

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

Clark D. Cunningham

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 the DOJ software capable of destroying the encryption and passcode protections built into the iPhone.¹ 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 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"² was technically not 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,"³ Americans began to feel—perhaps for the first time since the Revolutionary Era—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

-
1. Order Compelling Apple, Inc. to Assist Agents in Search, *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016).
 2. U.S. CONST. amend IV.
 3. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), <http://www.apple.com/customer-letter> [<http://perma.cc/8EU6-49JK>].

loss for Apple would “lead to a police state.”⁴ The day before the highly anticipated hearing, the DOJ unexpectedly requested an adjournment;⁵ 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 support Apple’s position.⁹ In a headline, 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

-
4. David Goldman & Laurie Segall, *Apple’s Lawyer: If We Lose, It Will Lead to a ‘Police State’*, CNNMONEY (Feb. 26, 2016, 12:56 PM), <http://money.cnn.com/2016/02/26/technology/ted-olson-apple> [<http://perma.cc/U3YQ-S6S3>].
 5. See Government’s *Ex Parte* Application for a Continuance, *In re Search of an Apple iPhone*, (C.D. Cal. Mar. 21, 2016), <http://www.scribd.com/doc/305549490/Apple-vs-FBI-Motion-to-Vacate> [<http://perma.cc/XKB2-KHEA>].
 6. See Government’s Status Report, *In re Search of an Apple iPhone*, No. 5:16-CM-00010 (C.D. Cal. Mar. 28, 2016), <http://www.plainsite.org/dockets/2xdz3nkmq/california-central-district-court/usa-v-in-the-matter-of-the-search-of-an-apple-iphone-seized-during-the-execution-of-a-search-war/> [<http://perma.cc/7QBJ-P5KZ>].
 7. Letter from Robert L. Capers, U.S. Attorney, U.S. Dep’t Justice, to Margo K. Brodie, Judge, E.D.N.Y. (Apr. 22, 2016) (“[T]he government no longer needs Apple’s assistance to unlock the iPhone, and withdraws its application.”), *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).
 8. See, e.g., *The Apple-F.B.I. Case*, N.Y. TIMES, <http://www.nytimes.com/news-event/apple-fbi-case> [<http://perma.cc/NT22-JXGC>] (indexing more than thirty *New York Times* articles, including four that appeared on the front page); *The Apple-FBI Debate over Encryption*, NAT’L PUB. RADIO, <http://www.npr.org/series/469827708/the-apple-fbi-debate-over-encryption> [<http://perma.cc/29BC-MZSC>] (indexing more than fifty National Public Radio stories); Lev Grossman, *Inside Apple CEO Tim Cook’s Fight with the FBI*, TIME (Mar. 17, 2016), <http://time.com/magazine/us/4262476/march-28th-2016-vol-187-no-11-u-s> [<http://perma.cc/YCC9-FXJS>] (covering the controversy on *Time*’s front cover).
 9. See, e.g., Michael D. Shear, David E. Sanger & Katie Benner, *In the Apple Case, a Debate Over Data Hits Home*, N.Y. TIMES (Mar. 13, 2016), <http://www.nytimes.com/2016/03/14/technology/in-the-apple-case-a-debate-over-data-hits-home.html> [<http://perma.cc/8WLQ-8HW3>] (describing the “enormous” pushback against the government’s position).
 10. Editorial, *Why Apple Is Right To Challenge an Order To Help the F.B.I.*, 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> [<http://perma.cc/X3ST-UWY8>].
 11. Editorial, *The FBI vs. Apple: The White House Should Have Avoided This Legal and Security Showdown*, WALL ST. J. (Feb. 19, 2016, 10:17 AM), <http://www.wsj.com/articles/the-fbi-vs-apple-1455840721> [<http://perma.cc/884M-36JH>].

