

No. 06-50581
IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA) (NO. CR 05-772-DDP)
)
Plaintiff-Appellant,)
)
v.)
)
MICHAEL TIMOTHY ARNOLD)
)
Defendant-Appellee.)
_____)

**BRIEF FOR AMICI CURIAE
ASSOCIATION OF CORPORATE TRAVEL EXECUTIVES
AND ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF DEFENDANT-APPELLEE**

Appeal from The United States District Court
For the Central District of California

RANDALL BRATER
Arent Fox LLP
1050 Connecticut Ave., N.W.
Washington, D.C. 20036

Of Counsel:

JOHN M. GURLEY
TIMOTHY P. KANE
Arent Fox LLP
1050 Connecticut Ave., N.W.
Washington, D.C. 20036
202-857-6000
Attorneys for Amici Curiae

TABLE OF CONTENTS

	<u>Page</u>
INTEREST OF AMICI CURIAE	1
SUMMARY OF ARGUMENT	3
ARGUMENT	4
A. THE SEARCHES	6
B. SUSPICIONLESS BORDER SEARCHES OF LAPTOP COMPUTERS RAISE SPECIAL CONSTITUTIONAL CONCERNS	9
CONCLUSION	29

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

<i>ACLU v. National Sec. Agency</i> , 438 F. Supp. 2d 754 (E.D. Mich. 2006)	6
<i>Alexander v. United States</i> , 362 F.2d 379 (9th Cir. 1966)	19
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976)	10, 27
<i>Bantam Books, Inc. v. Sullivan</i> , 372 U.S. 58 (1963)	25
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	17-18
<i>Burse v. United States</i> , 466 F.2d 1059 (9th Cir. 1972)	22
<i>Camara v. Municipal Court</i> , 387 U.S. 523 (1967)	17
<i>Go-Bart Importing Co. v. United States</i> , 282 U.S. 344 (1931)	18
<i>Heidy v. U.S. Customs Service</i> , 681 F.Supp. 1445 (C.D. Cal. 1988)	23, 28-29
<i>In re Guantanamo Detainee Cases</i> , 355 F. Supp. 2d 443 (D.D.C. 2005)	5
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	23-24, 27
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	13-14
<i>Lo-Ji Sales, Inc. v. New York</i> , 442 U.S. 319 (1979)	22
<i>Marcus v. Search Warrant</i> , 367 U.S. 717 (1961)	11, 26
<i>McIntyre v. Ohio Elections Commission</i> , 514 U.S. 334 (1995)	25
<i>Payton v. New York</i> , 445 U.S. 573 (1980)	17
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997)	24
<i>Roaden v. Kentucky</i> , 413 U.S. 496 (1973)	22

<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	11, 22
<i>Steagald v. United States</i> , 451 U.S. 204 (1981)	17
<i>Thornhill v. Alabama</i> , 310 U.S. 88 (1940)	26
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006)	12
<i>United States v. Alfonso</i> , 759 F.2d 728 (9th Cir. 1985)	22
<i>United States v. Arnold</i> , 454 F. Supp. 2d 999 (C.D. Cal. 2006).	passim
<i>United States v. Barth</i> , 26 F. Supp. 2d 929 (W.D. Tex. 1998)	12
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987)	6
<i>United States v. Flores-Montano</i> , 541 U.S. at 149 (2004)	14, 28
<i>United States v. Furukawa</i> , No. 06-145, 2006 WL 3330726 (D. Minn. 2006)	19
<i>United States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006) (en banc)	12
<i>United States v. Ickes</i> , 393 F.3d 501 (4th Cir. 2005)	20
<i>United States v. Meija</i> , 720 F.2d 1378 (5th Cir. 1983)	14
<i>United States v. Montoya de Hernandez</i> , 473 U.S. 531 (1985)	14
<i>United States v. Park</i> , No. CR-05-375, 2007 WL 1521573 (C.D.Cal. 2007)	19
<i>United States v. Price</i> , 472 F.2d 573 (9th Cir. 1973)	11
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977)	10-11, 18, 28
<i>United States v. Reyes</i> , 922 F. Supp. 818 (S.D.N.Y. 1996)	12
<i>United States v. Romm</i> , 455 F.3d 990 (9th Cir. 2006)	16, 19
<i>United States v. Schoor</i> , 597 F.2d 1303 (9th Cir. 1979)	21-22

<i>United States v. Soto-Teran</i> , 44 F.Supp.2d 185 (E.D.N.Y. 1996)	14
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990)	4-5
<i>United States v. U.S. Dist. Ct.</i> , 407 U.S. 297 (1972)	23-24, 26-27
<i>Wolf v. Colorado</i> , 338 U.S. 25 (1949)	17

MISCELLANEOUS

Ty Howard, <i>Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files</i> , 19 Berkeley Tech. L.J. 1227, 1233–34 (2004)	16
Orin Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531, 569 (2005)	passim
S. Rep. No. 99-541, at 5 (1996)	13
Joe Sharkey, <i>At U.S. Borders, Laptops Have No Right to Privacy</i> , N.Y. TIMES, October 24, 2006	7-8
Joe Sharkey, <i>To Do List: Rename Laptop Files 'Grandma's Favorite Recipes'</i> , N.Y. TIMES, November 7, 2006	7-8

No. 06-50581

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA)	(NO. CR 05-772-DDP)
)	
Plaintiff-Appellant,)	
)	
v.)	
)	
MICHAEL TIMOTHY ARNOLD)	
)	
Defendant-Appellee.)	
_____)	

Brief for Amici Curiae

I. INTEREST OF THE AMICI CURIAE

Amici are the Association of Corporate Travel Executives (“ACTE”) and the Electronic Frontier Foundation (“EFF”).

