SPRING
2014

National Security and Mass Internet Surveillance: Blue Penciling the Fourth Amendment?

INTELLIGENCE LAW FINAL PAPER

TONY GLOSSON

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects...." The reference to papers is not an accident; it's not a scrivener's error. It reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government. Because my colleagues in the majority don't see this right as very important, they authorize the government to read every scrap of paper that crosses our borders, whether in a pocket or purse, a package, suitcase or envelope. My concurring colleagues don't recognize this right at all, and thus give customs agents free rein to conduct whatever search they please, for whatever reasons they choose, unless they destroy property or invade the body.

But the Founders were as concerned with invasions of the mind as with those of the body, the home or personal property—which is why they gave papers equal rank in the Fourth Amendment litany. The sum and substance of today's opinion is that we remove papers as an independent sphere of constitutional protection, treating them simply as a species of effects. Because our commission as federal judges does not authorize us to blue-pencil words written by the Founding Fathers, I respectfully dissent.

Kozinski, J., dissenting in United States v. Seljan, 547 F.3d 993 (9th Cir. 2008).

CONTENTS

I. INTRODUCTION

In 2005, the public learned of the Bush administration's decision to permit warrantless wiretapping of American citizens.[1] In 2006, news broke about the Bush administration's efforts to monitor internet traffic.[2] An engineer at AT&T discovered the scheme when he noticed an abnormal hardware configuration that essentially split off copies of the traffic coming into one of AT&T's switching centers in California.[3] Under the test set forth in *Katz v. United States*, however, the government must obtain a warrant to intercept the contents of communications in which United States citizens have an objectively reasonable expectation of privacy.[4] Administration officials maintained that the program was nevertheless legal under the Executive's national security powers.[5] The Bush Administration claimed that the program targeted only those in contact with people in certain foreign countries,[6] and later announced it would bring the program under FISA court oversight.[7]

Seven years later, Edward Snowden began revealing the extent of the NSA's domestic surveillance programs.[8] A similar debate has ensued, but scholars and jurists are

[1] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005).
[2] Matt Richtel & Ken Belson, *U.S. Focused on Obtaining Long-Distance Phone Data, Company Officials Indicate*, N.Y. TIMES (May 18, 2006), http://www.nytimes.com/2006/05/18/us/18call.html.
[3] David Kravets, *NSA Leak Vindicates AT&T Whistleblower*, WIRED (June 27, 2013), http://www.wired.com/2013/06/nsa-whistleblower-klein/.
[4] Katz v. United States, 389 U.S. 347 (1967).
[5] *See* William E. Moschella, Letter to Senate Select Committee on Intelligence (Dec. 22, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.
[6] *Id*. at 1.
[7] Alberto Gonzales, Letter to the Senate Committee on the Judiciary (Jan. 17, 2007), *available at* http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf
[8] See Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 05, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

still unsure as to the constitutionality of the government's spying initiatives.[9] While the NSA's behavior raises a number of legal and political questions, one particularly interesting question involves the opinion of its attorneys regarding interception of the content of online communications. Although it is generally accepted that the Fourth Amendment protects the content of communications between United States citizens,[10] the Snowden revelations raise the specter of an NSA that is comfortable with particularly aggressive interpretations of the scope of its legal and constitutional authority.[11]

If the government were to make these arguments in court, the venue would be a secret court established under the Foreign Intelligence Surveillance Act ("FISA").[12] This arrangement poses two practical problems for scholars interested in the constitutionality of the government's national security activities. First, the Snowden revelations strongly suggest that, were the NSA to conduct massive surveillance of internet traffic, the program itself would be conducted under tight secrecy. Accordingly, potential plaintiffs would never be able to bring suit—or indeed, even to know whether their rights had been infringed in the first place—resulting in very little public judicial guidance. Second, the FISA court itself rarely releases opinions to the public—and when it does, they are often

[9] *Compare* Klayman v. Obama, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013) (holding that the NSA's telephone metadata collection program violates the Fourth Amendment) *with* ACLU v. Clapper, Civ. No. 13-3994 (S.D.N.Y. Dec. 27, 2013) (upholding the program).

[10] *E.g.*, United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.") [hereinafter *Keith Case*]; WAYNE R. LAFAVE ET AL., 2 CRIM. PROC. § 4.3(a) (3d ed. 2013) ("Today, the contents of telephone conversations are ordinarily protected by the Fourth Amendment.").

[11] See Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, 15 (Jan. 23, 2014) ("[T]he government should not base an ongoing program affecting the rights of Americans on an interpretation of a statute that is not apparent from a natural reading of the text. In the case of Section 215, the government should have made it publicly clear in the reauthorization process that it intended for Section 215 to serve as legal authority to collect data in bulk on an ongoing basis.").

[12] Foreign Intelligence Surveillance Act, 50 U.S.C. § 36.

heavily redacted.[13] Consequently, scholars lack occasion to evaluate either the credibility of the government's justifications, or the FISA court's treatment of those theories.