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

-
12. Clarence Page, *Apple’s Standoff with FBI Is About More than One iPhone*, CHI. TRIB.: PAGE’S PAGE (Feb. 26, 2016, 1:05 PM), <http://www.chicagotribune.com/news/opinion/page/ct-apple-fbi-marco-rubio-iphone-page-perspec-0228-20160226-story.html> [<http://perma.cc/VR57-WN5G>].
 13. See, e.g., *Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016) (questions to FBI Director James Comey by Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary; Rep. John Conyers, Rep. Jerrold Nadler, Rep. Zoe Lofgren, Rep. Ted Poe & Rep. Hakeem Jeffries, Members, H. Comm. on the Judiciary), 2016 WestLaw NewsRoom 6586673; Interview by Scott Simon with Rep. Ted Lieu, *After Apple Case, Encryption vs. National Security Dilemma Has Just Begun*, NAT’L PUB. RADIO (Apr. 2 2016, 8:06 AM), <http://www.npr.org/2016/04/02/472784761/after-apple-case-encryption-vs-national-security-dilemma-has-just-begun> [<http://perma.cc/ZK57-UWXR>] (“[T]here has been not a single case that the FBI or anybody else can come up with that would have showed that had the FBI had a back door to a smartphone that they could have stopped any terrorist attack anywhere. What the FBI really is trying to do is to make some law enforcement investigations easier so they can prosecute criminals. It is not a terrorism issue. It really is a law enforcement investigatory tool issue. And the question is - do you want to make some law enforcement investigations easier, but damage national security in the process?”); Cecilia Kang, *Ron Wyden Discusses Encryption, Data Privacy and Security*, N.Y. TIMES (Oct. 9, 2016), <http://www.nytimes.com/2016/10/10/technology/ron-wyden-discusses-encryption-data-privacy-and-security.html> [<http://perma.cc/NGV6-UM4D>].
 14. Mark Hosenball & Dustin Volz, *Exclusive: White House Declines To Support Encryption Legislation – Sources*, REUTERS (Apr. 7, 2016, 6:27 AM), <http://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0X32M4> [<http://perma.cc/NDV4-KR4R>]; Dustin Volz, Mark Hosenball & Joseph Menn, *Push for Encryption Law Falts Despite Apple Case Spotlight*, REUTERS, (May 27, 2016, 6:00AM), <http://www.reuters.com/article/usa-encryption-legislation-idUSL2N18N2oG>, [<http://perma.cc/C72K-95UM>]; Danny Yadron, *Oregon Senator Threatens To Filibuster Any Attempt To Weaken Encryption*, GUARDIAN (Mar. 30, 2016, 10:04 PM), <http://www.theguardian.com/us-news/2016/mar/30/oregon-senator-ron-wyden-filibuster-encryption-rightscon> [<http://perma.cc/3RFE-DMV5>].

duty in a world of rapidly evolving digital technology.”¹⁵ Two weeks after the court in San Bernardino issued its order, representatives introduced bipartisan legislation to create a congressionally led expert commission,¹⁶ and in March the House Judiciary Committee and the House Energy and Commerce Committee jointly established a Bipartisan Encryption Working Group.¹⁷

Two recent lawsuits filed by Microsoft against the DOJ have only increased the need for further legislative action.¹⁸ On April 14, 2016, Microsoft sued the 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 emails stored “in the cloud” on Microsoft servers.¹⁹ In July, the U.S. Court of Appeals for the Second Circuit ordered that Microsoft’s motion to quash such a search warrant in a different case be granted because the statute used by the DOJ did not authorize warrants for emails stored outside the United States.²⁰

This recent use of high-profile litigation to challenge the power of search warrants strikingly parallels a series of lawsuits from the 1760s. One such case was a petition brought by citizens of Boston asking the Superior Court to stop issuing “writs of assistance” that authorized forcible entry into their homes to search any “Vaults, Cellars . . . or other Places” and to open “any Trunks,

15. MAJORITY STAFF OF H. HOMELAND SEC. COMM., 114TH CONG., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE 3 (2016), <http://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf> [<http://perma.cc/WZ7P-ZFX8>].

16. Digital Security Commission Act of 2016, H.R. 4651, 114th Cong. (introduced Feb. 29, 2016); see also *McCaul-Warner Commission on Digital Security*, H. HOMELAND SEC. COMM., <http://homeland.house.gov/mccaul-warner-commission-2/> [<http://perma.cc/DY63-6DEN>].