ACTE is a not-for-profit organization dedicated to protecting the interests of business travelers worldwide through research, lobbying, and education. Founded in 1988, ACTE has approximately 2,500 members, including American citizens and citizens of foreign countries. ACTE’s headquarters are located in Alexandria, Virginia.

EFF is a nonprofit organization that works to protect civil liberties, privacy, and consumer rights in the digital age. Founded in 1990, EFF has more than

13,000 members throughout the United States. EFF's headquarters are located in San Francisco, California.

Both amici have a keen interest in the privacy rights of travelers entering and leaving the United States. In the case of ACTE, this interest derives from reports by some ACTE members that American border officials randomly searched and seized their laptop computers. ACTE's individual members have an obvious interest in protecting confidential information contained on their laptop computers. Further, ACTE and its members have an interest in the economic health and well-being of the international travel industry and therefore contest government policies that unnecessarily chill international travel.

In the case of EFF, their interest arises from their ongoing efforts to encourage and challenge government and industry to recognize the threats that new technologies pose to civil liberties and personal privacy. EFF has special familiarity with and interest in constitutional privacy issues that arise with new technologies.

Both amici believe that suspicionless searches and seizures of laptop computers at the border threaten to render meaningless the Fourth Amendment's prohibition against unreasonable searches and seizures. Amici also believe that the instant case will be crucial in protecting personal privacy, proprietary business information, privileged legal communications, and the like by delineating an

important limit to the government's authority to collect electronic information about its citizens.

II. SUMMARY OF ARGUMENT

In this appeal, the executive branch of our government seeks blanket authority to read, seize, and store all of the information retrievable from the laptop computers and other electronic devices carried by travelers who cross our national borders. In seeking this authority from the Court, the government bases its appeal on the bright-line distinction it mistakenly perceives between the government's limited authority to search an international traveler's body and its supposedly limitless authority to search and seize *anything* outside the body. *See Gov't's Opening Br. 45-46.* The government's argument is untenable, and the implications of the government's argument are great.

Amici respectfully argue that the government's position – *and current practice* – subjects innocent travelers to unconstitutionally invasive searches of their laptop computers and other electronic devices. Indeed, the government currently conducts these searches at random, without reasonable suspicion, and without regard for the constitutionally protected interests to which travelers are entitled. As the District Court correctly recognized, laptop computers are quite different from gas tanks, suitcases, and other closed containers, because laptops routinely contain vast amounts of the most personal information about people's

lives – not to mention privileged legal communications, reporters’ notes from confidential sources, trade secrets, and other privileged and valuable information.

United States v. Arnold, 454 F. Supp. 2d 999, 1003-04 (C.D. Cal. 2006).

For the reasons discussed in this brief, the unique nature of electronic information stored on laptop computers requires courts to recognize an appropriate standard that reasonably protects the privacy of our citizens. Further, the particularly invasive and unconstrained nature of these searches, as described in more detail below, invites the government to abuse its power by making an end run around the Fourth Amendment. This Court should recognize that reasonable suspicion of criminal activity is a necessary prerequisite before border agents search or seize the electronic contents of laptop computers. Amici respectfully request that the Court affirm the District Court’s ruling.

III. ARGUMENT

The government’s appeal contends that suspicionless border searches of the contents of laptop computers do not implicate the Fourth Amendment. In essence, the government argues that when an American citizen like Mr. Arnold returns home from abroad, he has the same Fourth Amendment rights in his transported property as a foreign citizen has in his property in a foreign land; in other words, he has no Fourth Amendment rights whatsoever. *See, e.g., U.S. v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (Fourth Amendment does not apply to

foreign citizens in foreign countries; *see also In re Guantanamo Detainee Cases*, 355 F. Supp. 2d 443, 458-59 (D.D.C. 2005). The government appeal invites the Court to extend this constitutional vacuum to our borders so that Customs and Border (“CBP”) agents may continue to randomly search, seize, and copy the electronic information stored on travelers’ laptop computers.

The government claims that, unless border officials are given this unchecked power, the courts will “seriously undermine the nation’s vital interest in protecting its borders” by “effectively rendering computer devices the smuggler’s container of choice for electronic contraband.” (Gov’t’s Opening Br. 16.) The government’s assertion is ridiculous. It is well-established that the Fourth Amendment protects communications between the United States and foreign countries. *See, e.g., United States v. Cavanagh*, 807 F.2d 787, 789-91 (9th Cir. 1987) (finding that FISA’s warrant requirements for monitoring communications between Americans and foreign agents satisfies the Fourth Amendment). Where the executive branch surveils such communications without cause and without complying with FISA, the government violates the Fourth Amendment. *See ACLU v. National Sec. Agency*, 438 F. Supp. 2d 754, 773-74 (E.D. Mich. 2006).

