Comments

An Affair to Learn from: Enhanced Procedural Safeguards for Government Access to Stored Communications

By Francesca M. Lanpher*

Introduction

In NOVEMBER 2012, the United States lost, from resignation, its CIA Director, General David Petraeus,[1] one of the most decorated generals in the U.S. Army.[2] The chain of events leading to Petraeus's resignation also revealed the General's extramarital affair with his biographer (and Army reservist), Paula Broadwell.[3] During a criminal investigation into Broadwell,[4] the Federal Bureau of Investigation ("FBI") learned that the biographer previously sent anonymous

* J.D. University of San Francisco School of Law (2014); B.A. International Studies, The Johns Hopkins University (2009). Thank you to Keren Vanisi for her thoughtful comments and support during the publication process. Thank you to University of San Francisco School of Law Professor Susan Freiwald for her inspiration and enthusiasm in the classroom, as well as her staunch representation of the Fourth Amendment. Finally, thank you to my family and husband, Ryan Lanpher, for their unending and invaluable support.

1. Jennifer Epstein, Jonathan Allen & Josh Gerstein, *Gen. David Petraeus Resigns as CIA Director, Citing Affair*, Politico (Nov. 9, 2012), http://www.politico.com/news/stories/1112/83643.html.

2. *See* Biography of General David H. Petraeus, U.S. Dep't of Def., http://www.defense.gov/bios/biographydetail.aspx?biographyid=166 (last visited Nov. 12, 2014).

3. *Timeline of Petraeus Affair Scandal*, Fox News Politics (Nov. 13, 2012), http://www.foxnews.com/politics/2012/11/13/timeline-petraeus-affair-scandal/; Samantha Grossman, *Paula Broadwell, David Petraeus' Biographer and Alleged Mistress*, Time (Nov. 12, 2012), http://newsfeed.time.com/2012/11/12/paula-broadwell-petraeus-biographer-and-alleged-mistress/#ixzz2C2uWN6rq (explaining that Broadwell graduated from West Point and has been recalled to active duty several times to focus on counterterrorism).

4. Richard Engel, *Petraeus' Biographer Paula Broadwell Under FBI Investigation over Access to His Email, Law Enforcement Officials Say*, NBC News (Nov. 9, 2012), http://usnews.nbcnews.com/_news/2012/11/09/15056607-petraeus-biographer-paula-broadwell-under-fbi-investigation-over-access-to-his-email-law-enforcement-officials-say?lite.

harassing e-mails to Jill Kelley, a Florida socialite who worked closely with the U.S. Central Command military base in Tampa.[5] Kelley initiated the investigation of Broadwell when she allowed the government access to an e-mail in her account in an attempt to find her harasser.[6] This initial instance of consensual surveillance of a single e-mail eventually led to the investigation of at least four more individuals' private e-mail accounts without their knowledge.[7] As a result of the surveillance, the individuals suffered not only a tremendous loss of privacy, but also sustained life-altering consequences.[8] The Broadwell investigation highlights the immense governmental power to search stored e-mail content, the impact on the lives of those searched, and the need for enhanced procedural safeguards on government surveillance.[9]

Part I of this Comment provides an overview of the Petraeus scandal, describes the relevant players, and explains the consequences of the government's surveillance for each individual. Part II analyzes three instances where the government's access of electronic data during the investigation raised privacy concerns: (1) when Jill Kelley voluntarily turned over her e-mails to the FBI; (2) when the FBI identified Broadwell as Kelley's pseudonymous e-mail harasser; and (3) when the FBI discovered the e-mail account that Broadwell and Petraeus used to communicate with each other. Each incident implicates a different legal standard that law enforcement officials seeking such electronic information must meet. More significantly, these incidents reflect the relatively unchecked power of the government to access private information without the knowledge or consent of the user. The current regulatory scheme does not sufficiently rein in the government's surveillance power, and the Petraeus investigations highlight a significant need for new legislation. This Comment offers statutory solutions that Congress should implement to improve regulation of government surveillance.

5. *See* Howard Kurtz, *Jill Kelley Says Paula Broadwell Tried to 'Blackmail' Her*, DAILY BEAST (Jan. 22, 2013), http://www.thedailybeast.com/articles/2013/01/22/jill-kelley-says-paula-broadwell-tried-to-blackmail-her.html.

6. *See* Eric Schmitt & Elizabeth Bumiller, *Another General Is Tied to the Petraeus Inquiry*, N.Y. TIMES (Nov. 13, 2012), http://www.nytimes.com/2012/11/14/us/top-us-commander-in-afghanistan-is-linked-to-petraeus-scandal.html?_r=0; Jill Kelley, *How the Government Spied on Me*, WALL ST. J. (Nov. 5, 2013), http://online.wsj.com/news/articles/SB10001424052702303482504579179670250714560.

7. *See infra* Part I.B.

8. *See infra* Part I.B.

9. *See id.*; *infra* Part II.

It is important to note that this Comment focuses on the need for heightened procedural safeguards for surveillance of *stored communications* in criminal investigations. Surveillance of stored communications differs from traditional surveillance methods that monitor targets in real time—e.g. wiretaps and bugs—specifically with respect to notifying a target that he or she has been surveilled. Traditionally, notifying a target risked disrupting the investigation since the target could destroy evidence. However, in the context of stored communications, this risk becomes less serious, or even non-existent.[10] In certain circumstances discussed in this Comment, the law requires investigators to notify the target of stored communication surveillance. In practice, investigators notify the user *after* gaining access to the communications from a third-party service provider, where the communication is stored. Therefore, since investigators have already gained access to the communications when the user is notified, there is no risk of the user destroying such evidence. Additionally, the government can delay notice to the user if it proves that the investigation will be compromised.[11] Further, it can obtain a preservation order requiring the third-party service provider to save copies of stored communications[12] to ensure that no content is lost prospectively.

I. Overview of the Scandal and the Consequences for Each Player

The facts of the Petraeus scandal and the hardships suffered by those involved illustrate the government's immense and unchecked surveillance power over stored e-mail content and should provide the impetus for legislative change.

A. The Scandal

The media frenzy over Petraeus's affair began with Jill Kelley, Tampa socialite and honorary ambassador to the U.S. Central Command Coalition Forces.[13] Kelley received an anonymous message in

10. See *infra* Part II.C.2.i for a response to concerns regarding giving notice of surveillance in criminal investigations involving stored communications.

11. 18 U.S.C. § 2705 (2012).

12. 18 U.S.C. § 2703(f) (2012).

13. Michael Daly, *Jill Kelley's Campaign to Befriend Petraeus, Allen, and Other Top Brass*, DAILY BEAST (Nov. 14, 2012), http://www.thedailybeast.com/articles/2012/11/14/jill-kelley-s-campaign-to-befriend-petraeus-allen-and-other-top-brass.html. Kelley served as a social liaison to the MacDill Air Force Base in Tampa and maintained close relationships with the top commanders at Central Command, including General Petraeus and General Allen. *Id.*

the Yahoo! e-mail account she shared with her husband.[14] The sender of the message, using the pseudonym "kelleypatrol,"[15] allegedly sent Kelley multiple troubling e-mails that contained threats, blackmail, and extortion.[16] Many speculated that jealousy surrounding Kelley's close relationship with General Petraeus sparked the barrage of e-mails, but Kelley claimed she did not know the sender's motivation.[17] However, Kelley "knew [she] was being stalked"[18] and felt threatened enough to notify the FBI in May 2012.[19] At that time, Kelley went to her family friend, FBI Special Agent Frederick Humphries, who brought the e-mails to the FBI cybercrime division.[20] Investigators examined the e-mails and became concerned over language that indicated the sender knew the travel plans and locations of both Petraeus and the U.S. Commander in Afghanistan, General John Allen.[21] When two congressmen and FBI director Robert Mueller learned of the situation, they began an investigation to unmask kelleypatrol.[22]

Initially, the FBI examined every e-mail in Kelley's account, as a "routine step," to determine the identity of kelleypatrol.[23] The sender had registered the e-mail account anonymously, requiring investigators to employ forensic techniques using electronic metadata to determine the identity of the account owner.[24] The FBI compiled a list of the e-mail accounts accessed from the same Internet Protocol ("IP")

14. Kurtz, *supra* note 5.

15. Barton Gellman, *Spyfall*, TIME (Nov. 15, 2012), http://swampland.time.com/2012/11/15/spyfall/.

16. Kurtz, *supra* note 5 (explaining that, allegedly, there were fewer than ten e-mails); *see generally* Kelley, *supra* note 6; (explaining that though the e-mails did not warn Kelley to stay away from Petraeus, Kelley perceived the e-mails as "increasingly severe, and without being explicit, threatening").