17. Press Release, H. Energy & Commerce Comm., Upton, Pallone, Goodlatte, Conyers Announce Bipartisan Encryption Working Group (Mar. 21, 2016), <http://energycommerce.house.gov/news-center/press-releases/upton-pallone-goodlatte-conyers-announce-bipartisan-encryption-working> [<http://perma.cc/ZXA5-C4UQ>]; Press Release, H. Energy & Commerce Comm., Congressional Leaders: Bipartisan Encryption Working Group Making Progress (June 22, 2016), <http://energycommerce.house.gov/news-center/press-releases/congressional-leaders-bipartisan-encryption-working-group-making-progress> [<http://perma.cc/CQT5-B7MT>].

18. See, e.g., Press Release, Office of Senator Orin Hatch, Hatch Urges DOJ to Work with Congress on ICPA (Oct. 13, 2016), <http://www.hatch.senate.gov/public/index.cfm/2016/10/hatch-urges-doj-to-work-with-congress-on-icpa> [<https://perma.cc/E53Q-X2KE>] (urging the Department of Justice to work with Congress on new legislation to respond to the Second Circuit’s decision in *Microsoft*).

19. First Amended Complaint for Declaratory Judgment, *Microsoft Corp. v. U.S. Dep’t of Justice*, No. 16-cv-00538-JLR (W.D. Wash. June 17, 2016), 2016 WL 3381727.

20. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197, 201-02 (2d Cir. 2016).

Chests, Boxes, fardells or Packs” where smuggled goods or merchandise were “suspected . . . to be concealed.”²¹ This case and the ensuing controversy over writs of assistance were among the critical events leading to the American Revolution.²² A second series of cases, filed in England, successfully challenged the use of warrants to arrest suspected authors and publishers of political pamphlets and to seize all their personal papers. These warrants were condemned as “general warrants” because they authorized nationwide general searches and were not limited to specifically identified persons, places, and papers.

This Essay will examine the writs of assistance and general warrants cases of the 1760s to show how they helped establish the following bedrock principles underlying the Fourth Amendment:

- The right to keep private papers secure from government surveillance is essential to liberty.²³
- Search warrants are a grave threat to the security of private papers.²⁴
- General warrants to seize and search all of a person’s private papers must be prohibited.²⁵

After reviewing this history, this Essay will show how the DOJ’s current practices in using search warrants for electronically stored information (ESI) violate these fundamental principles. This Essay concludes by proposing new legislation to restore Fourth Amendment protections to our “private papers” now kept in digital form.

21. JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY, BETWEEN 1761 AND 1772, app. 404-05 (Boston, Little, Brown & Co. 1865).

22. See text accompanying notes 26-30, *infra*; Oliver M. Dickerson, *Writs of Assistance as a Cause of the Revolution*, in THE ERA OF THE AMERICAN REVOLUTION 40 (Richard B. Morris ed., 1939); Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1, 13-25 (1994).

23. See text accompanying notes 31-41, *infra*; Donald A. Dripps, “Dearest Property”: *Digital Evidence and the History of Private “Papers” as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49 (2013).

24. See text accompanying notes 31-41, *infra*; Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 771-81, 807 (1994).

25. U.S. CONST., amend. IV (“The right of the people to be secure in their . . . papers . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . and particularly describing the . . . things to be seized.”); 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), at *3-15 (explaining that the purpose of Fourth Amendment’s “particularly describing” requirement is to prevent issuance of general warrants).

I. WHY WE HAVE THE FOURTH AMENDMENT

No less an authority than John Adams²⁶ has told us “the child Independence was born” in 1761²⁷ when James Otis filed a petition pro bono on behalf of a group of Boston citizens opposing reissuance of writs of assistance.²⁸ According to Adams’s eyewitness account, Otis told the court that the writ of assistance was “the worst instrument of arbitrary power, the most destructive of English liberty,”²⁹ after which “[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.”³⁰

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.³¹ 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, [e]ntitled *The North Briton*, No. 45 . . . and . . . any of them having found, to apprehend and seize [them], together with their papers.”³² The dragnet search led to the arrest of John Wilkes, a member of Parliament, for being the suspected author. When officers searched Wilkes’s London home and encountered a table with locked drawers, they asked instructions of Lord Halifax, who replied that the drawers must be opened and all manuscripts seized.³³ After summoning a locksmith, the officers took “all the papers in those

26. Adams, later to serve as the second President, seconded the motion for independence passed by the Continental Congress on June 7, 1776, and was appointed to the Committee of Five that drafted the Declaration of Independence. See DAVID MCCULLOUGH, JOHN ADAMS 117-36 (2001).

