THE YALE LAW JOURNAL FORUM
JULY 27, 2016

Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt

Cindy Cohn

Robert Litt, General Counsel of the Office of the Director of National Intelligence, has offered a new analysis for the Fourth Amendment in the Information Age, grounded in two cases arising from the NSA's domestic surveillance programs.[1] As opposing counsel or amicus in the cases he cites in his argument, I thought it would be useful to respond.

The first case Mr. Litt discusses is *Jewel v. National Security Agency*, in which I am counsel for the plaintiffs.[2] *Jewel* arises, in part, out of the NSA's collection and search of the content of communications from fiber optic cables that form the Internet's backbone. Mr. Litt claims that Congress formally authorized this program,[3] which the government calls UPSTREAM, by passing Section 702 of the FISA Amendments Act in 2008—a contention with which I strongly disagree.[4]

The second case is *Klayman v. Obama*, where I argued on behalf of the *amici* in support of the plaintiffs in the D.C. Circuit.[5] *Klayman* arises from the NSA's mass telephone records collection conducted until late 2015 under Section 215 of the USA PATRIOT Act.[6] Telephone records collection is also at issue in three cases where my organization, the Electronic Frontier Foundation

1. Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J. F. 8 (2016), http://www.yalelawjournal.org/forum/fourth-amendment-information-age [http://perma.cc/4PSQ-QE9P].
2. Jewel v. Nat'l Sec. Agency, No. C 08-04373 JSW, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015).
3. Litt, *supra* note 1, at 12.
4. 50 U.S.C. § 1881(a)(2012).
5. Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015).
6. 50 U.S.C. § 1861 (2012).

("EFF"), represents the plaintiffs: *Jewel*,[7] *First Unitarian Church of Los Angeles v. NSA*[8] and *Smith v. Obama*.[9]

Like Mr. Litt, I am not a legal academic but, like him, I have the practical experience of having handled numerous lawsuits involving the Fourth Amendment and national security, in my case for over 20 years. Also like Mr. Litt, I do not propose a comprehensive theory of the Fourth Amendment. Instead, this Essay responds to his suggestions and points to what I submit is a better starting point—the International Principles on the Application of Human Rights to Communications Surveillance, also known as the Necessary and Proportionate Principles[10]—for considering the problems he raises with Fourth Amendment doctrine.

Mr. Litt makes two initial statements with which I agree. First, he notes that the "reasonable expectation of privacy" test currently employed in Fourth Amendment jurisprudence is a poor test for the digital age. Second, he states that the "third-party doctrine"—under which an individual who voluntarily provides information to a third party loses any reasonable expectation of privacy in that information—should not be an on-off switch for the Fourth Amendment. On this second point, Mr. Litt wisely recognizes that some members of the Supreme Court are uneasy with the third-party doctrine.[11] His misgivings about the third-party doctrine are most welcome; many in the government, including the Department of Justice in *Klayman*, continue to claim that all constitutional protection shuts off whenever data is entrusted to a service provider.

From there, however, our paths diverge quite sharply.

Mr. Litt argues that since the "reasonable expectation of privacy" formulation is not well suited to digital surveillance, it should simply be eliminated. This would leave a "reasonableness" balancing test to carry the entire weight of the Fourth Amendment's protection against governmental intrusions. He says that a court in each case should balance the "actual harm" suffered by the individual affected by the surveillance with the governmental

---

7. *Jewel* contains claims based on telephone records collection as well as collection from the Internet backbone.

8. Complaint, First Unitarian Church of L.A. v. Nat'l Sec. Agency, Civ. No. 13-3287. (N.D. Cal. July 16, 2013).

9. Smith v. Obama, 816 F.3d 1239 (9th Cir. 2016).

10. *Necessary & Proportionate*, NECESSARY & PROPORTIONATE COALITION (May 2014), http://necessaryandproportionate.org/principles [http://perma.cc/L4NU-4KMM]. A list of privacy organizations that cooperatively drafted the Principles can be found here: http://necessaryandproportionate.org/about [http://perma.cc/H3EF-8TBN].

11. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

interests in conducting the surveillance.[12] This argument throws the baby out with the bathwater. By abandoning the "reasonable expectation of privacy" standard without a suitable replacement, Mr. Litt also implicitly suggests abandoning the foundational constitutional protection against general warrants,[13] as well as the rule that a warrantless search of someone with a reasonable expectation of privacy is *per se* unconstitutional unless an exception applies.[14]

Eliminating the *per se* rule and the prohibition on general warrants would also help the government evade one of the strongest arguments against UPSTREAM surveillance in *Jewel v. NSA*. There, the government has admitted that it conducts warrantless full-content searches of a large number of nonsuspect Americans' communications that travel over the Internet backbone—contrary to Mr. Litt's contentions that such factual assertions are purely hypothetical.[15] The government calls this "about" searching, since it searches the content of communications for messages that are "about" targets, in addition to the searching it does for messages to or from the targets themselves.[16] There are FISA court orders signing off on this activity at a very high programmatic level.[17] But these orders do not address the suspicionless collection and search of Americans' international communications, nor the large "incidental" collection and search of Americans' fully domestic communications without any probable cause.

Under current doctrine, since Americans have a reasonable expectation of privacy in the content of their communications, full-content searching is *per se* unconstitutional unless an exception to the warrant requirement applies. None does. In order to prevail, therefore, the government must convince the Supreme Court to read a broad national security "special needs" exception into the Fourth Amendment authorizing mass, suspicionless seizure and full-content searches of millions of nonsuspect Americans' most private international and domestic communications. That is a tall order: the Court

12. Litt, *supra* note 1, at 14.

13. Stanford v. Texas, 379 U.S. 476 (1965) (holding that a warrant ordering officers to search for books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings, and other written instruments concerning the state Communist Party was a general warrant and therefore violated the constitutional requirement that warrants particularly describe things to be seized).

14. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

15. Litt, *supra* note 1, at 13.

16. *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 84-86, PRIVACY & C.L. OVERSIGHT BOARD (Jul. 2014), http://www.pclob.gov/library/702-Report.pdf [http://perma.cc/WU4C-UW28].

17. *See, e.g.*, *In Re* DNI/AG Certification, No. 702(i)-08-01, at *18 (U.S. FISC Sept. 4, 2008), http://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf [http://perma.cc/8HV4-C9NR].

would effectively have to create an implied national security exception to the Fourth Amendment that would admittedly affect billions of communications by millions of innocent Americans.

Such a large implied exception does not readily align with history: the Fourth Amendment contains no national security exception, even though it was adopted in the shadow of the Revolutionary War. Further, the Fourth Amendment was expressly intended to prevent general warrants.[18] The FISA Court of Review—where the government alone presents its case and the arguments and decisions are kept secret—has recognized some form of a national security exception.[19] But the government may not wish to see the Supreme Court, whose proceedings are adversarial and highly public, consider whether to create such a large and unprecedented exception.

Moreover, Mr. Litt's balancing test is unbalanced at its inception. According to his argument, courts can only evaluate the "actual harm" to a single person from mass surveillance because his reformulation retains the caselaw holding that Fourth Amendment rights are personal and cannot be asserted vicariously.[20] Meanwhile, Mr. Litt's formulation would allow the government to present its interest broadly without also showing "actual" increased safety of Americans as a result of the surveillance, much less the individual safety of the plaintiff. Indeed, Mr. Litt likens the increased safety to an insurance policy, which protects its holder even when no claim is ever filed.[21]

In practice, the government almost always claims that details of the "actual" surveillance of a person, or even whether a person's communications are included in the surveillance, are protected by the state-secrets privilege, making it even more difficult for the individual to show particularized harm. As a result, it is difficult to imagine a situation where the government would not prevail under Mr. Litt's framing.

More importantly, Mr. Litt's central claim is that there can be no actual harm when a person's communications are seized by the government and searched, even with content searching, as long as computers but not humans conduct the search. He says that communications are "unseen and unknown" until they turn up in search results that are shown to a human, adding that

18. Stanford, 379 U.S. at 481 (noting that the Fourth Amendment "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant").