17. Kurtz, *supra* note 5.

18. *Id.*

19. *See* Gellman, *supra* note 15.

20. Mike Carter, *Shirtless FBI Agent: Photo Was Joke Emailed to Friends, Reporter*, SEATTLE TIMES (Nov. 14, 2012), http://seattletimes.com/html/localnews/2019684905_agent15m.html?prmid=4939.

21. Sari Horwitz & Kimberly Kindy, *Lawmakers Keep Pressing on Petraeus Timeline*, DAILY HERALD (Nov. 17, 2012), http://www.dailyherald.com/article/20121117/news/711179835/?interstitial=1; *see also* Gellman, *supra* note 15.

22. Carter, *supra* note 20. Humphries brought the situation to U.S. Representative Dave Reichert, who passed the information on the House Majority Leader Eric Cantor, who then relayed the message to FBI Director Robert Mueller. *Id.*

23. *See* Schmitt & Bumiller, *supra* note 6.

24. Scott Shane & Charlie Savage, *Officials Say F.B.I. Knew of Petraeus Affair in the Summer*, N.Y. TIMES (Nov. 11, 2012), http://www.nytimes.com/2012/11/12/us/us-officials-say-petraeuss-affair-known-in-summer.html?pagewanted=2&nl=todaysheadlines&emc=edit_th_20121112&_r=1&.

address within the same time frame as kelleypatrol.[25] Investigators then crosschecked these account owners against guest lists from hotels in the various cities from which kelleypatrol accessed the Internet.[26] These techniques ultimately revealed Paula Broadwell as the account owner and sender of the kelleypatrol e-mails.[27]

The FBI proceeded to search the content of additional e-mail accounts registered under Broadwell's name, which led to the discovery of the Gmail account shared by Broadwell and Petraeus.[28] Instead of exchanging e-mails from separate accounts, Broadwell and Petraeus had shared access to a single account.[29] The couple had composed messages to each other and saved them in a draft folder.[30] The contents of the messages suggested that the two were having an affair.[31]

B. After the Investigation: Consequences for Each Player

The FBI investigation of Broadwell resulted in life-altering consequences for General David Petraeus. On Friday, December 9, 2012, Petraeus resigned from his role as Director of the Central Intelligence Agency ("CIA"). Petraeus's resignation came after he admitted to an extramarital affair with Broadwell—a punishable offense in the mili-

25. Chris Soghoian, *Surveillance and Security Lessons from the Petraeus Scandal*, ACLU (Nov. 13, 2012), http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal.

26. *Id.*

27. *Id.* Internet service providers, such as Yahoo and Google, keep user IP address login records for about a year. *Id.* These records include geolocation data associated with the user, which can be obtained by U.S. law enforcement with a subpoena. *Id.* By logging into other e-mail accounts on the same computer, and consequently the same IP address, associated with her identity, Broadwell created a data trail by which investigators could connect the accounts and identify her. *Id.* She could have taken steps to protect her IP address, but she sent e-mails from many different hotels, which "decreased the anonymity set of potential suspects." *Id.*; *see also* Gellman, *supra* note 15; Shane & Savage, *supra* note 24.

28. *See* Richard Lardner, *Petraeus Case Shows FBI's Authority to Read Gmail, Other Email Services*, HUFFINGTON POST (Nov. 12, 2012), http://www.huffingtonpost.com/2012/11/12/petraeus-fbi-gmail_n_2119319.html ("FBI agents eventually determined that the email trail led to Broadwell, according to two federal law enforcement officials . . . . As they looked further, the FBI agents came across a private Gmail account that used an alias name. On further investigation, the account turned out to be Petraeus's.").

29. Soghoian, *supra* note 25.

30. *Id.* Some users employ this technique with the belief that it creates a communication trail that is harder to trace, but "[e]mails saved in a draft folder are stored just like emails in any other folder in a cloud service, and further, the providers can be compelled, prospectively, to save copies of everything (so that deleting the messages after reading them won't actually stop investigators from getting a copy)." *Id.*

31. *See* Soghoian, *supra* note 25; Lardner, *supra* note 28.

tary[32]—citing it as his reason for stepping down.[33] As part of the criminal investigation into Broadwell, the FBI investigated Petraeus to determine whether he contributed to Broadwell's harassing e-mails to Kelley.[34] The government ultimately chose not to file charges against either Petraeus or Broadwell.[35]

The investigation also negatively affected Broadwell and her family. After the scandal hit newsstands, Broadwell became the center of a national controversy. Additionally, as part of the investigation into Broadwell and after the FBI found classified information on Broadwell's computer, the government conducted a multi-hour search of the Broadwell family home in North Carolina.[36] Ultimately, the FBI concluded that no security breach occurred.[37] However, the Army later revoked Broadwell's promotion from major to lieutenant colonel, pending an internal investigation for wrongdoing.[38]

Jill Kelley found herself dealing with the fallout of the investigation almost a year after the scandal. While she declined to press charges against Broadwell,[39] Kelley brought suit against the government for invasion of privacy.[40] Through the lawsuit, Kelley apparently hoped to unveil the government actors who leaked her name and e-mails to the media in the wake of the scandal in late 2012.[41] She claimed that the leaks violated the 1974 Privacy Act,[42] the FBI failed to provide her with the appropriate security protection to which she was entitled as the victim of a criminal investigation, and the investigation caused her financial loss.[43] Kelley sought monetary damages and an apology.[44]

32. *See* 10 U.S.C. § 934 (2012); United States v. Hickson, 22 M.J. 146 (1986).

33. Epstein, Allen & Gerstein, *supra* note 1.

34. Lardner, *supra* note 28.

35. Kurtz, *supra* note 5.

36. Cleve R. Wootson, Jr., Pam Kelley & Elisabeth Arriero, *FBI Agents Search Paula Broadwell's Home*, McClatchy DC (Nov. 12, 2012), http://www.mcclatchydc.com/2012/11/12/174472/fbi-agents-search-home-of-paula.html.

37. Lardner, *supra* note 28.

38. Barbara Starr, *First on CNN: Paula Broadwell Military Promotion Revoked*, CNN (Feb. 20, 2013), http://security.blogs.cnn.com/2013/02/20/first-on-cnn-paula-broadwell-military-promotion-revoked/.

39. Kurtz, *supra* note 5.

40. Pete Yost, *Gov't Seeks Dismissal of Petraeus-Related Lawsuit*, Army Times (Sept. 24, 2013), http://www.armytimes.com/article/20130924/NEWS/309240042?utm_source=twitterfeed&utm_medium=twitter.

41. *Id.*

42. *Id.*; 5 U.S.C. § 552a(b) (2012).

43. Yost, *supra* note 40; 5 U.S.C. §552a(e)(10).

44. Yost, *supra* note 40.

Additionally, the search of Kelley's e-mail account generated serious consequences for her family friend, FBI Agent Fred Humphries.[45] During the investigation, the government uncovered an e-mail communication from Humphries containing a photograph of him shirtless, posing between target dummies.[46] Humphries captioned the photograph "Which One's Fred?" and sent it to Kelley in 2010.[47] Agent Humphries asserted that the e-mail was a "tongue-in-cheek" joke that he sent to dozens of friends and acquaintances and was not meant to be sexual.[48] The FBI also conducted an internal misconduct probe into Humphries because he raised concerns about improper FBI interference with the investigation outside FBI channels.[49] Humphries claimed that the FBI did not appropriately investigate the kelleypatrol e-mails.[50]

The FBI's search of Kelley's e-mail account also created significant hardships for General John Allen, the top U.S. Commander in Afghanistan at the time.[51] The search revealed potentially flirtatious e-mail correspondence between Kelley and Allen.[52] Initial reports

45. *See* Carter, *supra* note 20.

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*; Michael Isikoff, *Agent Feared FBI Was Stalling Petraeus Investigation Until After 2012 Election*, NBC News Investigations Blog (Nov. 7, 2013), http://investigations.nbcnews.com/_news/2013/11/07/21337699-agent-feared-fbi-was-stalling-petraeus-investigation-until-after-2012-election (explaining that the FBI Office of Professional Responsibility investigated Humphries for "unauthorized disclosure" of law enforcement information and that Humphries declined to disclose details regarding the investigation but maintains that he would handle the matter similarly if it arose again).