27. *No. 44 Petition of Lechmere (Argument on Writs of Assistance)*, in 2 LEGAL PAPERS OF JOHN ADAMS 107 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (quoting Letter from John Adams to William Tudor (March 29, 1817)).

28. *Id.* at 139-44.

29. *Id.* at 140.

30. *Id.* at 107 [bracket in original].

31. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 443 (2009) (“The warrant against *The North Briton Forty-Five* was among the most potent stimulants to adjudication in British legal history [T]he warrant figured directly in at least thirty suits or trials. Derivative trials numbered sixteen or more.”); ROBERT R. REA, *The General Warrant in the Courts of Law: The Cases Arising from North Briton No. 45*, in THE ENGLISH PRESS IN POLITICS 1760-1774, at 59-69 (1963).

32. *Money v. Leach* (1765) 97 Eng. Rep. 1075, 1078; 3 Burr. 1742, 1747.

33. *Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 491, 494, 496; Lofft, 1, 5, 10, 14.

drawers and a pocket-book of Mr. Wilkes's," put them in a sack, and carried them away.³⁴

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."³⁵ He went on, "If such a power is truly invested in a Secretary of State . . . it . . . is totally subversive of . . . liberty . . ."³⁶

In another pamphleteer lawsuit, the plaintiff's lawyer told the jury:

[R]ansacking a man's secret drawers and boxes to come at evidence against him[] is like racking his body to come at his secret thoughts [H]as a Secretary of State a right to see all a man's private letters of correspondence, family concerns, trade and business? [T]his would be monstrous indeed; and if it were lawful, no man could endure to live in this country."³⁷

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 judicial decisions in Fourth Amendment jurisprudence:³⁸ he declared that "[p]apers are . . . [our] dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"³⁹ and concluded that "I can safely answer, there is no[]" "written law that gives any magistrate" the power to search and seize personal papers.⁴⁰

34. *Id.* at 491.

35. *Id.* at 498.

36. *Id.*

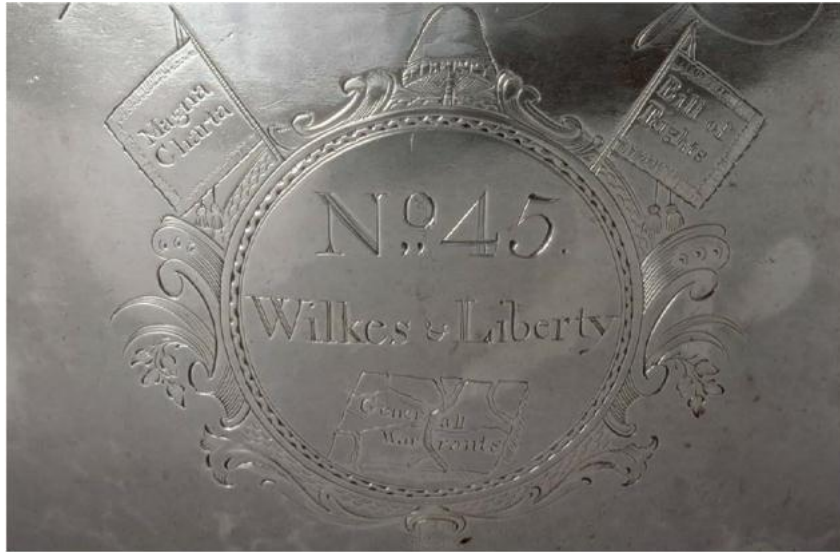
37. *Entick v. Carrington* (1765) 95 Eng. Rep. 807, 812; 2 Wils. K.B. 275, 282. For a larger excerpt of the *Entick* decision, see 19 T. B. HOWELL, A COMPLETE COLLECTION OF STATE TRIALS AND PROCEEDINGS FOR HIGH TREASON AND OTHER CRIMES AND MISDEMEANORS: FROM THE EARLIEST PERIOD TO THE YEAR 1783: 1753-70, at 1030 (1816).