This paper attempts to begin addressing that gap, examining potential arguments the government may make to support mass surveillance programs. This paper focuses on the interception of the content of internet communications; it does not evaluate arguments surrounding the surveillance of noncontent information, or "metadata." In Part II, it sets forth the relevant statutory and constitutional framework governing interception of the content of communications. In Part III, it briefly defines Fourth Amendment searches and seizures for the purpose of data collection. Part IV then examines arguments for full take operations inside the United States, in which the NSA attempts to surveil all traffic flowing through a domestic Internet Service Provider's (ISP) network. It identifies the sobriety checkpoint exception to the Fourth Amendment warrant requirement as a potential theory on which the NSA may argue such a program is constitutional. It concludes that these theories overlook serious differences between the limited invasiveness of checkpoints and the pervasive nature of mass content surveillance. In Part V, the paper examines an alternate scenario in which the NSA attempts to monitor international traffic at major access hubs by which United States networks are connected with the rest of the world. Under this approach, the NSA would rely on the border search exception[14] to the Fourth Amendment to justify internet surveillance. This paper determines that the Supreme Court's reasoning in upholding the border search exception is inapplicable to a mass surveillance program because such a program fails to serve the principal 'filtering' interest

[13] *See* Electronic Privacy Information Center, *Opinions of FISC and FISCR* (last visited 04.01.14), http://epic.org/privacy/terrorism/fisa/fisc.html.
[14] *See, e.g.*, Von Cotzhausen v. Nazro, 107 U.S. 215 (1883) (upholding the warrantless seizure of a shawl at the Port of Milwaukee); *see also* discussion in Section V.

realized by border searches. Finally, Part VI wraps up the discussion with the observation that, on the whole, courts have resisted these attempts at 'blue penciling' privacy protections out of the Fourth Amendment.

II. LEGAL FRAMEWORK GOVERNING COLLECTION OF THE CONTENT OF COMMUNICATIONS IN THE UNITED STATES

Absent a warrant or constitutional exception to the warrant requirement, the government cannot intercept the content of communications between persons within the U.S. The legal protections against interception of content information derive from two sources: first, constitutional privacy protections, including the Fourth Amendment to the Constitution; and second, statutory privacy protections, including Title III of Omnibus Crime Control and Safe Streets Act of 1968, (the "Wiretap Act"),[15] and FISA.[16] Because this paper argues that the Constitution guards against warrantless searches of the content of communications in the national security context, this Part focuses on the former source of privacy protections, briefly surveying landmark cases in Fourth Amendment law and then, where applicable, explaining how those cases interact with statutory protections.[17] These cases set the stage for the discussion of Fourth Amendment exceptions in the balance of the paper.

a. Katz v. United States: *The Content of Private Communications is Protected*

In *Katz v. United States*, the trial court permitted the prosecution to introduce evidence that police obtained by attaching a recording device to the exterior of a phone

[15] Wiretap Act, 42 U.S.C. § 2511.
[16] FISA, 50 U.S.C. § 36.
[17] *See* Subpart c. (summarizing the Keith Case, 407 U.S. 297).

booth that the defendant subsequently utilized.[18] Disapproving of the trial court's narrow reading of the Fourth Amendment, the Supreme Court reasoned that Fourth Amendment protection "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[19] The Court was particularly concerned that popular means of communication retained the same degree of protection as technology advanced: "[t]o read the Constitution more narrowly," the Court chided, "is to ignore the vital role that the public telephone has come to play in private communications."[20] The Court concluded that, in using a phone booth, a person is "surely entitled to assume that the words he utters in to the mouthpiece will not be broadcast to the world."[21] Over time, the Court's pronouncement in *Katz* has become a linchpin of Fourth Amendment protection against interception of private electronic communications—including those conducted online.[22]

b. Smith v. Maryland: *In Isolation, the Noncontent Information about a Particular Communication is Unprotected*

In *Smith v. Maryland*, the Supreme Court confronted another form of electronic surveillance.[23] This time, the police had directed the defendant's phone company to install a device called a pen register outside his home.[24] The pen register recorded the phone numbers that the defendant dialed, but did not capture audible component of his call.[25] Drawing on the formulation of the test for Fourth Amendment protection found in Justice

[18] Katz v. United States, 389 U.S. 347 (1967).
[19] *Id*. at 353.
[20] *Id*. at 352.
[21] *Id*.
[22] *E.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that an email subscriber "enjoys a reasonable expectation of privacy in the contents of emails"); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1039 (2010) ("[T]he Fourth Amendment ordinarily requires a warrant for the collection of the contents of Internet communications.").
[23] Smith v. Maryland, 442 U.S. 735 (1979).
[24] *Id*. at 737.
[25] *Id*.