Thus, the smuggler’s so-called “container of choice” for electronic contraband is actually the internet itself. A foreign “smuggler” may simply email information into the United States to avoid a suspicionless search or, easier yet,

may simply post the information on the internet. The District Court’s ruling therefore does not undermine our “nation’s vital interest in protecting its borders” any more than FISA or the internet.

In the final analysis, the only question before the Court is whether the government, without any particularized suspicion and without any court oversight, can review the information stored on laptop computers carried across the border by international travelers. Amici believe that such searches are patently unreasonable and thus prohibited by the Fourth Amendment. Amici respectfully request that the Court deny the government’s appeal.

A. The Searches¹

Travelers who arrive in the United States from abroad know that they may be searched by border authorities. Customs and Border Protection (“CBP”) agents regularly inspect travelers’ shoes and luggage, ask routine questions, and review legal documentation. Travelers likewise have become accustomed to removing their laptop computers from carry-on bags so that agents may x-ray the computer or otherwise inspect it to ensure that it does not contain explosives or drugs.

¹ In describing these searches, amici rely on media stories, reports by their own members, and the record in the instant case. Further, the government’s appeal certainly *argues* that searches like those described herein are constitutional under the Fourth Amendment. Thus, regardless of how widespread and well-documented these suspicionless searches are, this description is relevant to the Court’s analysis. Indeed, amici believe that Mr. Arnold’s case offers a rare glimpse inside our border officials’ systematic but unchecked policy of randomly searching, seizing, and copying the contents of traveler’s laptop computers.

A border search, however, takes on an entirely different character when a CBP agent turns on a traveler's computer, opens their electronic files, and begins reviewing the contents. What is your biggest secret? Do you have any embarrassing health conditions? Have you ever had a family crisis? Often, the answers to questions like these are contained on laptop computers.

In a typical laptop search, a border agent will turn on (or instruct the traveler to turn on) the computer and then begin reviewing files on the computer. *See* Joe Sharkey, *At U.S. Borders, Laptops Have No Right to Privacy*, N.Y. TIMES, October 24, 2006, at C8 (“Sharkey I”); Joe Sharkey, *To Do List: Rename Laptop Files ‘Grandma’s Favorite Recipes’*, N.Y. TIMES, November 7, 2006, at C6 (“Sharkey II”); *see also Arnold*, 454 F. Supp. 2d at 1001. If the agents see something of interest – or even if they see nothing at all of interest – the agents may confiscate the computer and tell him or her that the computer will be returned by mail when the agents are done with it. *See* Sharkey II; Affidavit of John M. Gurley, June 18, 2007, ¶ 3, attached as Exhibit 1; *Arnold*, F.Supp.2d at 1001.

After border authorities confiscate a computer, they may copy its contents by creating a “mirror image” of the hard drive. *See* Gurley Aff. ¶ 4. Through this method, they obtain all of the contents of the computer's memory, including deleted files, files implanted unknowingly on the computer via the internet, and password-protected files. Amici currently do not know whether or how the copied

contents of seized computers are reviewed, stored, and shared with other government agencies.² *But see* Gurley Aff. ¶ 4 (explaining that in at least one instance border agents provided to the U.S. Department of Justice a mirror image of the hard drive of a traveler’s computer, where the traveler was not suspected of criminal activity). Within a week or so, border agents mail the computer back. *See id.* In some instances, however, the computers are not returned, without explanation. *See* Sharkey I.³

Although laptop searches by border agents have raised increasing concerns among businesses, individual travelers, and the media during the last year, they still come as a surprise to most travelers. *See, e.g.,* Sharkey I. Indeed, in an October 2006 survey of business travel managers, ACTE found that only six percent of the managers knew that border agents randomly search, seize, and copy the contents travelers’ computers, and only one percent had received reports from

² In November 2006, Arent Fox LLP submitted a FOIA request to the Department of Homeland Security (“DHS”) seeking information on these and other issues pertinent to this amicus brief. In February 2007, DHS provided a “partial” response to the FOIA request that contained nothing more than general DHS training materials for law enforcement officers. DHS has not provided any subsequent information pursuant to the FOIA request.

³ One possible explanation is that CBP simply “loses” some seized computers. Indeed, a recent report by the Office of the Inspector General found that CBP loses *its own* laptop computers and “has not established effective inventory management for its laptop computers.” *Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security*, OIG-07-16 at 12, 15 (December 2006).

travelers that their laptops had in fact been seized by U.S. border officials. *See* ACTE Survey Results, attached as Exhibit 2. The survey results reflect that even very experienced business travelers are completely surprised to learn that the U.S. government conducts these searches and seizures randomly. *See id.*

Further, these searches give businesses and individuals a reason not to travel across U.S. borders to conduct business, simply to protect their privacy. Some businesses will likely expend significant resources protecting confidential information from border searches, for instance by purchasing “travel computers” that do not contain any saved information. Of course, companies also incur direct costs when a border agent seizes a laptop computer during a business trip.