38. See, e.g., *Boyd v. United States*, 116 U.S. 616, 626-27 (1886). ("As every American statesman, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom [Lord Camden's opinion in *Entick*], . . . it may be confidently asserted that its propositions were in the minds of those who framed the fourth amendment to the constitution, and were considered sufficiently explanatory of what was meant by unreasonable searches and seizures.").

39. HOWELL, *supra* note 37, at 1066.

40. *Id.*

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.⁴¹ 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.”⁴²



Otis’s arguments before the court in Boston gave early articulation⁴³ to “the right of the people to be secure in their . . . houses” recognized in the first clause of the Fourth Amendment;⁴⁴ the pamphleteer lawsuits in England similarly contribute to our understanding of the guarantee in the first clause of “the right of the people to be secure in their . . . papers.”⁴⁵ The second clause of the

-
41. 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.*’”).
 42. Paul Revere, *Sons of Liberty Bowl*, MUSEUM OF FINE ARTS BOSTON, <http://www.mfa.org/collections/object/sons-of-liberty-bowl-39072> [<http://perma.cc/NVK4-YQG5>].
 43. Adams’ Minutes of the Argument at Suffolk Superior Court, Boston, on Feb. 24, 1761, in 2 LEGAL PAPERS OF JOHN ADAMS, *supra* note 27, 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.”).
 44. U.S. CONST. amend. IV (emphasis added).
 45. *Id.* 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).

Fourth Amendment, which contains what is known as the “particularity requirement”—“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*”⁴⁶—can also be traced back to these early 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.”⁴⁷ In the *Wilkes* case, Chief Justice Pratt denied that the defendants had the right “to break open escutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away . . . and . . . [and he denied] a discretionary power given . . . to search wherever their suspicions may chance to fall.”⁴⁸

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.”⁴⁹ Ultimately both Virginia and New York conditioned approval on adoption of a bill of rights that included a search warrant provision that incorporated key points from the 1761 Otis argument and closely modeled John Adams’s work on the Massachusetts Constitution.⁵⁰

This history makes clear that the text of the Fourth Amendment was addressed to the kinds of search warrants that were opposed in the writs of assistance and general warrants litigation. In particular, as we now turn to the DOJ’s use of search warrants for email stored in a cloud or on cell phones, we should keep in mind the facts of the *Wilkes* case, described as “*the paradigm search and seizure case for Americans*”⁵¹ in the eighteenth century, and especially the image of royal officers breaking open a locked cabinet, gathering all the papers they can find, and carrying them off for later review.

46. U.S. CONST., amend IV (emphasis added).

47. Adams’ Minutes of the Argument at Suffolk Superior Court, Boston, on Feb. 24, 1761, in 2 LEGAL PAPERS OF JOHN ADAMS, *supra* note 27, at 125-26, 141 (capitalization in original).

48. *Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 498 (KB).

49. 3 DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 448-49 (J. Elliot ed., 2d ed. 1881).

50. Thomas K. Clancy, *The Framers’ Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 981, 1031-51 (2011).

51. Amar, *supra* note 24, at 772 (emphasis in original).

II. UNCONSTITUTIONAL SEARCH WARRANT PRACTICES

The FBI's efforts to break iPhone encryption are only the latest chapter in a very troubling story. Instead of recognizing the Fourth Amendment's special protections for private papers, the DOJ is 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 a cloud, or on a cell phone. The DOJ standard operating procedure is to obtain warrants that authorize copying the entire database. 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 so chooses.⁵²

In 2009, a new section was added to Federal Rule of Criminal Procedure 41 (Search and Seizure) on "Warrant[s] Seeking Electronically Stored Information." The new provisions 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, followed by (2) "later review," typically by an expert in computer forensics, "to determine what [ESI on the drive] falls within the scope of the warrant."⁵³ 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: (a) [t]he contents of all emails stored in the account . . . [and] (b) [a]ll records or other information . . . including address books, contact and buddy lists, pictures, and files . . ." ⁵⁴ 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."⁵⁵

The DOJ has now brought the two-step process to cell phone searches, the troubling consequences of which are on display in *United States v. Ravelo*. In

52. Comput. Crime & Intellectual Prop. Section, *Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP'T JUST. 79-83 (3d ed. 2009), <http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf> [<http://perma.cc/NEX5-P75T>] ("Do Not Place Limitations on the Forensic Techniques That May Be Used to Search").