Harlan's *Katz* concurrence, the *Smith* Court asked whether the defendant had "exhibited an actual (subjective) expectation of privacy" that "society is prepared to recognize as reasonable."[26] As it turned out, the distinction between collection of the call's audible content on the one hand, and the noncontent records about the call on the other, made all the difference: because "all telephone users realize that they must convey phone numbers to the telephone company,"[27] the defendant could not reasonably have expected his call records to remain private.[28] Accordingly, the Court upheld the trial judge's decision to admit the pen register evidence.[29] Like *Katz*, *Smith* has been extended into the internet context[30]—thus, while warrantless interception of the content of internet communications is unconstitutional, warrantless interception of an ISP subscriber record is not.

c. United States v. United States District Court *(Keith Case): The Warrant Requirement Applies to Domestic Security Investigations*

In *United States v. United States District Court*, the government conducted a warrantless wiretap in connection with the attempted bombing of a Central Intelligence Agency field office in Michigan.[31] The government argued that the wiretap evidence, excluded by the trial court, should have been admitted notwithstanding the *Katz* warrant requirement for wiretapping.[32] In support, the government contended that "special circumstances applicable to domestic security surveillance" counseled in favor of an exception to the

---

[26] *Id*. at 740 (quoting Katz, 389 U.S. at 361 (Harlan, J., concurring)).
[27] *Id*. at 742.
[28] *Id*. at 743.
[29] *Id*. at 746.
[30] *E.g.*, United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) ("There is no difference of constitutional magnitude between this aspect of the pen register and the government's monitoring here of the total volume of data transmitted to or from [the defendant's] account . . . We therefore hold that the computer surveillance techniques that Alba challenges are not Fourth Amendment searches.").
[31] Keith Case, 407 U.S. 297.
[32] *Id*. at 303.

warrant requirement.[33] Declining the invitation to create a domestic security exception, the Court stressed that existing exceptions are "few in number and carefully delineated."[34] In this case, despite the government's attempted invocation of Executive domestic security responsibilities, the Court concluded that the judiciary is well-positioned to weigh that responsibility in evaluating warrant applications, and that "[i]f the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probably cause for surveillance."[35]

Some commentators attempt to quarantine this case by defining down the Fourth Amendment-restricted domestic security function to near-irrelevancy in favor of the (arguably) unrestricted foreign intelligence gathering function.[36] Because modern security threats are more dynamic and unpredictable than those in the past courts, the argument goes, courts should conceptualize mass surveillance as *foreign* intelligence-gathering to afford the government flexibility to collect data ahead of time that may become useful later.[37] Perhaps anticipating such theories, the *Keith* Court took pains to emphasize that it was aware the question arose "at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history."[38] Nevertheless, it was precisely this ambiguity that led the Court to stress the indispensability of the warrant requirement:

---

[33] *Id*. at 318.
[34] *Id*. (citing Katz, 389 U.S. at 357).
[35] *Id*. at 320.
[36] *See, e.g.*, Richard Henry Seamon, *Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits*, 35 HASTINGS CONST. L.Q. 449, 492 (2008) ("[T]he [Executive's] power justifies surveillance outside FISA even today . . ."); *see also* 50 U.S.C. § 1804(a)(6)(B) (2010) (reflecting a change that lowered the court order threshold for foreign intelligence electronic surveillance from requiring that the "primary purpose" is collection of foreign intelligence information to requiring only that it be a "significant purpose").
[37] *Id*.
[38] Keith Case, 407 U.S. at 319-20.

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech . . . History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation.[39]

The Court here is unwavering: doubt must be resolved in favor of the citizen's liberty, and against the Executive's power—and mass surveillance perpetrates these exact harms against precisely the same people. Nonparticularized collection facilitates selective investigation because the data need not be deliberately collected; it is instantaneously available—even absent political motivation, there are countless dubious reasons one may wish to access citizens' data once it has been compiled.[40] Additionally, mass surveillance is even *more* likely than garden-variety surveillance to chill dissent because it infringes on associational privacy by enabling link analysis methodology.[41] The fact is that if foreign intelligence is not limited to targeted investigation of defined threats—and is instead broad enough to encompass mass surveillance—the concept becomes no more discrete than domestic intelligence, and consequently implicates the same constitutional limitations.

---

[39] *Id*. at 313-14.
[40] *See* Siobhan Gorman, *NSA Officers Spy on Love Interests*, WSJ (Aug. 23, 2013), http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.
[41] Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 357 (2008).

Thus, for the Court's Fourth Amendment carve-out for foreign intelligence to be doctrinally viable, foreign intelligence activities must be particularized.

Nevertheless, this observation does not end the discussion because the Court also noted that "Congress may wish to consider protective standards for [domestic security] which differ from those already prescribed for specified crimes in Title III."[42] Accordingly, the government may argue that mass email collection comports with the Fourth Amendment provided the FISA Court—and by extension, Congress—approves of it.

That argument, however, misconceives the 'standards' to which the Court referred. "In cases in which the Fourth Amendment requires that a warrant to search be obtained, '*probable cause' is the standard* by which a particular decision to search is tested against the constitutional mandate of reasonableness."[43] Accordingly, the relevant standard is the degree of legally defensible suspicion required before the government may establish probable cause to conduct a search or seizure. That standard, reasoned the Court, bears an inverse relationship with the government interest or "need for the inspection," such that the weightier the government interest, the more lenient the requisite evidentiary standard with respect to the person, place, or thing named in the warrant.[44] It strains credulity, however, to assert that there exists a point at which the government interest becomes so fantastic as to render the existence of *any* particularized suspicion altogether irrelevant.[45]