50. *See* Isikoff, *supra* note 49.

51. *See* Schmitt & Bumiller, *supra* note 6 (explaining that when the FBI found flirtatious e-mail exchanges between Allen and Kelley, it expanded its investigation to include these e-mails); Elisabeth Bumiller & Scott Shane, *Investigation Into General Narrows Look at E-Mail*, N.Y. Times (Nov. 27, 2012), http://www.nytimes.com/2012/11/28/us/general-allen-investigation-narrows-focus.html?pagewanted=1&_r=1 (explaining that the e-mails were sent by the FBI to the Pentagon on November 11 to determine whether they involved any offenses under military law, like inappropriate language on a government computer or adultery and security breaches, by General Allen).

52. *See* Bumiller & Shane, *supra* note 51 (explaining that the e-mail correspondence had not been made public, but law enforcement described some of the e-mails as "sexually explicit" and "embarrassing," and that General Allen's camp refuted these allegations and argued that the e-mails were "innocuous" and did not say anything "beyond language like 'you're a sweetheart'"); William R. Levesque, *Jill Kelley Says Some of Gen. Allen's Emails Were 'Flirtatious,'* Tampa Bay Times (Feb. 13, 2013), http://www.tampabay.com/news/military/macdill/jill-kelley-says-some-of-gen-allens-emails-were-flirtatious/1275156 (explaining that Kelley later asserted some of the emails were in fact flirtatious).

claimed that Kelley and Allen exchanged thousands of e-mails,[53] but the Pentagon later confirmed that it narrowed its focus to "60 to 70 e-mails that 'bear a fair amount of scrutiny.'"[54] However, the government later determined that the correspondence did not reflect a flirtatious exchange.[55] Not only did this revelation prompt a government investigation of the commander, it also derailed Allen's appointment as NATO Supreme Allied Commander in Europe.[56]

The consequences for each of these five individuals—stemming from a single person's consent to government surveillance—demonstrate the tremendous loss of privacy exchanged for the pursuit of a criminal investigation.[57] The investigation focused on unveiling Broadwell's identity as Jill Kelley's harasser, yet resulted in severe fallout for General Petraeus, General Allen, and FBI Agent Fred Humphries. In particular, General Petraeus committed a largely moral indiscretion, yet experienced arguably unwarranted consequences, including the exposure of his affair, loss of his high-profile position,[58] and possibly loss of international respect. The entire group suffered even though the government ultimately chose not to bring criminal charges after its investigation of Broadwell.[59] In the end, the government cleared General Allen,[60] as of November 14, 2012, did not take or anticipate taking further action against FBI Agent Fred Humphries,[61] and never suspected Jill Kelley of any wrongdoing.[62] The po-

53. Pete Yost & Robert Burns, *John Allen-Jill Kelley Emails Were 'Flirtatious': Senior Defense Official*, HUFFINGTON POST (Nov. 13, 2012), http://www.huffingtonpost.com/2012/11/13/john-allen-jill-kelley_n_2122173.html.

54. Bumiller & Shane, *supra* note 51.

55. *See* Thom Shanker, *Pentagon Clears Commander Over E-Mails*, N.Y. TIMES (Jan. 22, 2013), http://www.nytimes.com/2013/01/23/us/pentagon-clears-general-allen-over-e-mails-with-socialite.html?ref=johnrallen.

56. *See* Bumiller & Shane, *supra* note 51; Thom Shanker & Michael D. Shear, *General Selected for NATO Post Will Retire, Citing Wife's Health*, N.Y. TIMES (Feb. 19, 2013), http://www.nytimes.com/2013/02/20/us/gen-john-r-allen-nominated-for-nato-post-to-retire.html?ref=johnrallen&_r=0.

57. *See* Horwitz & Kindy, *supra* note 21; Gellman, *supra* note 15. Investigators claimed during the initial review of the harassing emails sent to Kelley that the "emails concerned [them] because they indicated that the sender knew of the travel plans of Petraeus and Gen. John R. Allen." Gellman, *supra*.

58. *See* Epstein, Allen & Gerstein, *supra* note 1.

59. Kurtz, *supra* note 5.

60. Shanker & Shear, *supra* note 56.

61. Rhonda Schwartz & Jason Ryan, *Veteran FBI Agent Frederick Humphries Got Ball Rolling on Petraeus Probe*, ABC NEWS (Nov. 14, 2012), http://abcnews.go.com/Blotter/veteran-fbi-agent-frederick-humphries-ball-rolling-petraeus/story?id=17722771.

62. *See* Shanker & Shear, *supra* note 56.

tential national security concern, which revealed no actual threat,[63] was insufficient to justify the loss of privacy suffered by these five individuals, two of whom were only tangentially related to the original investigation.

II. Government Surveillance of Electronic Data During the Broadwell Investigation

The current regulatory scheme in the United States does not adequately check the government's power to access private information about an individual without his or her knowledge or consent. Three instances of government surveillance of electronic data during the investigation of Paula Broadwell demonstrate the lack of protection the current legal regime gives the privacy interests at stake. These instances occurred when: (1) Jill Kelley voluntarily offered the contents of the e-mail in her account to the FBI; (2) the FBI used electronic metadata to identify Broadwell as the sender of the harassing e-mails; and (3) the FBI accessed the content of the shared Gmail account of Broadwell and Petraeus.

Under the current legal regime, government agents must meet different legal standards to obtain initial clearance to conduct each of these three types of surveillance.[64] These legal standards attempt to balance a user's constitutional privacy interest in her electronic data against law enforcement's need to conduct criminal investigations.[65] An analysis of each incident and an application of the appropriate legal standard to each demonstrate that the current regime does not sufficiently protect privacy.

A. Jill Kelley Voluntarily Gives the FBI Access to Her E-mail Account

At the inception of the scandal, Jill Kelley turned over the string of harassing e-mails from kelleypatrol to the FBI, as well as access to her entire e-mail account.[66] The FBI sifted through the content of all e-mails sent or received by Kelley from that account.[67]

63. Lardner, *supra* note 28.

64. *See infra* Parts II.A.1, II.B.1, II.C.1.

65. *Id.*; U.S. CONST. amend IV.

66. *See* Kelley, *supra* note 6. Almost a year after the scandal, Kelley disputed that she turned over several e-mails to the government and claimed that she and her husband "authorized the FBI to look at one threatening email . . . and *only* that email, so that the FBI could identify the stalker." *Id.*

67. *See id.*

1. Legal Standard

The 1966 Supreme Court case *Hoffa v. United States*[68] provides the legal standard for when a user voluntarily allows the government to access her stored e-mail content. The case originally established this legal standard for when someone voluntarily offers oral information to the government, but it is now applied similarly to cases involving electronic information. In *Hoffa*, a criminal defendant revealed incriminating information to a government informant during meetings in the defendant's hotel room.[69] The government later used this information against the defendant at trial.[70] The defendant argued that his discussion with the informant in his hotel room was protected by the Fourth Amendment and therefore must be excluded from use at trial.[71] The Court, however, ultimately determined that no Fourth Amendment violation occurred.[72] It reasoned that the Fourth Amendment protects one from unwarranted government intrusion "when he places himself or his property within a constitutionally protected area,"[73] like the defendant's hotel room. But in this case, the defendant was not relying on the security of his hotel room when he revealed the incriminating information to the informant.[74] The informant did not enter the room surreptitiously, was present with defendant's consent, "and every conversation which he heard was either directed to him or knowingly carried on in his presence."[75] The defendant assumed the risk when he relied "upon his misplaced confidence that [the undercover informant] would not reveal his wrongdoing."[76]

Kelley's situation, in which she voluntarily allowed the government access to the content of her stored e-mail, provides an even stronger example of a user assuming the risk when revealing or hand-

68. 385 U.S. 293 (1966).

69. *See id.* at 296–300.

70. *See id.* at 295.

71. *Id.* at 300 ("The argument is that [the informant's] failure to disclose his role as a government informer vitiated the consent that the [defendant] gave to [the informant's] repeated entries into the suite, and that by listening to the [defendant's] statements [the informant] conducted an illegal 'search' for verbal evidence.").

72. *Id.* at 302.

73. *Id.* at 301.

74. *Id.* at 302.