53. FED. R. CRIM. P. 41(e)(2)(B), Note to Rule 41(e)(2), Committee Notes – 2009 Amendment.

54. Search and Seizure Warrant, Joint App'x A44-48, *Microsoft Corp. v. United States (In re Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197 (2016).

55. *Id.*, Joint App'x at A47.

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,”⁵⁶ totaling approximately 90,000 separate items.⁵⁷ The U.S. Attorney wrote a letter remarkably similar to the letter Lord Halifax sent to Wilkes centuries ago:

FIGURE 1.⁵⁸

LETTER FROM LORD HALIFAX TO MR. 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

FIGURE 2.⁵⁹

LETTER FROM MR. KOGAN TO JUDGE MCNULTY

⁵⁶ Letter from José R. Almonte, Assistant U.S. Attorney, U.S. Dep’t Justice, to Lawrence S. Lustberg, Gibbons P.C. (Feb. 19, 2016), United States v Ravelo (D.N.J. *indicted* Nov. 5, 2015), (2:15-cr-00576-KM) (no. 86-1).

⁵⁷ Letter from Lawrence S. Lustberg, Gibbons P.C., to Kevin McNulty, Judge, Dist. N.J. (Apr. 29, 2016), United States v. Ravelo (D.N.J. *indicted* Nov. 5, 2015), (2:15-cr-00576-KM) (no. 84-1).

⁵⁸ Reprinted in FATHER OF CANDOR, A LETTER CONCERNING LIBELS, WARRANTS, SEIZURE OF PAPERS AND SURETIES FOR THE PEACE OF BEHAVIOUR 56 (London: J. Almon ed., 5th ed.1765) (emphasis in original).

⁵⁹ Letter from Andrew Kogan, Assistant U.S. Attorney, U.S. Dep’t Justice, to Kevin McNulty, Judge, Dist. N.J. (May 23, 2016), United States v Ravelo (D.N.J. *indicted* Nov. 5, 2015), (2:15-cr-00576-KM) (no. 90). “Privileged” refers to possible attorney-client privileged communications.

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

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 return the phone to Ravelo, thus ruling that the cell phone was seized and searched in violation of the Fourth Amendment, “the government w[ill] likely retain copies of the contents of the Phone” and may still use that digital data against Ravelo in a variety of ways.⁶⁰

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.⁶¹ The DOJ has defended step one by saying that effective computer forensics require access to the complete database, and has refused to limit the second step of review of the database,⁶² thus enabling the kind of “email by email” review

60. Letter from Andrew Kogan, Assistant U.S. Attorney, U.S. Dep’t Justice, to Kevin McNulty, Judge, Dist. N.J. (July 12, 2016), *United States v Ravelo* (D.N.J. indicted Nov. 5, 2015), (2:15-cr-00576-KM) (no. 90); see historical evidence to the contrary from the writs of assistance and general warrants cases, note 76, *infra*.

61. 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), at *3-15 (collecting cases and critiquing the two-step process as violating the Fourth Amendment’s particularity requirement).

62. See *id.*; *Computers and Obtaining Electronic Evidence in Criminal Investigations*, *supra* note 52.

that is authorized by the Microsoft warrant⁶³ and that the *Ravelo* prosecutors intend to use.⁶⁴

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 neither notice to the person affected nor the opportunity to be heard.⁶⁵ Reliable estimates indicate that thousands of ESI search warrants are kept secret every year through orders to seal the file from both the public and the person affected.⁶⁶ 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.⁶⁷ As argued in the current Microsoft suit challenging DOJ-requested gag orders,⁶⁸ 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 of their emails 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 in the introduction are encouraging because Congress is the best forum for developing a comprehen-

63. Search and Seizure Warrant, Joint App'x A44-48, *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197 (2016).

64. *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), at *3-4.

65. *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008).

66. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 313 (2012) (describing the search warrant docket of federal magistrates as "the most secret docket in America" and presenting analysis indicating that more than 30,000 federal search warrants issued nationwide in 2006 pursuant to the Electronic Communications Privacy Act were entered subject to an order to seal and that the annual numbers have likely increased since then).

67. *Id.* at 330-33.