---

[42] Keith Case, 407 U.S. at 322.
[43] *Id*. at 323 (quoting Camara v. Municipal Court, 387 U.S. 523, 534-35 (1967)) (emphasis added).
[44] *Id*.
[45] Consider that even for the universal requirement of housing code inspections, upheld in Camara, the Court found it necessary to establish particularized suspicion: "The passage of a certain period without inspection might of itself be sufficient in a given situation to justify the issuance of warrant . . . 'probable cause' to issue a warrant to inspect must exist if reasonable legislative or administrative standards for conducting an area inspection are satisfied *with respect to a particular dwelling*." Camara, 387 U.S. at 538 (emphasis added). If such is the case for an infrequent and trivial trespass, concerned only with the structural integrity of a given

Thus, the Court's invitation to Congress is, by its own terms, an acknowledgement of congressional authority to provide for the issuance of warrants on a lesser showing of suspicion than ordinarily necessary—*not* a wholesale nullification of the Fourth Amendment's particularity requirement.[46]

Consequently, in the domestic security context, the fundamental constitutional rules of the road permit isolated metadata collection,[47] but disallow warrantless interception of content of communications, including those transpiring online.

III. SEARCHES AND SEIZURES OF DATA

Having set forth the constitutional framework governing searches, it is helpful to consider briefly the Fourth Amendment's application to data. Because the NSA can obtain access to data without physically taking the storage device in which it resides or from which it originates, NSA attorneys will likely make two arguments. First, they may adopt Professor Ric Simmons' position,[48] arguing that the NSA may scan communications for the presence or absence of specific data[49] without thereby conducting a search provided that the scanning algorithm does not reveal any legitimate content.[50] If the algorithm returned a positive alert, the NSA would then argue that the output supplies reasonable suspicion to

---

edifice, one is hard-pressed to imagine that the Court would depart from established precedent to bless a *nonparticularized* search of the citizenry's most intimate interactions.

[46] U.S. CONST. amend. IV.

[47] After Smith v. Maryland, Congress *is* free to permit warrantless surveillance of metadata. If conducted in a nonparticularized manner, however, that practice too may have Fourth Amendment implications. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

[48] Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002) [hereinafter *From Katz*].

[49] For example, a secret file taken from the government.

[50] Scott J. Glick, *Virtual Checkpoints and Cyber-Terry Stops: Digital Scans to Protect the Nation's Critical Infrastructure and Key Resources*, 6 J. NAT'L SECURITY L. & POL'Y 97, 117 (2012) ("[U]nder the approach discussed in this article, the digital scans of the contents of such communications would initially involve no human review and would only be looking for malicious digital signatures.") [hereinafter *Virtual Checkpoints*].

conduct a full search.[51] Second, the NSA may argue that automatically copying data does not effect a search or seizure until a government agent reviews that data.[52]

To illustrate the first approach, Professor Simmons writes:

> [C]onsider an improved version of Carnivore . . . which did not filter based on address but instead could sift through the content of all the transmissions passing through the server to which it was attached and copy only those which contained unambiguously illegal content: pictures of child pornography, for example, or orders to transfer funds in illegal amounts. Let us also assume that these transmissions would be copied, but they would not be opened or read by human beings without a warrant; thus, the only information that would result from this monitoring of the internet would be that a given transmission contained evidence of illegal activity.[53]

This approach relies on *Illinois v. Caballes*[54] and *United States v. Place*.[55] In those cases, the Supreme Court upheld exterior "sniff searches" of a car and a suitcase, respectively.[56] Because dog sniff searches revealed only "the presence or absence of narcotics, a contraband item," and "do[] not expose noncontraband items that otherwise would remain hidden from public view,"[57] the Supreme Court in those cases concluded that no Fourth Amendment search had occurred.[58] Thus, Professor Simmons concludes that an algorithm that reveals only the presence or absence of specific contraband data—a so-called *binary* search—is constitutionally permissible even without a warrant.[59]

However, that view seems to mischaracterize the Court's analysis. In those cases, the drug dogs at no point broke the seal surrounding the closed suitcase or car to access their

---

[51] *Id*. at 117 ("[F]urther analysis would only take place if there was a reasonable basis to believe that a malicious digital code may be present.").
[52] *Id*. at n.18 (citing Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531, 535 (2005)) ("[A] search is best described as the process by which data is exposed to human observation.").
[53] Simmons, *From Katz to Kyllo*, 53 HASTINGS L.J. at 1352.
[54] Illinois v. Caballes, 543 U.S. 405 (2005).
[55] United States v. Place, 462 U.S. 696 (1983).
[56] Caballes, 543 U.S. at 407; Place, 462 U.S. at 699.
[57] Place, 462 U.S. at 707.
[58] Caballes, 543 U.S. at 410; Place, 462 U.S. at 707. The Court in Place ultimately overturned the defendant's conviction on different grounds. *Id*. at 710.
[59] Simmons, *From Katz to Kyllo*, 53 HASTINGS L.J. at 1352.

contents in any capacity. Instead, their alert was based on the presence of contraband particles escaping the closed container into the nearby vicinity.[60] Indeed, that distinction is crucial because "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."[61] Accordingly, the Supreme Court has emphasized that "an exterior sniff of an automobile does not require entry into the car . . . Like the dog sniff in *Place*, a sniff by a dog that simply walks around a car is much less intrusive than a typical search."[62] The reasoning supporting dog sniff cases, therefore, is inapplicable where the government deigns to breach the *contents* of communications. Accordingly, the *Katz* warrant requirement for searching contents of communications remains intact, and may not be avoided merely by performing a "binary" search.