75. *Id.*

76. *Id.* at 302–303 ("The risk of being overheard by an eavesdropper or by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of *risk we necessarily assume* whenever we speak." (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (emphasis added)).

ing over information to the government. The government did not secretly gain access to Kelley's e-mail content without her knowledge. Instead, Kelley had full awareness that she was giving the information in her e-mails to a government agency.[77] The defendant in *Hoffa* revealed confidential information to an undercover informant, unaware that he was speaking to a government actor.[78] Kelley, however, maintained full knowledge that she gave private information in her e-mail account to the government.

Moreover, although Kelley provided the information to the government for a specific purpose—to facilitate a criminal investigation—and the government disclosed the private e-mail content to the media,[79] current law provides Kelley, or any similarly affected third parties, with no Fourth Amendment protection for such disclosure.[80] Kelley knowingly and voluntarily handed her e-mail account over to the government, assuming the risk that the government would disclose its contents to third parties, such as the press.[81] This ultimately resulted in surveillance not only of Jill Kelley, but also of several other individuals without their consent.[82]

2. Lack of Protection Offered by Current Regime and Need for Legislative Change

The government surveillance of Kelley's stored e-mail content and disclosure of private information demonstrates the insufficiency of outdated legal protections for privacy interests and the need for legislative change. *Hoffa* involved government surveillance and disclosure of incriminating, yet private, information about a certain individual, which the individual *personally* volunteered in the presence of the

77. Kelley, *supra* note 6; *see also* Schmitt & Bumiller, *supra* note 6.

78. *Hoffa*, 385 U.S. at 296–300.

79. *See* Christina Wilkie, *Jill Kelley Sues FBI, Defense Department in Petraeus Scandal*, HUFFINGTON POST (June 3, 2013), http://www.huffingtonpost.com/2013/06/03/jill-kelley-sues-fbi-defense_n_3381167.html.

80. *See Hoffa*, 385 U.S. at 302. Kelley may have a Fourteenth Amendment privacy claim against law enforcement for the disclosure of her personal matters to the media since the disclosure was unrelated to the facilitation of the investigation. The claim would be relatively weak, however, since a similar claim has only been successfully raised in the context of a person's privacy interest in medical information. *See* Doe v. Borough of Barrington, 729 F. Supp. 376 (D.N.J. 1990) (weighing a family's privacy interest in medical records against the societal interest in disclosure, and holding that a police officer violated the family members' Fourteenth Amendment privacy rights by disclosing the father's AIDS virus infection to community members with whom not even casual contact had been made).

81. *Hoffa*, 385 U.S. at 302.

82. Schmitt & Bumiller, *supra* note 6; Carter, *supra* note 20.

government.[83] The private information at stake in *Hoffa* was cabined to a single individual,[84] whereas the privacy interests at stake during the Broadwell investigation implicated various individuals: the investigation of Kelley's e-mails resulted in surveillance of Kelley's private life, as well as the private lives of General John Allen and FBI Agent Fred Humphries.[85] The *Hoffa* standard currently allows for other individuals to suffer consequences even though they did not consent to the surveillance.[86]

The harms experienced by General Allen and FBI Agent Humphries as a result of Kelley's actions demonstrate a serious need to update the law. Congress should incorporate into the Stored Communications Act ("SCA")[87] a provision requiring judicial oversight even if a person allows law enforcement to search her e-mail content. If the government gains access to a single e-mail or even several e-mails from a given account, it should be required to obtain a warrant based on probable cause[88] to access the rest of the e-mails in that account, rather than be given automatic access to them all. Additionally, in any given case of electronic surveillance of stored e-mails, the government should take a cue from the Wiretap Act and give timely notice to the people surveilled.[89] Unless the government files charges against a surveilled person or leaks the private information to the press, it is unlikely that the person will ever discover that the surveillance took place.[90] Notice would allow the individual to bring Fourth Amendment claims against the government if he or she believed that the

83. *Hoffa*, 385 U.S. at 302.

84. *See id.* at 301–02.

85. Schmitt & Bumiller, *supra* note 6; Carter, *supra* note 20.

86. *Hoffa*, 385 U.S. at 302–03. Because one person's voluntary disclosure of private information is not within the scope of the Fourth Amendment's protection, the disclosure of e-mail content reveals communications between the person who disclosed the e-mails and another person. Therefore, both the person who revealed the e-mail content and the other person who participated in the e-mail exchange face the risk that the government will disclose the information in the e-mails to third parties.

87. 18 U.S.C. 121 §§ 2701–12 (2012). The SCA governs when law enforcement seeks records associated with any user subscribed to an ISP. See *infra* Parts II.B.1 and II.C.1 for a detailed outline of the statute's current protections. At present, there are no statutory safeguards in place for a situation in which a person volunteers access to her stored e-mail content.

88. *See infra* Part II.C.1 (discussing the standard for probable cause, which requires that the government show a "fair probability that contraband or evidence of a crime will be found in a particular place" (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

89. *See* 18 U.S.C. § 2518(8)(d) (2012) (detailing the provision of the Wiretap Act that governs surveillance using wiretaps and bugs, which allows judges to order notice to those implicated by the surveillance even if they are not the target of the investigation).

90. Soghoian, *supra* note 25.

surveillance was performed illegally. Such added procedural mechanisms would help to protect the private information of people affected by voluntary e-mail disclosures to law enforcement.[91]

B. FBI Connects Broadwell to Kelleypatrol

The FBI employed forensic metadata techniques[92] to identify Broadwell as the person responsible for sending harassing e-mails to Kelley. Investigators searched for e-mail accounts that used the same IP address as the pseudonymously registered kelleypatrol.[93] To find such e-mail accounts, the FBI requested Internet service providers ("ISPs") to produce records listing the IP addresses that reflected the geographic location from which users had logged in.[94] Investigators then used the geolocation data associated with users' accounts to crosscheck against guest lists from hotels in the various cities from which kelleypatrol accessed the Internet.[95] This ultimately revealed Paula Broadwell as the account owner.[96]

1. Legal Standard

The SCA governs the process by which law enforcement officials may obtain records associated with a user subscribed to an ISP such as Google. The statute provides that an ISP "shall disclose to a governmental entity the . . . telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address"[97]—among other identifying information—"when the governmental entity uses an administrative subpoena authorized

91. See *infra* Part II.C.2.i for responses to concerns regarding giving notice of surveillance in criminal investigations.

92. Soghoian, *supra* note 25. Broadwell's account was registered anonymously, requiring investigators to use "forensic techniques—including a check of what other e-mail accounts had been accessed from the same computer address—to identify who was writing the e-mails." *Id.* When Broadwell logged into other e-mail accounts from the same computer she used to access kelleypatrol, Broadwell created a data trail that agents were able to use to link the accounts. *Id.* The metadata footprints left by the e-mails were used to determine the locations from which they were sent. *Id.*

93. *See id.*

94. *See id.*

95. *See id.*

96. Shane & Savage, *supra* note 24; Gellman, *supra* note 15.

97. 18 U.S.C. § 2703(c)(2) (2012). Under the statute, other information the government can obtain from an ISP with a subpoena includes a subscriber's "name; . . . address; . . . local and long distance telephone connection records, or records of session times and durations; . . . length of service (including start date) and types of service utilized; and . . . means and source of payment for such service (including any credit card or bank account number) . . . ." *Id.*

by a Federal or State statute or a Federal or State grand jury or trial subpoena . . . ."[98] The statute further provides that the "governmental entity receiving the records or information under this subsection is not required to provide notice to a subscriber or customer."[99] To acquire records of the IP addresses and geolocation data associated with a user's account—like the records used to identify Broadwell as kelleypatrol—the SCA requires only that law enforcement obtain an administrative subpoena.[100] But because the FBI has the ability to issue the subpoena, the procedure requires no judicial oversight,[101] which leaves an immense amount of unchecked power in the hands of the FBI.