68. First Amended Complaint for Declaratory Judgment at para. 37, *Microsoft Corp. v. U.S. Dep't of Justice*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), 2016 WL 3381727. As to the government's argument that the Fourth Amendment does not require notice to the target of the search, see Reply Supporting Motion to Dismiss Pursuant to Fed.R.Civ.P.12(B)(1) and 12(B)(6), at 11-13, *Microsoft Corp. v. U.S. Dep't of Justice*, No. 2:16-cv-00538JLR (W.D. Wash. Sep. 23, 2016).

sive 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.⁶⁹ We ought to take seriously the argument that, just as torture is always unlawful (even when national security may be at stake), Congress should categorically prohibit both federal and state governments from using warrants to obtain personal correspondence and other private information protected by user-controlled encryption that is stored on cell phones or in the cloud.

At a minimum, 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 should be vigilantly regulated to ensure compliance with the Fourth Amendment's particularity requirement. Such a regulation might include the following provisions, the first five of which track federal law regulating wiretapping and electronic surveillance:

- (1) Felony to obtain, disclose, or use ESI except as authorized by this statute;⁷⁰
- (2) Limited to specified serious crimes;⁷¹
- (3) Limited to circumstances where other investigatory procedures have already been tried or are unavailable;⁷²
- (4) Must be authorized by a DOJ official at least at the level of Deputy Assistant Attorney General or, for state warrants, the Attorney General of the relevant jurisdiction;⁷³ and

69. *Entick v. Carrington* (1765) 95 Eng. Rep. 807, 814; 2 Wils. K.B. 275; *Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 490; *Lofft* 1, 5 (1886).

70. *Cf.* 18 U.S.C. § 2511(1), (4) (2012) (stating that, except as otherwise provided in the statute, any person who (a) intentionally intercepts any wire, oral, or electronic communication or (b) intentionally discloses the contents of such interception shall be fined and/or imprisoned not more than five years); *id.* § 2515 (“Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding . . .”).

71. *Cf. id.* at § 2516(1)(a)-(t) (stating that the Attorney General may authorize an application for judicially-approved interceptions when such interception may provide evidence relating to particular serious offenses enumerated in the statute, such as those punishable by death or imprisonment for more than one year).

72. *Cf. id.* at § 2518(3)(c) (providing that a judge may authorize interception if she determines “on the basis of the facts submitted by the applicant” that “normal investive procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous”).

73. *Cf. id.* at § 2516(1) (listing DOJ officials at or above the level of acting Deputy Assistant Attorney General as having the authority to authorize a wiretap application); *id.* § 2516(2)

(5) Annual detailed report to Congress on ESI warrants.⁷⁴

(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.⁷⁵

The final proposal recognizes that the risk of tampering with or destroying the potential evidence identified in the warrant is minimized by seizure of the device or copying of the ESI. The target of the warrant is therefore entitled to similar rights to notice and a hearing as if his ESI had been sought by grand jury subpoena.⁷⁶ The other provisions of the sixth proposal are inspired by rec-

(explaining that the principal prosecuting attorney of any State or the principal prosecuting attorney of any political subdivision thereof may apply for a wiretap order if authorized by state statute).

74. *Cf. id.* at § 2519 (requiring each judge who issues a wiretap order to file a report with the Administrative Office of United States Courts (AOC), each state prosecutor who applies for a wiretap order to issue a similar report to the AOC, and the AOC itself to submit an annual report to Congress documenting the reports it has received); *see, e.g., Wiretap Report 2015*, U.S. CTS. (Dec. 31, 2015), <http://www.uscourts.gov/statistics-reports/wiretap-report-2015> [<http://perma.cc/6MB6-MBU2>].
75. This notice and hearing requirement could be deferred in exigent circumstances, such as probable cause that a terrorist attack was imminent. *Cf.* 18 U.S.C. § 2702(b)(8) (explaining that a provider of electronic communication service may disclose the contents of communication to a governmental entity without a warrant or court order if “the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency”).
76. *See, e.g., United States v. Kitzhaber (In re Grand Jury Subpoena, JK-15-029)*, 828 F.3d 1083, 1088 n.1 (9th Cir. 2016) (quashing grand jury’s subpoena of defendant’s email as overbroad and in violation of the Fourth Amendment and further describing a subpoena’s recipient’s ability to move to quash a subpoena before any search takes place as sufficiently protective of Fourth Amendment rights (citing *City of Los Angeles, Cal v. Patel*, 135 S. Ct. 2443, 2453 (2015))). In condemning a Lord Halifax general warrant, Lord Camden said: “It is executed against the party, before he is heard . . . ; . . . [i]t is executed by messengers . . . in the presence or absence of the party, as the messengers shall think fit [P]roper checks . . . would require [the messenger] to take an exact inventory, and deliver a copy [T]he want of [these precautions] is an undeniable argument against the legality of the thing.” Howell, *supra* note 37, at 1064-65, 1067. Likewise, Otis railed against the writ of assistance because “there’s no return, a man [the executing officer] is accountable to no person for his doings [as would be the case if an inventory was taken and returned with the warrant to the court]. Adams, Adams’ Minutes of the Argument at Suffolk Superior Court, Boston, on Feb. 24, 1761, *supra* note 27, at 142, 143. *See also Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 498 (KB) (“no inventory is made”).