Turning to the second argument, the government may seek to avoid the warrant requirement by copying mass quantities of citizens' data and storing it—without performing a manual search—until individualized suspicion can be established for a given individual or group. To justify this practice, the government must endorse Professor Orin Kerr's initial approach, now abandoned, that copying data does not seize it.[63] For precedential support, the government would likely have to rely on *Arizona v. Hicks*, a case in which the Supreme Court held that a police officer did not effect a seizure when he wrote down a serial number from the defendant's stereo during the course of an unrelated

---

[60] For more on how dog sniff searches work, *see* Dan Hinkel & Joe Mahr, *Tribune analysis: Drug-sniffing dogs in traffic stops often wrong*, CHI. TRIB. (Jan. 06, 2011), *available at* http://articles.chicagotribune.com/2011-01-06/news/ct-met-canine-officers-20110105_1_drug-sniffing-dogs-alex-rothacker-drug-dog.
[61] United States v. Ross, 456 U.S. 798, 822-23 (1982).
[62] City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000).
[63] *See* Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531, 563 (2005) ("Under my approach, courts should find that the creation of a bitstream copy is not an independent 'seizure.'"), *but see* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 704 (2010) ("My earlier approach did not recognize the importance of access to data in the regulation of government evidence collection . . . I now reject my earlier view.").

search.[64] According to the court, the officer's recording of the serial number "did not meaningfully interfere with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure."[65] NSA attorneys could claim that this reasoning shows that the NSA can copy internet traffic without effecting a seizure under the Fourth Amendment. On that view, the NSA need not secure a warrant to copy and store traffic without searching it.

This argument, however, again overlooks the fact that copying a serial number under the circumstances in *Hicks* merely replicated information *already exposed* under the "plain view exception"[66] during a legitimate search.[67] That exception carves out an allowance for observation and seizure of evidence visible during the course of a *separately-justified* search.[68] When the NSA clones and stores mass amounts of internet traffic, on the other hand, no such separate justification exists. Thus, copying the content of private communications—including internet traffic—constitutes a seizure.

Indeed, unlike writing down a serial number, copying data meaningfully interferes with the possessory interests of its owner. Among the bundle of sticks included in property ownership are the right of excludability and the right of destruction.[69] When the

---

[64] Arizona v. Hicks, 480 U.S. 321 (1987).
[65] *Id*. at 324.
[66] Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) ("It is well established that under certain circumstances the police may seize evidence in plain view without a warrant.").
[67] Hicks, 480 U.S. at 323 ("[A] bullet was fired through the floor of respondent's apartment, striking and injuring a man in the apartment below. Police officers arrived and entered respondent's apartment to search for the shooter, for other victims, and for weapons.").
[68] Coolidge, 403 U.S. at 465 ("An example of the applicability of the 'plain view' doctrine is the situation in which the police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character.").
[69] Scott J. Upright, *Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment*, 51 WM. & MARY L. REV. 291, 316-17 (2009) (quoting BLACK'S LAW DICTIONARY 1252 (8th ed. 2004))("[T]he copying of electronic files without probable cause should qualify as a meaningful interference with a possessory interest and, thus, an unreasonable seizure. This conclusion is

government copies data, it meaningfully interferes with (and, in fact, obliterates) its owner's ability to exclude others from its use and the right to destroy it.[70] Accordingly, it is no surprise that the Supreme Court has repeatedly referred to the electronic recording of communications as a seizure. In *New York v. Burger*, for example, the Court found unconstitutional "the search and seizure authorized by [New York's wiretap statute]," which consisted of "an ex parte order for eavesdropping."[71] In striking down the law, the Court described the evidence obtained by the wiretaps as "seized conversations."[72] Again, in *Katz*, the Court proclaimed that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[73] Still again, in *United States v. New York Telephone Company*, the Court held constitutional a certain authorization of an electronic "'search' designed to ascertain the use which is being made of a telephone . . . and the 'seizure' of evidence which the 'search' of the telephone produces."[74] Such language clearly indicates that electronically recording data seizes it. Therefore, the NSA seizes evidence when it copies internet traffic; any discussion of when or whether an agent ever looks at the data is irrelevant.

---

reached through a simple application of current property law. Black's Law Dictionary defines property as '[t]he right to possess, use, and enjoy a determinate thing .... Also, termed bundle of rights.'").

[70] *Id*. at 317 ("Once a traveler's electronic files are copied, that traveler loses the right to destroy that property because the government now controls an exact replica."); Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. at 712 ("The law should focus on when the person loses exclusive rights to the data.").

[71] Berger v. State of N.Y., 388 U.S. 41, 54 (1967).

[72] *Id*. at 60.

[73] Katz, 389 U.S. at 353.

[74] United States v. New York Tel. Co., 434 U.S. 159, 169 (1977).