19. *See In re* Directives, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008).

20. This argument relies upon the post-*Katz* ruling in *Rakas v. Illinois*, 439 U.S. 128, 133 (1978).

21. Litt, *supra* note 1, at 16.

only an "infinitesimal fraction" of the communications is ever seen by a human.[22]

This argument—what I call the "human-eyes" theory of the Fourth Amendment—is where we most seriously disagree. Mr. Litt's "human-eyes" theory would effectively authorize a surveillance state in which a person's every action and interaction could be technologically monitored and algorithmically analyzed without violating the Fourth Amendment, as long as a human only saw "suspicious" information selected by the technology.

There are four key problems with the "human-eyes" theory.[23]

First, Mr. Litt dismisses concerns about mass surveillance and its chilling effects as "overheated rhetoric."[24] Yet recent research confirms what we intuitively know to be true: the specter of mass government surveillance is enough to chill *completely legal* activities online if individuals feel that they might draw governmental attention.[25] The very existence of mass surveillance programs constricts individual liberty and democratic activity, regardless of whether a person is ultimately targeted. This concern is reflected in the First Amendment right of association as well as the Fourth Amendment's prohibition on unreasonable searches and seizures. In the landmark domestic surveillance case, *United States v. U.S. District Court (Keith)*, the Supreme Court recognized the risk, noting that in national security cases, there is often a "convergence of First and Fourth Amendment values not present in cases of 'ordinary crime.'"[26] Because of this convergence, *Jewel* and *First Unitarian Church of Los Angeles v. NSA* both raise First and Fourth Amendment issues.[27] The latter case contains evidence from a number of advocacy organizations such as Greenpeace, the National Lawyers Guild, and Second Amendment

22. *Id.* at 14.

23. Other commentators have also rejected this theory. *See, e.g.*, Kevin S. Bankston & Amie Stepanovich, *When Robot Eyes Are Watching You: The Law & Policy Of Automated Communications Surveillance*, 35-37 (U. of Miami Sch. of L. Working Paper), http://robots.law.miami.edu/2014/wp-content/uploads/2014/07/Bankston_Stepanovich_We_Robot.pdf [http://perma.cc/V5CK-MB4B].

24. Litt, *supra* note 1, at 14.

25. Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, BERKELEY TECH. L.J. (forthcoming 2016), http://ssrn.com/abstract=2769645 [http://perma.cc/RQR8-4QXB]; Lee Rainie & Mary Madden, *Americans Privacy Strategies Post-Snowden*, PEW RES. STUD. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden [http://perma.cc/8NXF-84HJ]; Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 293 (June 2016), http://jmq.sagepub.com/content/93/2/296.full.pdf [http://perma.cc/QB7G-DAZT].

26. United States v. U.S. District Court (Keith), 407 U.S. 297, 313 (1972).

27. *See* Complaint at *21-22, Jewel v. Nat'l Sec. Agency, No. C 08-04373 JSW, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015); Complaint at 2, First Unitarian Church of L.A. v. Nat'l Sec. Agency, Civ. No. 13–3287 (N.D. Cal. July 16, 2013).

groups, all of which experienced reductions in calls to their public "help" lines and other associational communications after the NSA's telephone records program became broadly public.[28]

Second, assurances that computer searches are safer and less invasive than human searches are not credible. Computers are generally more efficient than humans and will search every single word or bit of information where a human would likely not be able to do so. They are also generally less able to sufficiently judge the context of communications in order to exclude false positives. Moreover, computers are only as careful as their programmers and the algorithms, training data, and other methods they use. Thus, use of computers in "bad" searches can lead to dramatically worse results. For instance, shortly after Edward Snowden leaked information from the NSA, one story explained that due to a coding error, all of the people in the 202 area code, which covers Washington, D.C., were returned in response to a search that was meant to target foreigners abroad.[29]