B. Border searches of laptop computers raise special constitutional concerns.

People have a robust and reasonable expectation in the privacy of the contents of their laptop computers. The information contained on a citizen’s laptop computers is unique in its private nature, in its nearly limitless volume, in its pervasive role in our society, and in its capacity to be quickly copied, saved, and searched. The questions raised in this appeal thus are not amenable to facile analogies with file cabinets and gas tanks. As the Fourth Amendment ensures, the American people have a right to be subjected to only reasonable searches and seizures.

In balancing this right against the government's interest in protecting our borders, the Court should recognize not only the unique nature of these searches but also the wide ranging implications of the government's arguments. Indeed, under the government's reasoning, border authorities could systematically collect all of the information contained on every laptop computer, blackberry, and other electronic device carried across our national borders by every traveler, American or foreign. The government could then store and search all of this information without justification and without oversight from the courts. Even in such an extreme situation, the Fourth Amendment, according to the government's logic, simply does not apply. If accepted, the government's argument will establish an end run around the Constitution's prohibition against unreasonable searches and seizures.

The Fourth Amendment requirement of reasonableness embodies two central principles that must be observed, even in border searches. First, the scope of searches must be minimized because “[g]eneral warrants . . . are prohibited by the Fourth Amendment.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). The concern is “not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings.” *Id.* (internal quotation marks and citation omitted); see *United States v. Ramsey*, 431 U.S. 606, 624 (1977) (permitting officers to open bulky envelopes to search for contraband, but noting that if the envelopes had

contained correspondence, a warrant would have been needed to read the correspondence); *id.* at 615-616 (limiting scope of search to confirming or denying suspicions about contraband); *United States v. Price*, 472 F.2d 573, 575 (9th Cir. 1973) (customs officials were “not entitled, on the basis of appellant’s nervousness alone, to keep looking until they found something”).

Second, there must be meaningful oversight of government searches, even when no warrant is required. The Supreme Court has relied heavily on statutory and regulatory controls on official discretion in evaluating border searches. *See, e.g., Ramsey*, 431 U.S. at 611 (noting statutory authorization); *id.* at 612 n.8 (“the opening of mail is limited by a ‘reasonable cause’ requirement, while the reading of letters is totally interdicted by regulation”). Here, however, the government’s appeal implicitly seeks authorization for general warrantless searches that will not be subject to the oversight of the courts. Moreover, the Fourth Amendment’s requirements must be observed with “scrupulous exactitude” when searches or seizures intrude upon First Amendment freedoms, as they undoubtedly do here. *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *Marcus v. Search Warrant*, 367 U.S. 717 (1961).

1. People have a reasonable expectation of privacy in the information stored on their laptop computers.

A personal computer is among a person’s most private belongings. Laptop computers are virtual extensions of the mind, used to record and share our

thoughts, feelings, and activities; indeed, “they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.” Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (“Kerr”). As a result, our laptop computers contain as much information about us as our homes contain – perhaps more.

People naturally presume the privacy of the contents of their laptop computers, iPods, and cellular telephones. Americans “undoubtedly have a high expectation of privacy in the files stored on their personal computers.” *United States v. Adjani*, 452 F.3d 1140, 1146 (9th Cir. 2006). Thus, “for most people, their computers are their most private spaces.” *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting); *United States v. Barth*, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (finding reasonable expectation of privacy in files stored on hard drive of personal computer left with computer technician for limited purpose of repairing computer); *United States v. Reyes*, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager).

People use computers to think, to learn, to communicate, and to associate with others; in so doing, computers record what we think about, what we learn, what we say to others, and whom we associate with. To treat border searches of

personal computers as merely “routine” would permit the government to arbitrarily rummage through a long history of a person’s thoughts, feelings, and activities. Accordingly, border searches of laptop computers raise fundamental constitutional questions that cannot be facilely dismissed as “routine,” or as affecting only “property,” or as relevant to only the government’s security concerns.

2. Searches of personal electronic information devices like laptop computers are particularly invasive of personal privacy.

Congress has noted that “the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.” S. Rep. No. 99-541, at 5 (1996). Thus, “[t]he question we confront today is what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy.” *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) (requiring a warrant based on probable cause for the government to search a home using sophisticated thermal imaging technology). That same question is posed here. The border search doctrine has long authorized extensive, highly discretionary searches of physical objects carried by travelers. In the past, however, these searches did not invade every domain of an individual’s life; to the contrary, the searches only affected physical items that a traveler chose to carry across the border. For example, a traveler may choose to carry extensive paper files across the border, but such situations are certainly rare; with computers, the situation is common, not

exceptional. Technology now puts massive amounts of personal and proprietary communications and information within border officials' grasp; "computer searches involve entire virtual worlds of information." Kerr, at 534. Individuals, however, value the privacy of their computers even more precisely because they embody so much of their lives.

These unique circumstances require that this Court evaluate the privacy interests inherent in laptop border searches with extreme care. *Kyllo*, 533 U.S. at 36 ("the rule we adopt must take account of more sophisticated systems that are already in use or in development."). A routine border search is more limited in scope than a non-routine border search; thus, the intrusiveness of a search is a significant factor in distinguishing routine from non-routine border searches. *United States v. Flores-Montano*, 541 U.S. at 149, 152, 154-55 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985); *id.* at 541 n.4 (declining to decide level of suspicion for "nonroutine border searches such as strip, body cavity, or involuntary x-ray searches"); *United States v. Meija*, 720 F.2d 1378, 1382 (5th Cir. 1983) ("intrusion is keyed to embarrassment, indignity, and invasion of privacy").