IV. THE POLICE HIGHWAY CHECKPOINT POWER DOES NOT JUSTIFY GOVERNMENT ACCESS TO CONTENT INFORMATION

One way the NSA could seek to conduct mass internet content surveillance would be to monitor the content of internet communications conducted through one or more specific ISPs or applications. To take a concrete example, this type of program could take the form of the President Bush's Terrorist Surveillance Program, as exposed by Mark Klein, sparking the Room 641A controversy.[75] Installed on AT&T's network in a San Francisco office building, the system had "the capability to enable surveillance and analysis of internet content on a massive scale, including both overseas and purely domestic traffic."[76] Because information contained in the bodies of emails represents content information, it is protected by a warrant requirement under *Katz*.[77] However, the NSA cannot obtain a warrant to conduct mass surveillance because warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[78] Mass surveillance, by definition, is nonparticularized. Thus, those who support such monitoring must find support for a program like the Terrorist Surveillance Program in the existing exceptions to the Fourth Amendment warrant requirement for searches.

Sobriety checkpoints provide an attractive analogue for proponents of Executive mass surveillance power because checkpoints represent a rare context in which the Supreme Court has upheld inquiries into individuals for whom the government does not have particularized suspicion. Indeed, the Court's reasoning in one landmark case, *Michigan*

---

[75] Ryan Singel, *AT&T 'Spy Room' Documents Released, Confirm Wired News' Earlier Publication*, WIRED (June 12, 2007), http://www.wired.com/2007/06/att_spy_room_do/.
[76] *Id*.
[77] See Part II c. (summarizing Katz, 389 U.S. 347).
[78] U.S. CONST. amend. IV.

Department of State Police v. Sitz, superficially appears to map nicely onto mass internet surveillance: the court relied on the challenged checkpoint's "minimal" degree of delay to motorists and the effectiveness of the checkpoint program.[79] Mass internet surveillance, the NSA could claim, results in imperceptible or nonexistent delays to internet traffic, while supplying an effective tool against threats to national security.

This line of reasoning, however, is misdirected. First, while the delay to motorists is a plausible proxy for a search's intrusiveness in the context of checkpoints,[80] it is hardly the microsecond delay in content delivery that troubles civil libertarians. While an officer at a sobriety checkpoint can quickly tell whether an individual is likely to be intoxicated without intruding into the vehicle or exposing much irrelevant information at all, content surveillance exposes all manner of irrelevant information with the potential to lay bare the most intimate details of a person's life. Surveillance of content may reveal, for example, "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[81] Given the Court's recognition in the *Keith Case* of the government's inclination toward discrimination against those who disagree with its policies, the sheer manipulative power wielded by a government with that information likely renders such a program unconstitutional.[82] Unlike sobriety checkpoints,

---

[79] Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 452 (1990).
[80] *Id*. at 452 ("The trial court . . . accurately gauged the 'objective' intrusion, measured by the duration of the seizure . . . .").
[81] Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 12 N.Y.3d 433, 440 (2009)). Sotomayor here commented on the collection of GPS data, but the argument is much the same for the content of internet communications: searches for these locations, private messages discussing such visits, and anonymous internet postings about them are among the many ways with which searches of the content of internet communications threaten to reveal the same information as GPS data—and GPS data is itself often transmitted via the internet.
[82] Keith Case, 407 U.S. at 319-20.

mass content surveillance can hardly be said to be 'minimally intrusive.'[83] Moreover, checkpoint programs are distinguishable from mass content surveillance on another level: it is not at all apparent that mass content surveillance would yield the same degree of preventative efficacy as sobriety checkpoints.[84] At checkpoints, agents remove allegedly intoxicated drivers from the highway in real time, instantly neutralizing the threat that justified the government intrusion. By contrast, much of the information the NSA seeks must be analyzed and sometimes decrypted before becoming useful—at which point it may be too little, too late, or both. Because mass content surveillance diverges profoundly from sobriety checkpoints in terms of invasiveness and effectiveness, the latter cannot serve as a justification for the former.

Perhaps most importantly, the sobriety checkpoint analogy overlooks the fundamental limitations on the practice that make it constitutionally acceptable. For example, in *United States v. Martinez-Fuerte*, the court upheld the checkpoint at issue because its high degree of visibility and taxing demand on law enforcement resources provided effective guards against abuse:[85]

> Motorists using these highways are not taken by surprise as they know, or may obtain knowledge of, the location of the checkpoints and will not be stopped elsewhere . . . The regularized manner in which established checkpoints are operated is visible evidence, reassuring to law-abiding motorists, that the stops are duly authorized and believed to serve the public interest. The location of a fixed checkpoint is not chosen by officers in the field, but by officials responsible for making overall decisions as to the most

[83] Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). As noted above, mass internet surveillance is particularly intrusive because GPS data is just one type of information that is often transmitted via the internet.
[84] Glick, Virtual Checkpoints, 6 J. Nat'l Security L. & Pol'y at n.97 (citing Center for Disease Control, *Research Update: Sobriety Checkpoints Are Effective in Reducing Alcohol-Related Crashes* (2002)) ("[A]lcohol-related traffic deaths reduced by 20% in states that implemented sobriety checkpoints as compared to those that did not.").
[85] United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

> effective allocation of limited enforcement resources. We may assume that such officials will be unlikely to locate a checkpoint where it bears arbitrarily or oppressively on motorists as a class. And since field officers may stop only those cars passing the checkpoint, there is less room for abusive or harassing stops of individuals than there was in the case of roving-patrol stops. Moreover, a claim that a particular exercise of discretion in locating or operating a checkpoint is unreasonable is subject to post-stop judicial review.[86]

