suppress* (Apr. 29, 2016).

[50] Reprinted in Father of Candor, A LETTER CONCERNING LIBELS, WARRANTS, SEIZURE OF PAPERS AND SURETIES FOR THE PEACE OF BEHAVIOUR 56 (5th ed.) (London: J. Almon 1765), available at: http://clarkcunningham.org/Apple/History/English.html

[51] *Id., Letter in Opposition to Motion to Suppress* (May 23, 2016). "Privileged" refers to possible attorney-client privileged communications.

[52] *Id., Letter from United States Attorney Paul J. Fishman (July 12, 2016).*

require access to the complete data base and, as to step two, arguing that judges lack authority to require ESI warrants to "particularly describe[e] the place[s] to searched and the … things [items of information] to seized"[53] within that data base in order to prevent the kind of "email by email" review authorized by the Microsoft warrant and that the *Ravelo* prosecutors intend to use.[54]

The DOJ also enjoys a tremendous strategic advantage due to the lack of due process in most ESI searches. Search warrant applications are approved *ex parte*, based entirely on the government's one-sided presentation, with no notice to the person affected nor opportunity to be heard. The warrant is typically kept secret through an order to seal the file from both the public and the person affected. The government can appeal the magistrate's decision to deny a warrant application but the person affected has no right to judicial review before the warrant is executed. As argued in the current Microsoft suit challenging DOJ-requested gag orders,[55] the lack of due process is even worse when the warrant is directed at remotely stored email. The only way Americans affected by such gag orders will ever learn that the government has been able to read all their email is if the government decides to prosecute them and attempts to use what it has obtained to secure a conviction.

III. Congressional Action Is Needed

The bipartisan Congressional initiatives described above are very encouraging because Congress is the best forum for developing a comprehensive approach to ESI searches that honors the history and text of the Fourth Amendment.

In the Revolutionary Era, warrants to search private papers were consistently compared to extracting confessions by torture.[56] Therefore an argument worth serious consideration can be made that, just as torture is always unlawful (even when national security may be at stake), Congress should prohibit both federal and state governments from using warrants to obtain personal correspondence and other private information stored on cell phones or in the cloud that is protected by user-controlled encryption.

In any event, warrants to seize and search ESI stored on personal cell phones and computers or in personal cloud accounts, should be issued only for compelling reasons and vigilantly regulated to assure compliance with the Amendment's particularity requirement. Here is an outline of six legislative proposals; the first five track federal law regulating wiretapping and electronic surveillance.

(1) Felony to obtain, disclose, or use ESI except as authorized by this statute;[57]
(2) Limited to specified serious crimes;[58]
(3) Limited to circumstances where other investigatory procedures have already been tried or are unavailable;[59]

---

[53] U.S. CONST., amend IV.
[54] For a comprehensive overview *see* In the Matter of the Search of premises known as: Three Hotmail Email accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. March 28, 2016), slip op. 3-15; *see also* http://clarkcunningham.org/Apple/WhatsWrongWithCellPhoneSearchWarrants.html.
[55] *Microsoft v DOJ*, *supra* note ___.
[56] *Entick*, *supra* note __; *Wilkes*, *supra* note __, at 490. *See also Boyd*, *supra* note __, at 630.
[57] *Cf.* Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. § 2511 (1), (4), § 2515 (2016).
[58] *Cf. id.* § 2516(1)(a)-(t).
[59] *Cf. id.* § 2518(3)(c).

(4) Must be authorized by a DOJ official at least at the level of Deputy Assistant Attorney General or, for state warrants, the principal prosecuting attorney of the relevant jurisdiction;[60] and
(5) Annual detailed report to Congress on ESI warrants.[61]
(6) If a warrant authorizes seizure of a device containing ESI or the copying of ESI from such a device or any other storage media (such as a remote server), the device or copied ESI shall be held under court supervision until the owner of the ESI has been provided notice and an opportunity for a hearing to contest the terms of the warrant and/or the procedures to be used to search the device or copied ESI for one or more items of information described with particularity in the warrant.[62]

The final proposal recognizes that the risk of tampering with or destroying relevant evidence is eliminated by seizure of the device or copying of the ESI and therefore would provide similar rights to notice and a hearing as the target of the warrant would have if the ESI was sought by grand jury subpoena.[63] The other provisions of the sixth proposal are inspired by recommendations made by five federal appellate judges in 2010[64] and subsequently incorporated into computer search warrant procedures approved by the Vermont Supreme Court in 2012.[65]

[60] *Cf. id.* § 2516(1), (2).
[61] *Cf. id.* § 2519.
[62] The prior notice and hearing requirement could be deferred in exigent circumstances, such as probable cause that a terrorist attack was imminent.
[63] *See, e.g.*, In re Grand Jury Subpoena, JK-15-029, United States v. Kitzhaber, No. 15-35434, 2016 WL 3745541 (9th Cir. July 13, 2016).
[64] United States v. Comprehensive Drug Testing Inc., 621 F.3d 1162, 1178 (en banc) (9th Cir. 2010) (Kozinski, C.J., with whom Judges Kleinfeld, W. Fletcher, Paez and M. Smith join, concurring).
[65] In re Appeal of Application for Search Warrant, 71 A.3d 1158 (Vt. 2012).