3. The volume of information stored on computers means that the privacy invasion of a laptop border search is enormous.

With today's technology, a government search of a laptop computer can already reveal voluminous personal information about the owner. That the

government can and does keep such information, makes the problem even more acute. Further, the invasiveness of these searches will only grow as technology advances. Professor Kerr has rightly observed:

As our computers perform more functions and preserve more data, we may eventually approach a world in which a considerable chunk of our lives is recorded and stored in perpetuity in our computers. These details may end up stored inside our machines in a way that can be reconstructed later by a forensic analyst with remarkable accuracy.

Kerr, at 569. As a result, computer searches are by their nature uniquely invasive.

See id. In essence, a search of the contents of a laptop computer is simply electronic surveillance after the fact.

As the District Court here correctly observed:

People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets.

Arnold, 454 F. Supp. 2d at 1003-04; *see also United States v. Soto-Teran*, 44 F.Supp.2d 185, 191 (E.D.N.Y. 1996) (in the border search context, “a close reading of the contents of documents could intrude on a person’s privacy since such documents could deal with very personal matters, such as a diary or desk calendar”). Thus, while the *nature* of the information on personal computers alone poses serious risks to privacy interests, the risks are magnified by the fact that “[a]

laptop and its storage devices have the potential to contain vast amounts of information.” *Arnold*, 454 F.Supp.2d at 1003. Only an extensive search of a person’s home could be expected to provide the government with as much private information about a person as a search of their laptop computer could provide.

4. Personal computers often contain information that the individual does not know about, or has even sought to erase.

As discussed above, laptop computers contain a staggering amount of information about their owners but “[c]omputers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control.” Kerr, at 542. In essence, a traveler can be searched for material that she did not know she possessed, or even deliberately sought *not* to bring across the border.

For example, files that a user has deleted normally remain on one’s computer “because marking a file as ‘deleted’ normally does not actually delete the file.” *Id.*; see also *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006). In addition, internet browsers often retain not only the internet addresses of sites visited, but actual information, both text and images, accessed during the visit, even when the user had no intent to copy such information. See Ty Howard, *Don’t Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227, 1233–34 (2004). Thus, when a border agent searches the contents of a traveler’s

computer, he can find extremely detailed information not only about the computer owner, but also about anyone else who has used the computer, and anyone with whom the owner communicated through the computer.⁴

5. Laptop computer searches are indistinguishable from “general searches.”

The Fourth Amendment’s “basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.”

Camara v. Municipal Court, 387 U.S. 523, 528 (1967); *Wolf v. Colorado*, 338 U.S. 25, 27 (1949) (“The security of one’s privacy against arbitrary intrusions by the police – which is at the core of the Fourth Amendment – is basic to a free society.”). In particular, the Fourth Amendment was directed at searches of the kind that the English Crown had practiced through “general warrants” and “writs of assistance.” *Payton v. New York*, 445 U.S. 573, 583 (1980). The Founders objected to these practices because “they provided *no judicial check* on the determination of the executing officials that the evidence available justified an intrusion into any particular home.” *Steagald v. United States*, 451 U.S. 204, 220 (1981) (emphasis added).

In *Berger v. New York*, 388 U.S. 41 (1967), the case that launched the modern constitutional treatment of communications surveillance, the Supreme Court condemned government eavesdropping precisely because it authorized

⁴ This issue is not theoretical. In businesses and even law firms, “common” laptops are used during travel by employees who normally use desktop computers.

“indiscriminate use of electronic devices” and “actually permits general searches by electronic devices.” *Id.* at 58. “By its very nature,” eavesdropping “involves an intrusion on privacy that is broad in scope.” *Id.* at 56.

A suspicionless unrestricted search of a laptop computer is simply electronic eavesdropping after the fact. As such, it is distinguishable from the forbidden general searches of Colonial times only by the technologies involved. Indeed, when the Supreme Court noted that “a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out,” *Ramsey*, 431 U.S. at 618 n.13, it cited a case famous for its condemnation of general searches. *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931) (the Framers “emphasize[d] the purpose to protect against all general searches. Since before the creation of our government, such searches have been deemed obnoxious to fundamental principles of liberty”) (citation omitted).

If this Court permits “routine” border searches of laptop computers, it will be authorizing precisely the kind of general search that the Framers rejected, albeit through technologies they could never have anticipated. In seizing and searching a laptop computer, border agents can scrutinize huge amounts of information, communications, and activities of the computer’s owner, his or her family, and his or her business. Thus:

computer technologies may allow warrants that are particular on their face to become general warrants in practice. Computers

tend to play an ever greater role in our lives as computer technologies advance, as they are likely to record and store increasingly detailed pictures of our daily experience. ... These trends suggest that as time passes, rules created to prevent general searches for physical evidence may result in the equivalent of general searches for digital evidence.