Thus, in recognizing a rare departure from ordinary Fourth Amendment protections, the Court relied heavily on resource constraints to prevent abusive or unreasonable searches under the exception. In electronic surveillance, however, none of those practical safeguards exist.[87] Internet users cannot simply learn which "locations" to avoid such that they "will not be stopped elsewhere."[88] Instead, every bit of data sent or received from any location on any protocol is potentially subject to surveillance. Rather than being forced to pick and choose discrete checkpoint locations to which surveillance resources should be devoted, modern technology permits a "full take"[89] approach to mass surveillance. Worse, post-search judicial review is frequently infeasible because internet users may not even be aware of the search by which their rights have been violated. In short, the NSA can surreptitiously conduct surveillance on a far broader and more intrusive scale than would ever be imaginable for checkpoint operators. All these differences between police checkpoints and mass internet surveillance go to the heart of Fourth Amendment

---

[86] *Id*. at 559.
[87] Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility.").
[88] Martinez-Fuerte, 428 U.S. at 559.
[89] Katalog von Fragen, *Als Zielobjekt markiert*, DER SPIEGEL (July 8, 2013) (translation by Cryptome.com) ("'Full take' means that the system saves everything. If you send a data packet and if makes its way through the UK, we will get it. If you download anything, and the server is in the UK, then we get it. And if the data about your sick daughter is processed through a London call center, then ... Oh, I think you have understood . . . Even the Queen's selfies with her lifeguards would be recorded, if they existed.").

reasonableness, and cannot be ignored to blue-pencil the Fourth Amendment's protections in favor of the Executive's domestic security powers.

V. THE BORDER SEARCH EXCEPTION DOES NOT JUSTIFY SCANS OF INTERNATIONAL INTERNET TRAFFIC

Because Supreme Court checkpoint precedent cannot support deviating from the Fourth Amendment's protection for the content of internet communications, mass surveillance proponents may fall back to a more limited, but somewhat more plausible argument.[90] The argument expands on the Supreme Court's recognition of the right of the sovereign to keep harmful objects outside of its borders.[91] Based on this power, the Supreme Court has held that a person forfeits the protection of the Fourth Amendment's individualized suspicion requirement when crossing an international border, or passes through a functional equivalent, like an airport.[92] Thus, government agents can search every person travelling internationally without ever securing a warrant.

---

[90] *Compare* Glick, *Cyber-Terry Stops* (arguing that the border search exception supports international internet traffic surveillance) *with* U.S. Dep't of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (2006) (conspicuously missing any mention of the border search exception), *available at* www.epic.org/privacy/terrorism/fisa/doj11906wp.pdf.

[91] *See, e.g.*, Almeida-Sanchez v. United States, 413 U.S. 266 (1973).

[92] *Id*. at 272 ("Whatever the permissible scope of intrusiveness of a routine border search might be, searches of this kind may in certain circumstances take place not only at the border itself, but at its functional equivalents as well."). It is worth noting that the reasoning behind the "functional equivalent" doctrine cuts both ways: just as the constitutional allowance for warrantless border searches should extend *inward* to the functional equivalent of the border—airports—to account for the realities of modern transportation, likewise should the constitutional prohibition against warrantless border searches of internet traffic extend *outward* to the functional equivalent of the telecommunications "border"—undersea backbone cables—to account for realities of modern communications. Thus, the NSA's taps of these undersea cables are probably unconstitutional. *See* Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, THE ATLANTIC (July 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

On this exception, government attorneys may argue, as Department of Justice counsel Scott Glick does, that the NSA could search apparently international traffic under the border search exception.[93]

However, that justification ignores the purpose for which the exception is recognized. Far from enabling national security *investigative* interests, the exception exists to serve *protective* ones, under which harmful objects are filtered out before crossing the border. As the Supreme Court has explained it, "[c]ustoms officers characteristically inspect luggage and their power to do so . . . is intimately associated with excluding illegal articles from the country."[94] And again, "[h]istorically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry."[95] Therefore, the NSA cannot justify searches of cloned international internet traffic on the border search exception because searches of cloned traffic are wholly ineffectual at keeping things out of the United States. Even accepting the somewhat dubious proposition that the phrase "illegal articles" comfortably encompasses data that the NSA deems harmful to national security, merely searching a cloned traffic stream does not—and cannot—stop the original stream from traversing across the border and into the United States.

Conversely, if the NSA were to attempt to resolve this defect by actively filtering the data from the primary traffic stream in real time, it would face serious *First* Amendment hurdles because such a scheme imposes a prior restraint on speech. The Supreme Court has held that prior restraints are invalid—even when they purport to guard against unprotected speech—because "a censor's business is to censor," so "there inheres the

[93] Glick, *Virtual Checkpoints*, 6 J. NAT'L SECURITY L. & POL'Y at 129.
[94] United States v. Thirty-Seven (37) Photographs, 402 U.S. 363, 376 (1971).
[95] United States v. 12 200-Foot Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973).

danger that he may well be less responsive than a court . . . to the constitutionally protected interests in free expression. And if it is made unduly onerous, by reason of delay or otherwise, to seek judicial review, the censor's determination may in practice be final."[96] In most cases, the government attempts to effect a censorship regime through licensing speech,[97] while internet filtering would censor speech by blocking content that the NSA deems unprotected under the First Amendment. The constitutional interest, however, is the same: the government may not place the initial burden on the speaker to persuade the government to permit her speech; rather, the government must seek to punish unprotected speech *ex post*.[98] In any event, it seems unlikely at this point that the NSA would be interested in a filtering system, which would produce far fewer intelligence benefits in most cases than secretly monitoring communications.