2. Lack of Protection Offered by Current Regime and Need for Legislative Change

The procedural requirements in the SCA provide little to no protection for users' non-content ISP records, which can contain identifying information. The Broadwell investigation brings to light the need for heightened statutory safeguards for non-content subscriber records: investigators obtained identifying and geolocation information related to users' accounts without any judicial oversight.[102] This power allowed the FBI to cull through private information and identify Broadwell without any mechanism to hold it accountable for its techniques.[103] The search also involved the surveillance of other subscribers who had logged onto the Internet from the same IP address as kelleypatrol.[104] Because the statute does not require the government to notify these users,[105] the users will never know about the surveillance and therefore never be able to claim it was unlawful.[106] Without meaningful judicial oversight (e.g., requiring a judge to review and approve the administrative subpoena seeking the geolocation data at issue in the Broadwell investigation) the government maintains practically unchecked access to non-content ISP records. Unbridled access means a significant loss of control over information

98. *Id.*
99. *Id.* § 2703(c)(3).
100. *See id.* § 2703(c)(2).
101. *See id.*; Soghoian, *supra* note 25.
102. Soghoian, *supra* note 25.
103. *See id.*
104. *See id.*
105. 18 U.S.C. § 2703(c)(3).
106. *See* Soghoian, *supra* note 25.

about oneself, especially in combination with present-day investigative techniques.

To create a check against potential abuse, Congress should address this issue by amending the SCA to require independent review of an administrative subpoena sought by investigators under these circumstances. It should also require timely notice to those surveilled in this manner.[107] Without such notice, the target of the subpoena will likely never learn that the government obtained personally identifiable data.[108]

C. FBI Searches Broadwell and Petraeus's Shared Gmail Account

Once the FBI determined Broadwell's identity, it searched through the content of all the e-mail accounts associated with her name, including the Gmail account she shared with General Petraeus.[109] The content of the saved e-mail drafts in the account revealed the couple's extramarital affair.[110]

1. Legal Standard

Section 2703(c) of the SCA governs law enforcement requests for the content of stored e-mail communications.[111] According to the SCA, a stored communication is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"[112] and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[113] In other words, stored communications include a user's received e-mails, sent emails, and saved e-mail drafts that are stored with an ISP.[114] The statute provides that the government may compel an ISP to disclose the content of e-mail communications in electronic storage for 180 days or less[115] only pursuant to

107. *See id.*; *infra* Part II.C.2.i (responding to concerns regarding giving notice of surveillance in criminal investigations).

108. *See* Soghoian, *supra* note 25 (explaining that targets typically never learn of surveillance unless charges are filed or government officials leak details to the press).

109. *See id.*

110. Lardner, *supra* note 28.

111. *See* 18 U.S.C. § 2703(a)–(b) (2012).

112. 18 U.S.C. § 2510(17)(A) (2012).

113. *Id.* § 2510(17)(B).

114. *See Surveillance Self-Defense Project*, ELEC. FRONTIER FOUND., https://web.archive.org/web/20140818194417/https://ssd.eff.org/3rdparties/protect/email-inbox (accessed through the Internet Archive's Wayback Machine) (snapshot taken on Aug. 18, 2014).

115. 18 U.S.C. § 2703(a).

a court-issued warrant.[116] However, if a communication is in storage for more than 180 days and the government wishes to gain access to the communication, the government can either (1) obtain a warrant or (2) obtain a court order or subpoena and give notice to the user.[117] Though the government must give notice to a user if it obtains a court order or subpoena, the notice may be significantly delayed under certain circumstances.[118] The government's *interpretation* of the SCA does not require law enforcement agents to obtain a warrant to search opened e-mails, sent e-mails, or e-mails saved in the drafts box.[119] According to the government, these types of communications are not considered to be in "electronic storage" as defined by the SCA.[120] Therefore, regardless of the age of the communication, it does not qualify for warrant protection.[121]

Should the government need to obtain a warrant to compel disclosure of a stored communication, however, it must make a showing of "probable cause to search for and seize a person or property or to install and use a tracking device."[122] The probable cause standard requires a magistrate judge to decide if, "given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."[123] Whether the FBI obtained a warrant to gain access to the content of the shared Gmail account in the Broadwell investigation

116. *Id.*

117. *Id.* § 2703(a)–(b).

118. *Id.*; *see also infra* Part II.C.2.i (explaining that notice can be delayed up to ninety days if certain circumstances are present).

119. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 57 (2004) (explaining that Department of Justice manuals indicate that the government groups opened e-mails with those in long-term storage, i.e., older than 180 days, and that according to the SCA, agents need not obtain a warrant to access e-mails in long-term storage); Hanni Fakhoury et al., *When Will Our Email Betray Us? An Email Privacy Primer in Light of the Petraeus Scandal*, ELEC. FRONTIER FOUND. (Nov. 14, 2012), https://www.eff.org/deeplinks/2012/11/when-will-our-email-betray-us-email-privacy-primer-light-petraeus-saga (describing how the government believes the warrant requirement only applies to unopened e-mail and stating that "[t]he DOJ would likely consider draft messages as 'opened' email," as well); *Surveillance Self-Defense Project*, *supra* note 114 ("[U]nder the government's interpretation of the term 'electronic storage', the emails that arrive in your inbox lose warrant protection under the [SCA], and are obtainable with nothing more than a subpoena . . . as soon as you've downloaded, opened or otherwise viewed them. Similarly, the government believes that it can obtain the sent emails and draft emails that you store with your provider with only a subpoena . . . .").

120. *Surveillance Self-Defense Project*, *supra* note 114.

121. *See id. But cf.* 18 U.S.C. § 2703(a) (2012) (detailing how a warrant is necessary to obtain an e-mail communication that is in electronic storage *and* less than180 days old).

122. FED. R. CRIM. P. 41(d)(1) (2013).

123. Illinois v. Gates, 462 U.S. 213, 238 (1983).

remains unclear.[124] However, if the government did acquire a warrant, it has not been transparent about the factual predicate justifying the search.

2. Lack of Protection Offered by Current Regime and Need for Legislative Change

The government's surveillance of Broadwell and Petraeus's shared Gmail account demonstrates a significant lack of procedural safeguards. In addition to requiring a warrant for access to stored e-mail content, procedural safeguards can ensure government accountability and transparency in the surveillance of stored e-mail content. In particular, four inadequacies in the current law call attention to the need for enhanced procedural safeguards for the surveillance of stored e-mail content: (1) lack of notice to the target; (2) no minimization of non-incriminating e-mail content searched; (3) no particularity requirement in the warrant application; and (4) the sealing of the court record and docket. Each inadequacy will be addressed in turn.

i. Notice

The SCA explicitly provides that the target of a search need not be notified if the government obtains a warrant to compel the content of stored e-mail communications older than 180 days.[125] Lack of notice raises significant privacy concerns. Notice provides a target with

124. *See* E-mail from Susan Freiwald, Professor, University of San Francisco School of Law (Mar. 7, 2013, 1:14 PM EST) (on file with author) (explaining that Chris Soghoian, Principal Technologist and Senior Policy Analyst, ACLU Speech, Privacy and Technology Project, contacted the District Court handling the investigation to inquire whether the government had obtained a warrant and was told that the files were sealed); *compare* Evan Perez, Siobhan Gorman & Devlin Barrett, *FBI Scrutinized on Petraeus*, WALL ST. J. (Nov. 12, 2012), http://online.wsj.com/article/SB10001424127887324073504578113460852395852.html ("[The agents] used metadata footprints left by the emails to determine what locations they were sent from. They matched the places, including hotels, where Ms. Broadwell was during the times the emails were sent. FBI agents and federal prosecutors used the information as probable cause to seek a warrant to monitor Ms. Broadwell's email accounts."), *with* Rick Rothacker & David Ingram, *Identity of Second Woman Emerges in Petraeus' Downfall*, REUTERS (Nov. 12, 2012), http://www.reuters.com/article/2012/11/12/us-usa-petraeus-idUSBRE8A81FP20121112 ("[A] U.S. government official said the FBI investigation into the emails was fairly straightforward and did not require obtaining court orders to monitor the email accounts of those involved, including the personal email account of Petraeus."), *and* Fakhoury et al., *supra* note 119 (speculating that Google required the government obtain a warrant to compel disclosure of the stored e-mail content).