ommendations made by five federal appellate judges in 2010⁷⁷ and subsequently incorporated into computer search warrant procedures approved by the Vermont Supreme Court in 2012.⁷⁸

There have been warnings from an increasing number of federal judges about the DOJ's disregard for the particularity requirement of the Fourth Amendment in its use of ESI search warrants.⁷⁹ Scholars, including two former federal prosecutors with specialized knowledge about ESI search procedures, have also voiced concerns.⁸⁰ Over twenty years ago Akhil Amar claimed that a view of the Fourth Amendment as just a tool of criminal procedure, primarily protecting "criminals getting off on . . . technicalities," risked making the Amendment "contemptible in the eyes of judges and citizens."⁸¹ Amar's call for a "return to first principles" by reading carefully the words of the Fourth Amendment and the history that gave rise to those words⁸² fell largely on deaf ears. But in the last nine months, two of the three most valuable companies in America⁸³ have taken the offensive against the federal government to assert the Fourth Amendment rights of everyone. This offensive has the potential to reinvigorate the nation's commitment to the Fourth Amendment, generating mo-

77. *United States v. Comprehensive Drug Testing Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring).

78. *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1167, 1186 (Vt. 2012) (incorporating all provisions but the waiver of plain view seizure proposed by Judge Kozinski in *Comprehensive Drug Testing*).

79. *See, e.g.*, *United States v. Ganius*, 824 F.3d 199, 226 (2d Cir. 2016) (Chin, J. dissenting); *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), at *50; *In re Search of Apple iPhone*, 31 F. Supp. 3d 159, 164-65 (D.D.C. 2014); *Comprehensive Drug Testing*, 621 F.3d at 1178-80.

80. Paul Ohm, who led a task force in the DOJ Computer Crime and Intellectual Property Section, described ESI search warrants as "the closest things to general warrants we have confronted in the history of the Republic," saying in almost every computer search there is a "manifest lack of probable cause and particularity." *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 4, 11 (2011). Orin Kerr, who wrote the first edition of the DOJ manual on searching computers, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARVARD L. REV. 531, 574 n.189 (2005), has also concluded that ESI searches conducted by the DOJ seem "perilously like the regime of general warrants that the Fourth Amendment was enacted to stop. Everything can be seized. Everything can be searched." Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 11 (2015).

81. Amar, *supra* note 24, at 758-59, 799 (1994).

82. *Id.* at 759.

83. Stephen Gandel, *These Are the 10 Most Valuable Companies in the Fortune 500*, FORTUNE (Feb. 4, 2016), <http://fortune.com/2016/02/04/most-valuable-companies-fortune-500-apple> [<http://perma.cc/KU6S-PXQ8>] (noting that Apple is ranked number one, and Microsoft is ranked number three).

mentum for a much-needed and long-overdue reassessment of the use of warrants to seize and search electronically stored information, whether stored in cell phones or conventional computers, or in the cloud.

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. Cited case materials and other information are available at: <http://clarkcunningham.org/Apple/> [<https://perma.cc/7JPZ-BMXU>].

Preferred Citation: Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. F. 218 (2016) <http://www.yalelawjournal.org/forum/apple-and-the-american-revolution>.