Third, the "human-eyes" reformulation essentially writes the word "seizures" out of the text of the Fourth Amendment. The Supreme Court has long held that the prohibition against unreasonable seizures is grounded in property rights; for digital communications, the relevant possessory interest violated by a Fourth Amendment seizure is expressed as the right to "dominion and control" over property.[30] In *Jewel,* the government usurps individuals' "dominion and control" of their data by inspecting millions of nonsuspect communications as they travel across the fiber optic cables of providers like AT&T. The government attempts to skirt this problem by redefining "collection" as the point at which human eyes review the information. But this is inconsistent with plain meaning of the word "collection."[31] It is also

---

28. Plaintiffs' Motion for Partial Summary Judgment at 21-22, First Unitarian Church of L.A., Civ. No. 13–3287, http://www.eff.org/document/plaintiffs-motion-partial-summary-judgment-0 [http://perma.cc/8SW7-3E87]. Plaintiff's Declarations are available at http://www.eff.org/document/all-plaintiffs-declarations [http://perma.cc/64QH-P8WG].

29. Barton Gellman, *NSA Broke Privacy Rule Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html [http://perma.cc/AT2M-JSM3].

30. *See, e.g.*, Jacobsen v. United States, 466 U.S. 109, 112 (1984); United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014); United States v. Perea, 986 F.2d 633, 639-40 (2d Cir. 1993).

31. *See Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* 15, U.S. DEP'T DEF. (1982), http://fas.org/irp/doddir/dod/d5240_1_r.pdf [http://perma.cc/HZK6-AUEV] ("Data collected by electronic means is 'collected' only when it has been processed into intelligible form."); *see also* Glenn Kessler, *Clapper's 'Least Untruthful' Statement to the Senate*, WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html [http://perma.cc/JZD4-8E83] (quoting Director of National

inconsistent with the statutory law under Title III of the Omnibus Crime Control and Safe Street Act of 1968, which triggers a wiretap upon the "interception"[32] of an electronic communication "through the use of any electronic, mechanical, or other device,"[33] not at the point of human review.

Fourth, the government's arguments in *Jewel* in support of the "human-eyes" theory rest chiefly on inapplicable case law around dog sniffs for evidence of contraband such as drugs. While there is no "dog-sniff" exception to the Fourth Amendment, several cases have held that in certain situations a sealed package or luggage in transit can be briefly inspected for signs of contraband. Yet even a brief detention for purposes of a dog sniff is a "seizure" under the Fourth Amendment.[34] Moreover, dog sniffs are done to identify packages for detention; a warrant is needed to actually open the packages.[35] The speed of the sniff is also viewed as a proxy for the limited information revealed to the government; a simple, quick sniff reveals less information than a more thorough search.[36]

The context of UPSTREAM surveillance is dramatically different. The duration of the seizure bears no relationship to its intrusiveness. Even if the government completes its wholesale copying, filtering, and full-text analysis in a blink of an eye, those actions are still highly invasive. And unlike the dog sniffs, the investigation opens the *content* of the messages to government inspection.[37] Dog sniffs are also inapt comparisons because the only thing

---

Intelligence James Clapper as saying "[t]here are honest differences . . . when someone says 'collection' to me, that has specific meaning, which may have a different meaning to him").

32. *See* 18 U.S.C § 2511(1)(a) (2012); United States v. Councilman, 418 F.3d 67, 70-71, 79 (1st Cir. 2005) (en banc).

33. 18 U.S.C § 2510(4) (definition of interception).

34. United States v. Place, 462 U.S. 696, 697-99, 702-03, 706-07 (1983).

35. In *United States v. Hoang*, for example, an external dog sniff occurred without any detention or diversion of the package at all; the dog was let loose in a parcel processing room at FedEx. 486 F.3d 1156, 1158 (9th Cir. 2007). Only after the dog alerted to the package and the police had reasonable suspicion that the package contained contraband did the police detain the package. The package was not opened until a warrant was obtained. *Id.*

36. *Place*, 462 U.S. at 707 ("[T]he sniff discloses *only* the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited. . . . Therefore, we conclude that the particular course of investigation that the agents intended to pursue here—exposure of respondent's luggage, which was located in a public place, to a trained canine—did not constitute a 'search' within the meaning of the Fourth Amendment." (emphasis added)).

