

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 APPELLEE'S PETITION
FOR REHEARING EN BANC**

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	5
B. BORDER SEARCHES OF LAPTOP COMPUTERS RAISE SPECIAL CONSTITUTIONAL CONCERNS	9
CONCLUSION	18

TABLE OF AUTHORITIES

	<u>Page(s)</u>
FEDERAL CASES	
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976)	8
<i>Arizona v. Hicks</i> , 480 U.S. 321, 324 (1987)	4
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	14
<i>Camara v. Municipal Court</i> , 387 U.S. 523 (1967)	13
<i>Go-Bart Importing Co. v. United States</i> , 282 U.S. 344 (1931)	14
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	15-16, 17
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	10-11
<i>Maryland v. Macon</i> , 472 U.S. 463, 469 (1985)	4
<i>Payton v. New York</i> , 445 U.S. 573 (1980)	13-14
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997)	16
<i>Steagald v. United States</i> , 451 U.S. 204 (1981)	14
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006)	9
<i>United States v. Arnold</i> , 523 F.3d 941 (9th Cir. 2008)	passim
<i>United States v. Arnold</i> , 454 F. Supp. 2d 999 (C.D. Cal. 2006)	passim
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004)	11
<i>United States v. Furukawa</i> , No. 06-145, 2006 WL 3330726 (D. Minn. 2006)	15
<i>Unites States v. Giberson</i> , ___ F.3d ___, No. 07-10100, 2008 WL 2221008 (9th Cir. 2008)	8

<i>Unites States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006) (en banc)	9
<i>United States v. Meija</i> , 720 F.2d 1378 (5th Cir. 1983)	11
<i>United States v. Park</i> , No. CR-05-375, 2007 WL 1521573 (C.D.Cal. 2007)	15
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977)	passim
<i>United States v. Romm</i> , 455 F.3d 990 (9th Cir. 2006)	13, 15
<i>United States v. Soto-Teran</i> , 44 F.Supp.2d 185 (E.D.N.Y. 1996)	12
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990)	4
<i>United States v. U.S. Dist. Ct.</i> , 407 U.S. 297 (1972)	15, 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)	13
Orin Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531, 569 (2005)	passim
Ellen Nakashima, <i>Clarity Sought on Electronics Searches; U.S. Agents Seize Travelers' Devices</i> , THE WASHINGTON POST, February 7, 2008	6
S. Rep. No. 99-541, at 5 (1996)	10
Joe Sharkey, <i>At U.S. Borders, Laptops Have No Right to Privacy</i> , N.Y. TIMES, October 24, 2006	5-6
Joe Sharkey, <i>To Do List: Rename Laptop Files 'Grandma's Favorite Recipes'</i> , N.Y. TIMES, November 7, 2006	5-6

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.)	
<hr/>		

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 and foreign citizens. ACTE’s headquarters are 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 in 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 its members' reports that American border officials randomly search and seize their laptop computers. ACTE's members have an obvious interest in protecting their confidential information from government intrusion. Further, ACTE has an interest in the economic well-being of the international travel industry and therefore contests government policies that unnecessarily chill international travel.

EFF's interest arises from its ongoing efforts to encourage and challenge government and industry to recognize the threats new technologies pose to civil liberties and personal privacy. EFF has a unique interest in constitutional privacy issues that arise with new technologies.

Both amici believe that suspicionless searches and seizures of laptop computers at the border render meaningless the Fourth Amendment's prohibition against unreasonable searches and seizures. Amici believe that rehearing en banc and reversal of the panel's decision are necessary to protect personal privacy, proprietary business information, privileged legal communications, and the like by limiting the government's otherwise unconstrained power to collect electronic information about its citizens.

II. SUMMARY OF ARGUMENT

The panel's decision grants the government blanket power to review, seize, and store all of the information contained on laptop computers and other electronic devices carried by travelers who cross our national borders. *See United States v. Arnold*, 523 F.3d 941, 946 (9th Cir. 2008). The panel failed to recognize the difference between physical searches that incidentally reveal personal information – flipping through the pages of a diary or opening an envelope – and searches like those at issue here whose only purpose is to review and collect private information stored on travelers' computers. The panel's analysis was superficial and misguided, and the implications of its decision are great.

As the District Court correctly recognized, computers are 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 information. *United States v. Arnold*, 454 F. Supp. 2d 999, 1003-04 (C.D. Cal. 2006). Indeed, unlike other closed containers, a functioning computer is not a means for smuggling physical contraband and the searches at issue here do not help agents find physical contraband.

The unique nature of electronic information stored on laptop computers requires courts to recognize a standard that reasonably protects privacy in the

Information Age. Further, the particularly invasive and unconstrained nature of these searches threatens to create an end run around the Fourth Amendment.