125. 18 U.S.C. § 2703(a)–(b) (2012); *see also* Freiwald, *supra* note 119 (explaining that because the government groups opened e-mails with e-mails in long-term storage (older than 180 days), the opened e-mails are subject to the same lack of notice provision);

knowledge of the surveillance and consequently allows her to defend her rights.[126] Assume the government obtained a warrant based on probable cause to search the content of the drafts in Broadwell and Petraeus's shared Gmail account; current law would not have required investigators to notify Broadwell of such surveillance. If the government opted to use a court order or subpoena to gain access to the content, the SCA would have required that the government give notice of the surveillance.[127] According to the statute, however, such notice can be delayed for up to ninety days if certain circumstances are present.[128] To delay notice, the law requires the government to show that it has reason to believe that notice would create an adverse result that would interrupt the ongoing criminal investigation.[129] An adverse result can be "endangering the life or physical safety of an individual; . . . flight from prosecution; . . . destruction of or tampering with evidence; . . . intimidation of potential witnesses; or . . . otherwise seriously jeopardizing an investigation or unduly delaying a trial."[130]

The government commenced its investigation into Broadwell in June 2012, but assume it did not notify Broadwell of the surveillance at that time, obtained a ninety-day extension, and interviewed Broadwell in September 2012.[131] If this September interview served as Broadwell's first notice of the electronic surveillance on her e-mail accounts, it occurred more than ninety days after the government obtained a warrant, court order, or subpoena.[132] At this point, it was too late for her to challenge any unlawful search of her private content before it happened.[133] This instance reflects two deficiencies in the

Fakhoury et al., *supra* note 119 (explaining that the government likely considers draft messages to be opened e-mail).

126. Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261, 1299 (2013).

127. 18 U.S.C. § 2703(a)–(b).

128. 18 U.S.C. §§ 2703(b)(2)(B), 2705 (2012).

129. 18 U.S.C. § 2705.

130. 18 U.S.C. § 2795(a)(2) (2012).

131. Fakhoury et al., *supra* note 119.

132. Because of conflicting reports regarding the date of the initiation of the investigation into Broadwell and the date of her first interview, this assumption illustrates the functionality of the delayed notice section in the SCA and how, practically, most targets do not learn of electronic surveillance of their e-mail content. *Compare id.*, *with Timeline of the Petraeus Affair*, CNN POLITICS (Nov. 15, 2012), http://www.cnn.com/2012/11/12/politics/petraeus-timeline/.

133. Additionally, while the government eventually notified Broadwell and Petraeus of the search conducted on their shared Gmail account, many innocent citizens never learn of electronic surveillance of their e-mail content. *See* Stephen W. Smith, *Gagged, Sealed & Delivered*, 6 HARV. L. POL'Y REV. 313, 315 (2012); Susan Freiwald, *First Principles of Communications Privacy*, STANFORD TECH. L. REV. 3, ¶¶ 62–63 (2007).

SCA's current notice provision. First, if the government used a court order or subpoena to search the Gmail account and got the ninety-day extension, it is clear that law enforcement would not be held accountable for failing to give notice as soon as the extension expired. Second, none of the enumerated "adverse results" were present to justify delaying notice to Broadwell. In a criminal investigation of a member of the military who allegedly sent harassing e-mails, timely notice would not have risked the intimidation or death of a witness, flight of prosecution, or destruction of evidence.[134] Again, because the practical effect of electronic surveillance in the stored communications context involves government access to communications before the user receives notice of such access, there is no risk of the user destroying the evidence.[135]

Admittedly, at least "some measure of temporary secrecy for electronic surveillance orders during a criminal investigation is both reasonable and necessary,"[136] but SCA surveillance orders consistently remain undetected by the target until long after the close of the investigation.[137] To date, only Jill Kelley has asserted that the government unlawfully searched her e-mail,[138] but Broadwell's case demonstrates the difficulty a target may face in defending his or her Fourth Amendment rights against potentially unlawful electronic surveillance during a criminal investigation. Currently, surveillance of most stored e-mail content requires, at most, significantly delayed notice to the target.

In order to properly protect people's rights, Congress should include a blanket, non-delayed notice provision in the SCA. While still accommodating law enforcement's needs, Congresswoman Zoe Lofgren[139] has set forth an effective proposal.[140] She suggests notice be

134. Assuming investigators were concerned that Broadwell was privy to confidential information from Petraeus, they had already obtained her communications from ISPs; also, Broadwell willingly allowed the government to search her home and computer files during the investigation. *See* Wootson, Kelley & Arriero, *supra* note 36.

135. 18 U.S.C. § 2703(a)–(b) (2012).

136. Smith, *supra* note 133, at 315 ("Premature disclosure to the target or the general public could jeopardize the integrity of the ongoing investigation and encourage the target to flee or destroy evidence.").

137. *Id.* ("[Because surveillance orders remain sealed almost indefinitely], unless the investigation results in criminal charges, targets who are law-abiding citizens will never learn that the government has accessed their emails, text messages, twitter accounts, or cell phone records."); United States. v. Warshak, 631 F.3d 266, 284 (2010) (explaining that police got one ninety-day delay of notice extension, but Warshak did not get notice of e-mail surveillance until a year after it occurred).

138. Kelley, *supra* note 6.

139. *Biography of Congresswoman Zoe Lofgren California, 19th District*, CONGRESSWOMAN ZOE LOFGREN, http://www.lofgren.house.gov/biography/ (last visited Nov. 13, 2014).

given by serving targets with a copy of the warrant within three days after law enforcement has accessed the content.[141] However, this change would be subject to the existing notice delays in the statute.[142] To strike a more equitable balance between law enforcement needs and privacy interests, extension request applications should be particularized and set forth a specific time period for delay of notice, which law enforcement must strictly follow.[143]

ii. Minimization

The Wiretap Act,[144] which governs wiretaps and bugs, requires that investigators using these techniques "minimize the interception of communications not otherwise subject to interception."[145] Practically, this statutory language requires investigators to conduct the investigation in a manner that minimizes the surveillance of non-incriminating information.[146] For instance, in the traditional wiretap context, investigators must terminate the tap as soon as the surveilled conversation turns to a non-incriminating subject.[147] The statutory language ensures that investigators are held accountable to a judge for conducting their investigation in this manner.[148] The SCA does not have similar language to require such minimization in the surveillance of stored electronic communications. However, according to the Honorable James G. Garr, incorporating a minimization requirement would fulfill "the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized."[149] As in the traditional wiretap context, minimization in the stored communications context would include judicial oversight of the minimization efforts and ensure that investigators are held accountable for conducting their investigations in a manner that limits the surveillance of non-incriminating informa-

140. H.R. 983, 113th Cong. (2013), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-113hr983ih/pdf/BILLS-113hr983ih.pdf; 18 U.S.C. § 2705(a)(2) (2012).

141. H.R. 983.

142. *Id.*

143. Smith, *supra* note 133, at 332.

144. 18 U.S.C. §§ 2510–2522 (2012).

145. 18 U.S.C. § 2518(5).

146. *Urge Congress to Stop the FBI's Use of Privacy-Invading Software,* ACLU, https://www.aclu.org/urge-congress-stop-fbis-use-privacy-invading-software (last visited Nov. 13, 2014).

147. Jeff Strange, *A Primer on Wiretaps, Pen Registers, and Trap and Trace Devices*, Tex. Dist. & Cnty. Attorneys Ass'n (Sept. 24, 2009), http://www.tdcaa.com/node/4813.

148. 18 U.S.C. § 2518(5)–(6).

149. James G. Carr, The Law of Electronic Surveillance § 5.7(a), at 5–28 (1994).

tion. For instance, a judge's order authorizing surveillance of stored communications could require investigators to report to the judge the progress made toward the authorized objective and the need for continued surveillance.[150]

In theory, the interception of communications in transit, such as a real time phone conversation, can be distinguished from the surveillance of stored e-mail communications.[151] "[O]fficers cannot know in advance, which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of communications in order to make such a determination."[152] Thus, "[i]nterception . . . poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting."[153] In contrast, such risk can be controlled during the surveillance of stored electronic communications. Investigators may use keyword searches to locate relevant communications "without the necessity of reviewing the entire contents of all of the stored communications."[154]

However, the Broadwell investigation demonstrates the insufficiency of relying on law enforcement to minimize the surveillance of non-incriminating content without independent oversight or external regulations. As a result of the FBI's investigation to identify Broadwell as the sender of harassing e-mails to Jill Kelley, investigators searched and disclosed to the public e-mail conversations of three additional, unrelated individuals.[155] FBI Agent Fred Humphries, General John Allen, and General David Petraeus suffered significant repercussions stemming from the government's surveillance of the stored e-mail content during its investigation of Paula Broadwell.[156] The government could have used keyword searches to locate relevant communications and narrow its search, but the e-mails disclosed to the public with subject matter unrelated to protecting classified information[157] illustrate that the government either (1) did not use keyword searches or (2) used keyword searches and failed to sufficiently self-govern the