37. Other package and luggage cases also do not involve copying data or communications inside the container. *See* United States v. Va Lerie, 424 F.3d 694, 696-97 (8th Cir. 2005) (en banc) (holding that moving luggage from the bus to the bus station to seek a passenger's consent to search did not constitute a seizure); United States v. Schofield, 80 F. App'x. 798, 803 (3d Cir. 2003) (determining that lifting a detergent box to reveal only its unusual weight was "almost certainly" not a seizure); United States v. DeMoss, 279 F.3d 632, 634-35 (8th Cir. 2002) (finding that lifting a package off the conveyer belt was not a seizure because the

revealed in a contraband search is the presence or absence of illegal material. By contrast, mentioning the name of a U.S. target in an email or on a social network, which triggers UPSTREAM surveillance, is not only legal—it is fully protected speech.

Overall, Mr. Litt's formulation misses the central goal of the Fourth Amendment to prevent general searches. His argument is that, as long as no responsive information is found, the fact that a seizure and search occurred does not matter, even if done without suspicion and on a massive scale. This might be right if the Framers such as James Otis only objected to searches of their houses that turned up evidence of a crime. They did not.[38] In colonial times, of course, most of a person's "papers" and other sources of information were located in the home, while today those papers regularly travel via a person's ISP like AT&T and are stored digitally with services such as Facebook, Google, or Amazon. Nevertheless, the possessory privacy and dominion interest in the content of the information that Americans routinely store with such services and service providers—including medical records, financial information, business plans, and religious and personal communications—is no less important today than in the eighteenth century. While it might sound like historical science fiction, had the British troops instead employed robots able to search though a colonist's house in a matter of seconds, it seems doubtful that Otis and his compatriots would have been unconcerned.

These arguments by the government have already been rejected in analogous circumstances. For instance, the government's claim that using a "hash value" scan of a computer hard drive does not implicate the Fourth Amendment was rejected in *United States v. Crist*.[39] A hash value is generated by an algorithm that can be used to confirm that two digital files or objects are the same. The *Crist* court noted: "By subjecting the entire computer to a hash value analysis—every file, internet history, picture, and 'buddy list' became available for Government review," even though humans would only be

officers observed only external details that the sender had "virtually guaranteed . . . could be observed by the senses"); United States v. Gant, 112 F.3d 239, 242 (6th Cir. 1997) (finding that removing a bag from an overhead compartment was not a seizure); United States v. England, 971 F.2d 419, 420 (9th Cir. 1992) (involving a dog-sniff of a package in the mail); United States v. Hall, 978 F.2d 616, 618 (10th Cir. 1992) (involving lifting luggage to check its weight); United States v. Harvey, 961 F.2d 1361, 1363 (8th Cir. 1992) (same); United States v. Brown, 884 F.2d 1309, 1311 (9th Cir. 1989) (similar).

38. *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 481-82 (1965) ("Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws."); WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 377-78, 741-42 (2009).

39. 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008).

involved if the computer came up with a match.[40] Similarly, in *Bourgeois v. Peters,* a city requirement that every one of the 15,000 people who sought to attend an annual protest outside a military base pass through a magnetometer was found to be an unconstitutional search.[41] A magnetometer only detects the presence of metal, providing no other information to the human monitoring it. Emphasizing the complete absence of any legal support for "the broad authority to conduct mass, suspicionless, warrantless searches," the Eleventh Circuit explained that the city's position "would effectively eviscerate the Fourth Amendment."[42] Indeed, the Fourth Amendment "establishes searches based on evidence—rather than potentially effective, broad, prophylactic dragnets—as the constitutional norm."[43]

But even *Crist*, which involved the investigation of a single device that had been suspected of containing contraband, and *Bourgeois*, which was based on past incidents of illegal action, do not accurately reflect the breadth and the complete lack of suspicion involved in the NSA programs Mr. Litt defends. The expansion is twofold: both the number of nonsuspect people subject to review and the number of nonsuspect communications reviewed are far greater.