Moreover, while the Fourth Amendment may not require a warrant to *conduct a search* of an envelope at the border, the First Amendment likely imposes a warrant requirement for *actually reading* its contents. In *United States v. Ramsey*, the Supreme Court specifically relied on the fact that government agents were forbidden from actually reading the content of the correspondence without a warrant in dismissing the defendant's First Amendment challenges to the warrantless opening of his envelopes.[99] The Court intimated that, without such a requirement, speech may be chilled by the prospect of government observation of

---

[96] Freedman v. Maryland, 380 U.S. 51 (1965).
[97] *E.g., Id.*; Near v. State of Minnesota ex rel. Olson, 283 U.S. 697 (1931).
[98] Freedman, 380 U.S. 51. *See also* United States v. Am. Library Ass'n, Inc., 539 U.S. 194, fn.4 (2003) (implicitly accepting the dissent's characterization of filtering technology as a prior restraint if applied by the government, but declining to "extend[] prior restraint doctrine to the context of public libraries' collection decisions").
[99] *See* United States v. Ramsey, 431 U.S. 606, 623 (1977) ("The statute in question requires that there be 'reasonable cause to believe' the customs laws are being violated prior to the opening of envelopes. Applicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant.")

its content at the border.[100] Thus, the First Amendment probably requires a warrant to surveil the content of international electronic communications, thereby precluding any mass surveillance scheme.

There are still other indications that the border search exception is inapplicable to mass surveillance of internet traffic. First, because of the ease with which internet users can transfer electronic files into the United States without ever going through customs,[101] some commentators argue that the border search exception should not apply even to data stored on a physical drive carried on a person as she crosses an international border.[102] In light of the trivial or nonexistent benefit to the government's filtering interest that searching electronic devices at the border produces, these scholars believe that the high degree of intrusiveness makes the search *per se* unreasonable, and thereby violative of the Fourth Amendment's reasonableness standard.[103] If even searches of data contained on storage devices physically transported across the border are constitutionally suspect, searches of international internet traffic is likely much more so. Second, the *en banc* Ninth Circuit has recently limited the border search exception in the context of physical storage devices,

---

[100] *Id*. at 624 ("[R]eading of any correspondence inside the envelopes is forbidden. Any chill that might exist *under these circumstances* may fairly be considered . . . minimal.") (emphasis added).
[101] *E.g.*, Email, BitTorrent, cloud storage, etc.
[102] Upright, *Suspicionless Border Seizures of Electronic Files*, 51 WM. & MARY L. REV. at 325-26 (quoting Brinegar v. United States, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting)) ("[The Fourth Amendment guarantees] are not mere second-class rights but belong in the catalog of indispensable freedoms. Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government."); Ari B. Fontecchio, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 266 (2009) ("[T]he individual's interest should prevail where an agent has no good reason to search a traveler's laptop . . . This view would not require overturning any Supreme Court precedent, because . . . the data inside laptops falls outside the scope of the border search and special needs doctrines, and the Court has never held otherwise."); Lindsay E. Harrell, *Down to the Last .jpeg: Addressing the Constitutionality of Suspicionless Border Searches of Computers and One Court's Pioneering Approach in United States v. Arnold*, 37 SW. U. L. REV. 205, 238 (2008) ("If . . . United States Customs and Border Protection officials have no objective, articulable reasons to search a traveler's computer and no other exceptions apply, then a computer search should not only be unwarranted, but also unconstitutional.").
[103] *Id*.

requiring either a by-hand manual search or—in case of a forensic search—at least a small degree of individualized suspicion.[104] Either requirement would preclude mass surveillance of data if applied to international internet traffic.

VI. CONCLUSION

In the end, Judge Kozinski was right: privacy of thought, ideas, and conscience are important Fourth Amendment interests. Despite attempts to blue-pencil Fourth Amendment protection, courts have by and large guarded that protection over the years. Even as technology advances rapidly, that protective trend seems set to continue. Indeed, while the means of communication and investigation have both changed, the same reasoning that protects the content of snail mail and telephone protects that of electronic communications as well. Because scans evaluate content, they are Fourth Amendment searches, and because copying exercises control, it effects a seizure. The exceptions to the Fourth Amendment remain cabined to the carefully-delineated needs from which they arose. Police checkpoints are regulated, in part, by resource constraints; and the border search exception applies only to tangible items. Neither justification applies to electronic communications; thus, neither exception applies to internet traffic. Accordingly, whatever ways courts have blue-penciled the Fourth Amendment, mass content surveillance—by the NSA, or by law enforcement—remains unconstitutional.

[104] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) *cert. denied*, 134 S. Ct. 899 (U.S. 2014) *reh'g denied*, 13-186, 2014 WL 801197 (U.S. Mar. 3, 2014).