150. 18 U.S.C. § 2518(6).
151. Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994).
152. *Id.*
153. *Id.*
154. *Id.*
155. *See supra* Parts I.A.–B.
156. *Id.*
157. *See, e.g.*, Carter, *supra* note 20. For example, the content of the e-mail sent to Jill Kelley from FBI Agent Fred Humphries was clearly unrelated to the investigation into Broadwell. The content of the e-mail included a picture of Humphries posed between a pair of target dummies captioned "Which One's Fred?" *Id.*

results of those searches. A statutory minimization requirement would *explicitly require* the government to conduct the surveillance using methods to minimize the interception of communications irrelevant to the authorized objective,[158] such as keyword searching, and also incorporate a judicial oversight mechanism to ensure adequate protection of private information. Investigators would be held accountable to this standard by an independent judge, who could require reports during the investigation showing progress made toward the authorized objective and the need for continued surveillance.[159]

Congress rationalizes the minimization requirement in the wiretap context through the indiscriminate nature of the surveillance.[160] However, the surveillance of stored e-mail content, while not intercepted in real time like wiretap surveillance, proves to be just as indiscriminate. Where e-mails can contain a bevy of information unrelated to the criminal investigation, surveillance of a target's conversations inevitably results in the surveillance of innocent people and activities unrelated to the investigation's purpose.[161] Additionally, when the government's initial "routine step" in an investigation involves searching all the e-mails in an account,[162] information unrelated to the investigation will inevitably be disclosed.

Like the Wiretap Act, the SCA should incorporate a minimization requirement to protect against the risk of the government gaining access to non-incriminating stored electronic communications. Congress should require that surveillance of stored e-mail content be conducted in a manner that minimizes the surveillance of communications unrelated to the target and subject matter of the authorized

158. 18 U.S.C. § 2518(5) (2012).

159. 18 U.S.C. § 2518(6).

160. 18 U.S.C. § 2518; *see also* Freiwald, *supra* note 119, ¶ 67 (explaining how indiscriminate investigations implicate the core concerns of the Fourth Amendment) ("If law enforcement agents must intrude upon private activities to perform their jobs, the harm from intrusion is minimized to the extent the investigation reaches no further than necessary to uncover incriminating evidence.").

161. *See* Freiwald, *supra* note 119, ¶¶ 66, 68 ("Stored e-mails contain a vast archive of people's past activities. . . . Because of the extra richness of e-mails as compared to telephone conversations, there is every reason to believe that e-mail surveillance will be just as indiscriminate . . . In the *Warshak* case, the plaintiff claims that government agents acquired thousands of his personal e-mails, 'without particularization or limitation as to time frame, parties to the communication, or the subject matter of the communication.' Surveillance that may acquire information unrelated to the search justification requires judicial intervention to ensure that acquisition of non-incriminating communications is minimized.").

162. Schmitt & Bumiller, *supra* note 6.

objective of the original investigation.[163] For example, investigators would be statutorily required to use methods such as keyword searching and immediately terminate searching an email once they determine it is unrelated to the subject matter of the investigation, even if that means only through reading the title. The surveillance should also be required to terminate upon attainment of the authorized objective.[164] Additionally, Congress should demand annual reports disclosing the percentage of surveilled stored e-mail conversations that end up being incriminating.[165] Such reports should be published annually to allow the public to understand the electronic surveillance undertaken by the government and ensure that the government does not abuse its power.[166] This mechanism will correct for the indiscriminate nature of stored communication surveillance.[167]

iii. Particularity

Currently, the government's application for a warrant under the SCA does not require any showing of particularity.[168] The SCA requires that the government obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ,"[169] which in turn requires that the warrant "identify the person or property to be searched [or] identify any person or property to be

163. For instance, if the government is authorized to search e-mail exchanges in Jill Kelley's e-mail account and the authorized objective of the surveillance is to identify Broadwell as the sender of harassing e-mails to Jill Kelley, the subject matter of the e-mail content searched by investigators should not exceed those bounds.

164. *See, e.g.*, 18 U.S.C. § 2518(5) (2012) (providing a minimization requirement for the interception of live wire, oral, or electronic communications).

165. *See, e.g.*, 18 U.S.C. § 2519(2) (2012) (requiring that prosecutors and judges provide information for an annual report on wiretapping); ADMIN. OFFICE OF THE U.S. COURTS, WIRETAP REPORT (2012), *available at* http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx#saz; CHRISTOPHER SOGHOIAN, THE LAW ENFORCEMENT SURVEILLANCE REPORTING GAP 6 (2011), http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf ("The reports are extremely detailed, and for each wiretap, reveals the city or county, the kind of interception . . . the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, as well as the financial cost of the wiretap. . . . [However], there are no official statistics regarding law enforcement acquisition of stored communications data.").

166. *See, e.g.*, SOGHOIAN, *supra* note 165, at 6 ("The Administrative Office of the Courts has published reports for the years 1997 to the present. By comparing these reports, several interesting trends can be seen regarding the use of [ ] [wiretap] surveillance power by federal and state law enforcement agencies." (citation omitted)).

167. Freiwald, *supra* note 133, ¶ 67.

168. 18 U.S.C. § 2703 (2012).

169. 18 U.S.C. §2703(a).

seized . . . ."[170] A particularity requirement would require the government to give a detailed request for the surveillance of stored e-mail content. For instance, a warrant application in the Broadwell case would have required the government to identify a particularized time frame, specify a target or targeted individuals, and indicate the subject matter of the communication sought. Consequently, such a specific warrant would have limited the search within those boundaries. Because e-mail content contains a wealth of personal information,[171] the particularity requirement would have meaningfully narrowed the scope of the warrant application and protected unrelated private information from surveillance. Under current law, the SCA would not have required a warrant application in the Broadwell investigation to be particularized. If a warrant was issued in the Broadwell investigation, the SCA would have only obligated the government to establish probable cause[172] and *broadly* state a desire to conduct electronic surveillance of Broadwell's e-mails.[173] Thus, if a warrant was in fact secured in this case, the lack of particularization with respect to time frame and subject matter would have allowed investigators to search e-mails unrelated to the investigation[174]—as was ultimately the result.

The SCA must require the government to explain with particularity the information sought in its surveillance of stored e-mail content. Congress should amend the statute to require law enforcement to specify the target, parties to the communication, subject matter, and particular time frame within which the e-mails were sent, received, or initially drafted. Such particularity mechanisms will narrow the scope of the warrant, allowing investigators to search e-mail content while protecting unrelated people and content from electronic surveillance.

170. FED. R. CRIM. P. 41(e)(2)(A).

171. Freiwald, *supra* note 133, ¶ 66 ("A simple e-mail message has textual header information that discloses the time it was composed, its subject line plus any attachments, and the electronic addresses of the sender, the recipient, and any who receive courtesy copies of it. E-mails often include prior messages in their text, and analysis may reveal the computer on which the e-mail was composed, its path through the network, and the times the e-mail was opened, deleted, or forwarded. Moreover, people reveal in their e-mails more about their political opinions, religious beliefs, personal relationships, intellectual interests, and artistic endeavors than they ever revealed over the telephone.").

172. FED. R. CRIM. P. 41(d).

173. Fakhoury et al., *supra* note 119 (noting that warrants are often "quite broad," and the government may well have obtained e-mails from all of Broadwell's accounts under a single warrant).

174. For example, they could have reviewed unrelated e-mail content, like the drafts between Broadwell and Petraeus that revealed their extramarital affair. *See* Soghoian, *supra* note 25; Lardner, *supra* note 28; Fakhoury et al., *supra* note 119 ("As a result [of the broad warrant], there's no telling how much email the FBI actually read.").

iv. Sealing Court Records

Courts presently keep the majority of electronic surveillance orders and related court orders permanently sealed.[175] While the SCA does not contain a provision for automatically sealing court records,[176] the government often groups these orders with other electronic surveillance orders (e.g., orders for wiretaps, pen registers, and trap and trace devices) that require automatic sealing.[177] Combining the orders results in an automatic seal for all of the electronic surveillance involved.[178] This practice prevents the public from scrutinizing what judges permit the government to review.[179] Unsealing electronic surveillance court records would equip targets with knowledge to protect their rights, and such procedural transparency would help hold the government accountable for its investigation methods.[180]

The Broadwell investigation provides a prime example of how a lack of procedural transparency prevents the public from holding the government accountable for its electronic surveillance methods. As stated, the court sealed its records in the investigation, and it remains unknown whether investigators obtained a warrant to search Broadwell's e-mails.[181] Even if the government did obtain a warrant, sealing court records prevents the public from knowing the warrant's factual predicate. Disclosing the warrant's factual predicate would allow the public to evaluate, scrutinize, and challenge the application of the law

175. Smith, *supra* note 133, at 321. Smith, a Magistrate Judge in the Southern District of Texas, estimated that in 2006, magistrate judges issued more than 30,000 sealed electronic surveillance orders. *Id.* "To put this figure in context, magistrate judges in one year generated a volume of secret electronic surveillance cases more than thirty times the annual number of FISA cases; in fact, this volume of ECPA cases is greater than the combined yearly total of all antitrust, employment discrimination, environmental, copyright, patent, trademark, and securities cases filed in federal court." *Id.* at 322.