Mr. Litt relies on agency "minimization procedures" as a key factor in his "reasonableness" balancing test.[44] Of course, those, too, are generally kept secret—less than they used to be, as Mr. Litt points out, but they are still not fully transparent. But more importantly, there is still no opportunity for the public to know, much less a petitioner to challenge, whether the procedures that exist on paper in fact operate to sufficiently minimize the impact on nonsuspects inside or outside the United States. We do know that the government minimization procedures allow reuse of information for domestic criminal investigations.[45] But even such fundamental questions as how often Americans' information comes up in searches remain unknown despite many requests for information, including by House Committee members.[46] In the words of Supreme Court Chief Justice Roberts: "The Founders did not fight a

40. *Id.* at 585.

41. 387 F.3d 1303, 1307, 1316 (11th Cir. 2004).

42. *Id.* at 1311.

43. *Id.* at 1312.

44. Litt, *supra* note 1, at 16-17.

45. *See, e.g.*, Memorandum and Order at 31-16 (U.S. FISC November 6, 2015), http://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf [http://perma.cc/36CJ-S6W2].

46. Dan Froomkin, *Stonewalled by NSA, Members of Congress Ask Really Basic Question Again*, THE INTERCEPT (Apr. 22, 2016), http://theintercept.com/2016/04/22/stymied-by-nsa-members-of-congress-ask-really-basic-question-again [http://perma.cc/B5JC-LRDW].

revolution to gain the right to government agency protocols."[47] It is cold comfort for our constitutional rights to rest on secret, agency-promulgated procedures with no chance for adversarial investigation or challenge.

Mr. Litt's argument is that core protections of the Fourth Amendment itself are not suited to the digital age. He embraces broad searches of nonsuspects' communications and suggests that the legitimacy of digital surveillance should be largely decided based on internal agency procedures, rather than constitutional principles. Yet faced with a clash between these principles and advanced technology in *Kyllo v. United States*, the Supreme Court reaffirmed that the doctrine must keep pace with technology to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[48]

The Court's statement in *Kyllo* leads me to revisit where Mr. Litt and I agree. We each believe that the reasonable expectation of privacy test and the third-party doctrine should go. What should replace them? In my view, the "necessary and proportionate" formulation, which is grounded in principles of international law, can provide a means to consider a wider and more relevant range of issues. Indeed, EFF and a coalition of other organizations recently applied this formulation to communications surveillance.[49] As the name implies, the necessary and proportionate principles consider the proportionality of the surveillance, including how many innocent or non-targeted people are affected, and its necessity, including whether other potentially less invasive means have been exhausted. Relevant to Mr. Litt's concerns, this formulation also replaces the outdated lines between information stored locally and that held by third parties, and avoids the problems with the "reasonable expectation of privacy." It focuses instead on whether the government is going to obtain otherwise private information. It uses the concept of "protected information," which "includes, reflects, arises from, or is about a person's communications and . . . is not readily available and easily accessible to the general public."[50]

The Necessary and Proportionate Principles are just a starting point, but I submit that they are more in keeping with the Supreme Court's admonition in *Kyllo* that any changes in the doctrine must preserve privacy. What is clear is that if we are going to address where the Fourth Amendment should be in the digital age, we must do better than a free-form balancing test where the government will always be perched on the heavy end of the scales, and where

47. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

48. 533 U.S. 27, 34-35 (2001).

49. *Necessary and Proportionate*, *supra* note 10.

50. *Id.* at 7-12; *Necessary & Proportionate Global Legal Analysis*, NECESSARY & PROPORTIONATE COALITION (May 2014), http://necessaryandproportionate.org/global-legal-analysis [http://perma.cc/T65Y-8DM6].

the substitution of computers for humans somehow eliminates our Fourth Amendment right to be secure from unreasonable seizures and searches of our most private communications.

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. *Thanks to Andrew Crocker, Lee Tien, Sophia Cope, and Christine Bannan for their editorial assistance.*

Preferred Citation: Cindy Cohn, *Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt*, 126 YALE L.J. F. 107 (2016), http://www.yalelawjournal.org/forum/ protecting-the -fourth-amendment-in-the-information-age.