Kerr, at 565-566. This concern is amply borne out not only by this case but by other recent cases. *See, e.g., United States v. Park*, No. CR-05-375, 2007 WL 1521573 (C.D.Cal. 2007). Customs officials in fact conduct sophisticated searches of seized computers, looking at documents, deleted files, and Internet caches. *E.g., Romm*, 455 F.3d at 993; *United States v. Furukawa*, No. 06-145, 2006 WL 3330726 at *3-4 (D. Minn. Nov. 16, 2006). Thus, the laptop search at issue in this case is exactly the kind of unfocused, unwarranted, unchecked government search that the Founders sought to prohibit by passing the Fourth Amendment.

6. *There is a real risk of unconstrained “pretext” searches.*

Whenever law enforcement exercises unchecked power over its citizens, there is great risk that the government will, or will be perceived to, abuse that power. Amici are thus concerned that the government may access a traveler’s computer under the border search doctrine as a pretext for reasons unrelated to the customs laws. Border searches “made solely in the enforcement of Customs laws” must be distinguished “from other official searches made in connection with general law enforcement.” *Alexander v. United States*, 362 F.2d 379, 381 (9th Cir. 1966), *cert. denied*, 385 U.S. 977 (1966) (“Congress has in effect declared that a

search which would be ‘unreasonable’ within the meaning of the Fourth Amendment, if conducted by police officers in the ordinary case, would be a reasonable search if conducted by Customs officials in lawful pursuit of unlawful imports.”)

This Court should not allow the border search doctrine to override the rights of international travelers. One court described as “far-fetched” the possibility that “any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer ‘hard drive.’” *United States v. Ickes*, 393 F.3d 501, 50607 (4th Cir. 2005); *id.* at 507 (“Customs agents have neither the time nor the resources to search the contents of every computer.”). Unfortunately, the concern is no longer far-fetched; it has become a reality. While the government obviously does not search the contents of *every* laptop computer carried over the border, the government asserts that it may indeed search the contents of any and every one of those computers.⁵

Ultimately, of course, the constitutional question does not revolve around the number of computers that the government searches and seizes, but on the justification for its practice. Under the law the government seeks, agents would have a logical rationale for seizing and searching the contents of the laptop

⁵ As technology improves so will the governments ability to download computers and electronic media on a real-time basis.

computers carried by the family members of someone under criminal investigation, thus evading the otherwise burdensome limitations of the Fourth Amendment.

Such a search is only one example of what the government asks this Court to authorize as routine and constitutional. If the government lacks probable cause to search a traveler's laptop computer inside the United States, the government may exploit the border search doctrine by waiting until the person travels internationally. Given the frequency of international travel in the modern era, and given the commonness of laptop computers and similar electronic devices, law enforcement would naturally exploit such a loophole, if the courts permit.

Further, as Customs officials improve their ability to search computers, border searches of computers will become easier and more commonplace in the future. In short, the tremendous and ever-increasing storage capacity of modern computers may encourage the police to use border search authority to look for evidence of other types of crimes stored inside the suspect's machine.

United States v. Schoor, 597 F.2d 1303 (9th Cir. 1979), does not foreclose this argument. In *Schoor*, DEA agents who lacked probable cause to search alerted Customs officials that two passengers suspected of smuggling heroin in transistor radio shipments were en route to the United States on a flight from Thailand and requested that Customs search them, as they might be carrying narcotics. While this Court noted that “[t]he source of [customs officials’] suspicion is irrelevant in

sustaining the search,” *id.* at 1306 (citation omitted), the search in *Schoor* did not involve materials that raise the kinds of privacy concerns at issue in a search of a laptop computer. *Cf. United States v. Alfonso*, 759 F.2d 728, 737-38 (9th Cir. 1985) (“a search of the private living quarters of a ship is more intrusive than a search of other areas. . . . even in the context of a border search, the search of private living quarters on a ship should require something more than naked suspicion”).

7. The First Amendment protects many of the contents on laptop computers.

The First Amendment imposes special constraints on searches for and seizures of presumptively protected material, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979), and requires that the Fourth Amendment be applied with "scrupulous exactitude" in such circumstances. *Stanford*, 379 U.S. at 485. Consequently, the Court has imposed particularized rules applicable to searches for and seizures of allegedly obscene films, books, and papers. *See, e.g., Roaden v. Kentucky*, 413 U.S. 496, 497 (1973) ("seizure of allegedly obscene material, contemporaneous with and as an incident to an arrest for the public exhibition of such material . . . may [not] be accomplished without a warrant"). These rules, moreover, must be understood as protecting not only the defendant in this case but the public at large. *See Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972).

In addition, the First Amendment implications of these searches undermine the government's attempt to define laptop computers as ordinary closed containers. Indeed, in *Heidy v. U.S. Customs Service*, 681 F. Supp. 1445 (C.D. Cal. 1988), the district court explained that “[b]order search cases relaxing fourth amendment standards solely for the purpose of facilitating detection of physical objects sought to be imported unlawfully therefore are inapposite to this [informational] case.” *Id.* at 1450 (footnote omitted). Thus, “limited reading or perusal of writing that appears on objects sought to be imported inevitably may be required for the purpose of identifying the objects themselves,” but “a reading for the purpose of revealing the *intellectual content* of the writing requires encroachment upon first amendment protections far beyond the mere search and seizure of materials.” *Id.* This case involves the intellectual content of laptop computers. As soon as border agents cease looking for physical contraband inside a computer and instead begin reviewing the electronic files on the computer, they cross an important constitutional threshold.

a. Personal computers are critical to private communication.

