

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. Cunningham¹
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 words²⁰ fell largely on deaf ears. But the last nine months, in which two of the three most valuable companies in America²¹ 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 1761²² when James Otis filed a petition pro bono on behalf of a group of Boston citizens²³ 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-cited³² 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).

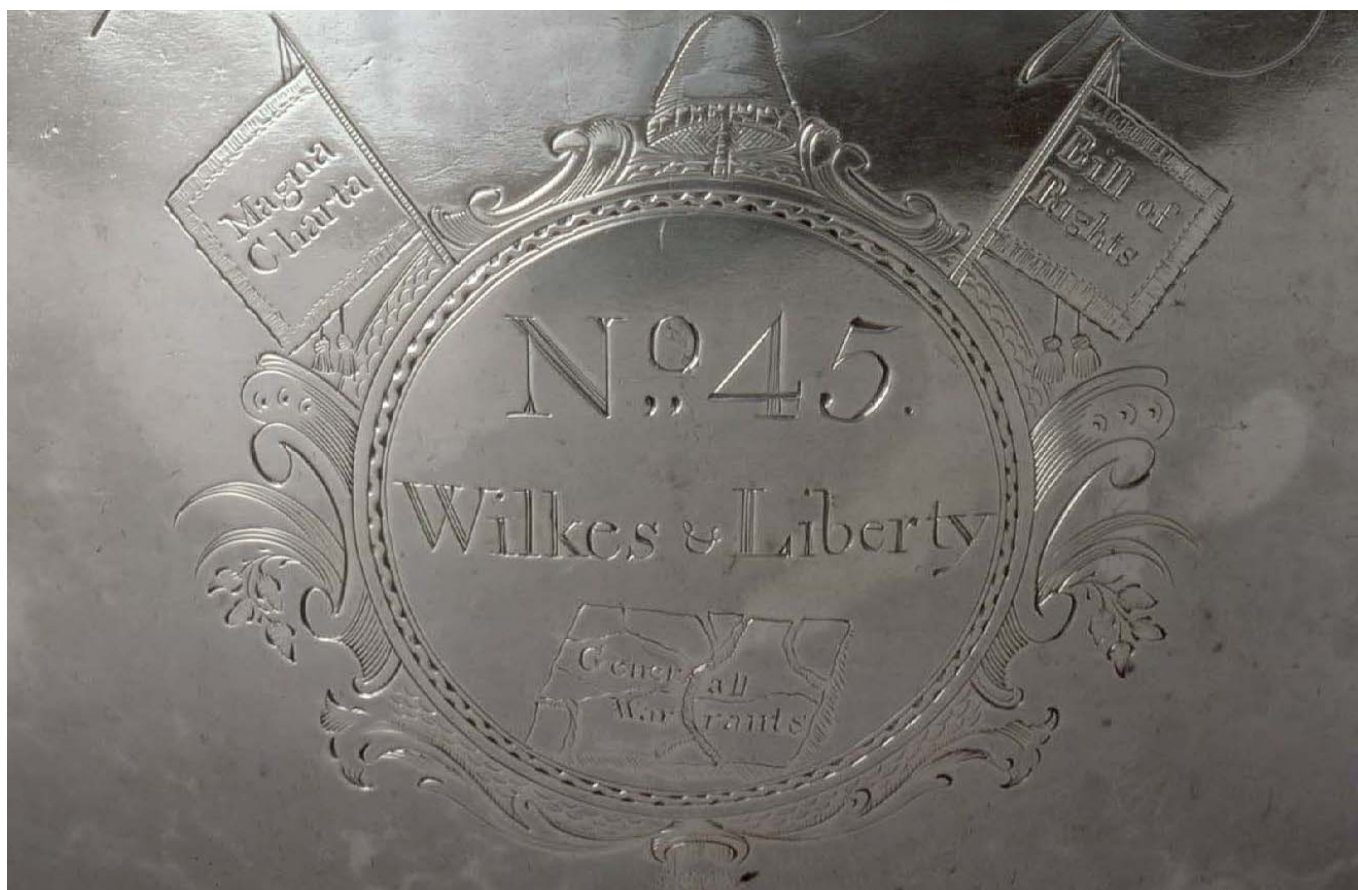
³² *See, e.g., Boyd v. United States*, 116 U.S. 524, 530 (1886).

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 articulation³⁷ 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:

<p>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 Halifax⁵⁰</p>	<p>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. Attorney⁵¹</p>
--	---

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 2010⁶⁴ 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).