176. 18 U.S.C. §§ 2701–2712 (2012).

177. Smith, *supra* note 133, at 325.

178. *See id.* ("[T]he secrecy provisions of the SCA are less stringent than other forms of ECPA surveillance such as wiretaps or pen registers. The default rule is that a 2703(d) order will not be sealed, nor will it be accompanied by a gag order absent a showing of one of the special circumstances listed in 2705(b). However, in many districts the government routinely avoids these weaker SCA secrecy provisions by the simple expedient of combining its request for a 2703(d) order and a pen/trap order into a single application and order. The combined order is then automatically sealed and gagged by the authority of the Pen/Trap Statute. Although [the statutes governing wiretap, pen and trap devices, and stored communications] do not contemplate such combined orders, no published court opinion has challenged the practice.").

179. *Id.* at 333.

180. *Id.* at 335–36.

181. *See* E-mail from Susan Freiwald, *supra* note 124.

governing surveillance of stored e-mail content.[182] Without open records, no meaningful discourse can take place regarding the procedures governing such electronic surveillance.

To achieve sufficient procedural transparency in criminal investigations and hold law enforcement accountable to the public, Congress must require courts to open records to public scrutiny.[183] The SCA should require judges to separately scrutinize and issue orders involving surveillance of stored communications to close the loophole that allows SCA orders to take advantage of the Wiretap Act and Pen/Trap Statute automatic sealing provisions.[184] Congress should then incorporate a provision in the Wiretap Act (as amended by ECPA), Pen/Trap Statute, and SCA requiring that court orders and records *not* be sealed unless the public nature of the court records poses a threat to law enforcement's legitimate ability to conduct an effective investigation. When that is the case, the government may request that the court issue a sealing order if it explains in detail the necessity for sealing the records and why more narrow alternatives or redaction cannot solve the problem. Also, courts should set a time limit for lifting the seal when the justification ceases to exist.[185]

3. Effective United States Law

While the current legal regime does not offer sufficient procedural safeguards, the Broadwell investigation reveals that ISPs may provide an effective check on the government. ISPs generally require the government to obtain and present a warrant to acquire stored e-mail content.[186] In fact, many speculate that Google itself, rather than the law, forced the government to obtain a warrant to gain access to

182. Smith, *supra* note 133, at 333 ("The public has no way to evaluate, much less have confidence in, sealed court orders. From the standpoint of the ordinary citizen, electronic surveillance is among the most intrusive governmental activities a court can authorize, yet it is also the most likely to be hidden from public view.").

183. *Id.*

184. *Id.* ("Congress should amend ECPA to eliminate automatic sealing for electronic surveillance applications, orders, and docket sheets. This is already the law regarding docket sheets in general.").

185. *See id.*

186. Fakhoury et al., *supra* note 119; *Who Has Your Back?*, ELEC. FRONTIER FOUND., https://www.eff.org/who-has-your-back-2014 (last visited Aug. 19, 2014). Google, as well as Adobe, Amazon, Apple, Dropbox, Facebook, Foursquare, Internet Archive, LinkedIn, Lookout, Microsoft, MySpace, Pinterest, Sonic.net, Spideroak, Tumblr, Twitter, Verizon, Wicker, Wikimedia Foundation, Wordpress, and Yahoo!, require a warrant for stored content. *Who Has Your Back?*, *supra*. The Electronic Frontier Foundation charts companies that protect user data from the government and the extent of such protections. *See id.*

Broadwell's Gmail account.[187] When ISPs push back on the government, the protection of e-mail content dramatically increases.[188]

ISPs are currently performing a role traditionally played by the legal regime to protect Fourth Amendment rights. While citizens should appreciate ISPs' efforts to check the government's surveillance power, they cannot depend on them for a long-term, comprehensive, and permanent solution.[189] Some companies still do not require a warrant for user content,[190] and Google's policy, for instance, could be transitory.[191] The company's legal team has voiced privacy con-

187. David Drummond, *Google's Approach to Government Requests for User Data*, GOOGLE: OFFICIAL BLOG (Jan. 27, 2013), http://googleblog.blogspot.com/2013/01/googles-approach-to-government-requests.html. Google's Chief Legal Officer David Drummond officially announced the leading ISP's company policy in early 2012: "We require that government agencies conducting criminal investigations use a search warrant to compel us to provide a user's search query information and private content stored in a Google Account—such as Gmail messages, documents, photos and YouTube videos. We believe a warrant is required by the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure and overrides conflicting provisions in ECPA." *Id.*; *see also* Fakhoury et al., *supra* note 119.

188. *See* Drummond, *supra* note 187; Fakhoury et al., *supra* note 119. Additionally, Richard Salgado, Google's Director for Information Security and Law Enforcement, is actively pursuing changes to the current statutory requirements covering stored e-mail content. Salgado maintains that the "inconsistent, confusing and uncertain standards" surrounding the electronic surveillance of stored email communications "reveal how ECPA fails to preserve the reasonable privacy expectations of Americans today." Written Testimony of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc., House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on "ECPA and the Cloud" 3 (Sept. 23, 2010), *available at* http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/google_testimony_rick_salgado.pdf; *see also Who Has Your Back?*, *supra* note 186 (stating that, in addition to Google, companies such as Apple, Credo Mobile, Dropbox, Facebook, Internet Archive, LinkedIn, Microsoft, Pinterest, Sonic.net, Spideroak, Tumblr, Twitter, Verizon, Wicker, Wikimedia Foundation, Wordpress, and Yahoo!, "fight for their users' privacy interests in Congress").

189. *See* Fakhoury et al., *supra* note 119 ("In EFF's experience, the government will seek a warrant rather than litigate the issue.").

190. *Who Has Your Back?*, *supra* note 186. Some influential companies, such as AT&T, Comcast, and Snapchat, do not require a warrant for user content. *Id.*

191. As Director of Google's Law Enforcement and Information Security team, Richard Salgado leads the effort on the ISP's protection of user information. If Salgado were to leave Google, his transparency philosophy and policy could arguably leave with him. Drummond, *supra* note 187; Written Testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google, Inc., House Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations, Hearing on "ECPA Part I: Lawful Access to Stored Content" (Mar. 19, 2013), *available at* http://judiciary.house.gov/_files/hearings/113th/03192013_2/Salgado%2003192013.pdf ("I oversee the company's response to government requests for user information . . . .").

cerns[192] while Richard Salgado[193] heads up the Information Security and Law Enforcement team, but the future of stored e-mail protection requires statutory safeguards, which provide relatively permanent, clear, and specific guidelines that will outlast any one senior counsel and will apply across all companies, not just Google.

Conclusion

The Broadwell investigation highlights the lack of procedural safeguards afforded by current statutes and effective law for stored e-mail content during a criminal investigation. The fallout of such surveillance can be dire, even for those who are not the target of the investigation. The current regime does not sufficiently protect the privacy interests at stake, as illustrated by the disproportionate consequences suffered by the people involved in the Petraeus scandal. Congress must update the SCA to: (1) provide notice to the target; (2) include a minimization requirement protecting non-incriminating e-mail content; (3) offer a particularity requirement in the government's warrant application; and (4) unseal court records pertaining to stored email communications. Through these enhanced procedural safeguards, Congress can strike the desired balance between law enforcement's need to exercise legitimate electronic surveillance and citizens' privacy and autonomy interests in stored e-mail content.

192. *See* Drummond, *supra* note 187; Written Testimony of Richard Salgado, *supra* note 188; Written Testimony of Richard Salgado, *supra* note 190.

193. Biography of Richard Salgado, CTR. FOR INTERNET AND SOC'Y, http://cyberlaw.stanford.edu/about/people/richard-salgado (last visited Aug. 19, 2014).