Private communications are generally protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 352 (1967). While physical entry of the home was the Framers' main concern, after *Katz* the “broader spirit” of the Fourth Amendment “now shields private speech from unreasonable surveillance.” *United*

States v. U.S. Dist. Ct., 407 U.S. 297, 313 (1972) (*Keith*) (“the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.”) (footnote omitted). Along with *Berger*, *Katz* reinforced the Fourth Amendment’s concern for the sanctity of personal communications.

Katz also made clear that constitutional protections must evolve with modern technology and social practices. In rejecting a pure “trespass” approach to the Fourth Amendment that would have denied protection to telephone communications, the Supreme Court explained: “To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.” *Katz*, 389 U.S. at 352. The same values and logic underlie the district court’s correct decision here. The personal computer (and other modern electronic devices) is central to private communication today. Under *Katz* and its progeny, border searches of laptop computers cannot be routine; to do so would ignore the personal computer’s “vital role.”

Personal computers and many other types of personal devices are frequently used not only to communicate with others via email, instant messenger services, blogs, chat rooms, and bulletin boards, but also simply to read information from the Internet, a new and powerful medium of expression that covers a range of topics “as diverse as human thought.” *Reno v. ACLU*, 521 U.S. 844, 852 (1997); *id.*

at 863 (Internet “is the most participatory form of mass speech yet developed, entitled to the highest protection from governmental intrusion.”) (internal citations omitted).

This protection is not limited to the contents of a person’s writings or communications; it extends as well to his or her identity and the identity of his or her correspondents. In the modern context, it includes knowledge about a person’s interests, the websites he or she reads, and the electronic files that he or she downloads. “Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (citation omitted).

b. Indiscriminate searches of information stored on laptop computers will chill speech.

The Supreme Court has long been vigilant about the potential for overreaching governmental power to chill speech. “It is characteristic of the freedoms of expression in general that they are vulnerable to gravely damaging yet barely visible encroachments.” *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963). The danger of unauthorized official surveillance parallels the danger of official censorship, which lies “not merely [in] the sporadic abuse of power by the

“censor but the pervasive threat inherent in its very existence.” *Thornhill v. Alabama*, 310 U.S. 88, 97 (1940).

This concern links the First and Fourth Amendments. Indeed, the Framers adopted the Bill of Rights “against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression. *Marcus*, 367 U.S. at 729. Surveillance of private communications therefore poses a grave danger to free 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.” *Keith*, 407 U.S. at 314. Thus, “fear of unauthorized official eavesdropping” may “deter vigorous citizen dissent and discussion of Government action in private conversation.” *Id.* at 314.

This danger inheres in suspicionless border searches of travelers’ laptops, especially given that the Customs Service is authorized to block the importation of “any book, pamphlet, paper, writing, advertisement, circular, print, picture, or drawing containing any matter advocating or urging treason or insurrection against the United States, or forcible resistance to any law of the United States.” 19 U.S.C. § 1305; *see Heidi*, 681 F. Supp. at 1450-51 (where Customs targeted materials regarding political dissent, “no dispute that the reading of the materials in

question and the creation and retention of the Records of Non-Violation ‘chill’ Plaintiffs’ rights of expression”).

c. Any rule permitting border searches of computers must ensure reasonable particularity, minimization and oversight.

The usual Fourth Amendment mechanism for protecting privacy is prior judicial authorization based on probable cause and specifying the scope of the search with particularity. In *Katz*, the Supreme Court explained that “bypassing a neutral determination of the scope of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police.” *Katz*, 389 U.S. at 358-359 (internal quotation and citation omitted); *Keith*, 407 U.S. at 318 (“post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.”) (citation omitted).

Accordingly, the Supreme Court has often relied on the judicial check when it permitted searches with a significant nexus to First Amendment material. *Andresen*, 427 U.S. 463, 482 n.11 (1976) (“In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are . . . among those papers authorized to be seized. Similar dangers . . . are present in executing a warrant for the ‘seizure’ of telephone conversations. In both kinds of searches, responsible officials . . . must

take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.”).

When there is no judicial check, as in the border search doctrine, the only avenue of restraint is clear and objective statutory or regulatory standards. For example, *Ramsey* clearly recognized that unconstrained border searches would chill speech. Although *Ramsey* found that border searches of international mailed letters did not chill speech, it expressly limited that finding to “the existing system of border searches,” which plainly required “‘reasonable cause to believe’ the customs laws are being violated prior to the opening of envelopes” and “flatly prohibit[ed], under all circumstances, the reading of correspondence absent a search warrant.” 431 U.S. at 623. *Ramsey* thus avoided the First Amendment issue based on “the existing statutory and regulatory protection.” *Id.* at 624 (footnote omitted).

Clearly, the reasonableness of a border search, at least where expression is involved, depends on legal constraints on official discretion. *Cf. Flores-Montano*, at 159 (Breyer, J., concurring) (“Customs keeps track of the border searches its agents conduct, including the reasons for the searches. This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner.”) (internal citation omitted); *see Heidi*, 681 F. Supp. at 1453 (rejecting Customs “Policy Directives” regarding searches of records of travelers’

expressional materials as “constitutionally impermissible” because of “chilling effect of this risk upon the exercise of first amendment rights of law-abiding citizens”).

In this situation, by contrast, there is no accountability mechanism or carefully drawn policy to protect privacy or First Amendment rights, either for Mr. Arnold’s computer or for the border searches of travelers’ computers generally. *Arnold*, 454 F. Supp. 2d at 1004 (“the government has not provided the Court with any record of the search that was completed at or near the time of the incident”).

IV. CONCLUSION

It is clear from the above discussion that the government’s appeal downplays the constitutional concerns raised when border agents randomly search and seize laptop computers from international travelers. The government’s appeal likewise fails to acknowledge the logical end of its argument; the government ultimately assumes that the Fourth Amendment prohibits the federal courts from offering any constitutional oversight of border searches and seizures that do not involve the human body. In so arguing, the government fails to accord personal privacy the constitutional value it was given by the Framers.

In closing, amici emphasize that the District Court here required *only* reasonable suspicion of a crime before border agents may properly search the contents of a traveler’s computer. Amici, like all Americans, greatly value secure

national borders, but also urge the Court to require that our borders be policed reasonably. Random suspicionless searches and seizures of laptop computer simply do not square with the Fourth Amendment's mandate of reasonableness. Amici respectfully request that the Court affirm the ruling below.

Respectfully Submitted,

RANDALL BRATER
Arent Fox LLP
1050 Connecticut Ave., N.W.
Washington, D.C. 20036
202-857-6000

Of Counsel:

JOHN M. GURLEY
TIMOTHY P. KANE
Arent Fox LLP
1050 Connecticut Ave., N.W.
Washington, D.C. 20036
202-857-6000

Attorneys for Amici Curiae

Exhibit 1

No. 06-50581

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

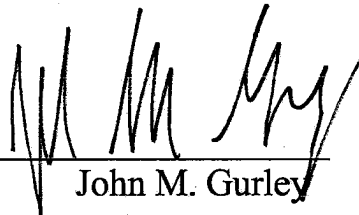
UNITED STATES OF AMERICA) (NO. CR 05-772-DDP)
)
Plaintiff-Appellant,)
)
v.)
)
MICHAEL TIMOTHY ARNOLD)
)
Defendant-Appellee.)
_____)

AFFIDAVIT OF JOHN M. GURLEY

JOHN M. GURLEY, being duly sworn, deposes and says:

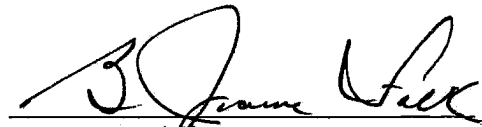
1. I am over 18 years of age, and I am competent to testify about the matters stated in this Affidavit. I make these statements from my own personal knowledge.
2. I am a partner at the law firm of Arent Fox LLP in Washington, D.C.
3. During September 2006, the son of a client told me that Customs and Border Patrol agents had seized his laptop computer at the Newark International Airport, without explanation. After about a week, the government returned the laptop computer by mail.
4. A few weeks later, a federal prosecutor at the U.S. Department of Justice contacted me and asked me for my client's son's consent for the Department

of Justice to review the contents of a copy of the seized computer's hard drive. The prosecutor stated that it was the belief of the Department of Justice that they could review the contents without consent, but that the Department of Justice nonetheless was seeking consent in order to avoid any legal issues in the future. The prosecutor also assured me the client's son was not under criminal investigation.



John M. Gurley

Subscribed and sworn to before me the 18th day of June, 2007.



Notary Public

My commission expires: 6-18-07.

B. Joanna Falk
District of Columbia
My Commission Expires:
March 31, 2010

Exhibit 2



ASSOCIATION OF
CORPORATE TRAVEL
EXECUTIVES

Association of Corporate Travel Executives October 2006 Lap Top Survey

Two hundred business travel managers were polled; 155 responded.

1) Are you aware that the U.S. Government – Customs and Border Protection (CBP) – takes the position that its agency may examine the contents of your laptop hard drive and other electronic media as part of their routine searches of travelers arriving in the U.S. from abroad?

87 percent: No
13 percent: Yes

2) Did you know that American and other international business travelers have had their laptops confiscated for several days by the CBP and that the CBP makes copies of the hard drives before returning the computers to their owners.

94 percent: No
6 percent: Yes

3) Have you ever had a traveler report that their laptop was confiscated by U.S. Customs or the Border Patrol.

99 percent: No
1 percent: Yes

4) Does your company currently have a policy regarding the sensitivity or proprietary nature of corporate information carried out of the country on laptops?

36 percent: No
35 percent: yes
29 percent: "looking into it"

5) Are you less likely to carry confidential business or personal information on your laptop on international trips given that the U.S. Government has in fact seized and copied American and international business traveler's computers?

86 percent: Yes
14 percent: No

The Association of Corporate Travel Executives (ACTE) is a not-for-profit association established by business travel managers in 1988 to provide meaningful education and networking opportunities. ACTE recognizes the interdependence between corporate travel purchasers and corporate travel suppliers and accords both sectors equal membership. ACTE's membership spans all sectors of business travel, from corporate buyers to agencies to suppliers in 50 countries.