Because the panel failed to recognize that the Fourth Amendment compels at least reasonable suspicion of criminal activity before border agents search and seize¹ the information stored on laptop computers, amici respectfully urge rehearing en banc.

III. ARGUMENT

In essence, the panel ruled that when an American citizens return home from abroad, they have the same Fourth Amendment rights in information stored on their laptop computers as a foreign citizen has in property in a foreign land; in other words, they have no Fourth Amendment rights at all. *See U.S. v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (Fourth Amendment does not apply to foreign citizens in foreign countries). The decision extends this constitutional vacuum to our borders so that Customs and Border (“CBP”) agents may continue to randomly search and seize electronic information stored on laptop computers. *See Arnold*, 523 F.3d at 946-47.

¹ Amici believe that when the government copies information stored on electronic devices, it *seizes* that information, as distinct from searching the device. Seizure is traditionally defined as that which “meaningfully interfere[s]” with a “possessory interest.” *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) (quoting *Maryland v. Macon*, 472 U.S. 463, 469 (1985)). Thus, the traveler’s possessory interest here is infringed by government copying, in addition to the privacy interest infringed by visual inspection.

A. The Searches

Travelers arriving in the United States from abroad expect to be searched by border authorities. CBP agents regularly inspect shoes and luggage, ask routine questions, and review legal documentation. Travelers likewise are accustomed to removing their laptop computers from carry-on bags so that agents may x-ray or otherwise inspect the computer to ensure that it does not contain contraband.

A border search, however, takes on an entirely different character when agents review and collect information from a traveler's computer. In a typical laptop search,² an agent will turn on (or instruct the traveler to turn on) the computer and then begin opening and reviewing files. *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 of interest – they may confiscate the computer and tell the traveler that the computer will be returned by mail when the government is done with it. *See* Sharkey II; Affidavit of John M. Gurley, June 18, 2007, ¶ 3, attached

² In describing these searches, amici rely on media stories, reports by their own members, and the record in the instant case. Amici believe that Mr. Arnold's case offers a rare glimpse inside our border officials' systematic but unchecked policy of randomly searching and seizing the contents of travelers' laptop computers.

as Exhibit 1; Ellen Nakashima, *Clarity Sought on Electronics Searches; U.S. Agents Seize Travelers' Devices*, THE WASHINGTON POST, February 7, 2008, at A1.

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 proprietary business information, privileged legal communications, deleted files, and password-protected files. In some instances, border agents provide copies of the computer’s contents to the U.S. Department of Justice, even where the traveler is not suspected of criminal activity. *See Gurley Aff.* ¶ 4. Within a week or so, border agents mail the computer back to the traveler. *See id.* Sometimes, however, the computers are not returned, without explanation. *See Sharkey I.*

Although laptop searches by border agents have raised increasing concerns among businesses during the last two years, they still come as a shock to most business travelers. *See Sharkey I.* 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 of travelers’ computers. *See ACTE Survey Results*, attached as Exhibit 2. The survey results reflect that even experienced business travelers are completely unprepared when the government seizes their computers. *See id.* The seizures ruin business trips, force companies to incur significant expense, and threaten the secrecy of confidential information.

Further, these random searches give businesses and individuals a reason not to travel across U.S. borders to conduct business, and they force businesses to expend significant resources protecting confidential information.

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

Business travelers, like all citizens, have a robust and reasonable expectation in the confidentiality of information stored on their laptop computers. That information 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 case thus are not amenable to the panel's facile analogies with luggage and gas tanks. *See Arnold*, 523 F.3d at 947.

The Fourth Amendment ensures that Americans 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 panel failed to recognize not only the unique nature of these searches but also the wide ranging implications of its holding. Indeed, under the panel's decision, border authorities now may 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 then may store and search all of this information without justification and without oversight from any court. Even in such an extreme situation, the Fourth Amendment, according to the

panel's reasoning, does not apply. If left undisturbed, the decision will establish an end run around the Constitution's prohibition against unreasonable searches.³

The Fourth Amendment reasonableness requirement embodies two central principles that must be observed, even at the border. 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 agents to open bulky envelopes to search for contraband, but noting that if the envelopes contained correspondence, a warrant would be needed to read the correspondence).

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 612 n.8 (“the opening of mail is limited by a ‘reasonable cause’ requirement, while the reading of letters is totally interdicted by

³ *United States v. Giberson*, ___ F.3d ___, No. 07-10100, 2008 WL 2221008 (9th Cir. May 30, 2008), does not support the panel's decision. In *Giberson*, the police obtained search warrants for the defendant's home and, later, for his computer in connection with an investigation of fake government identification cards. 2008 WL 2221008 at *1-2. In executing the latter warrant, law enforcement discovered child pornography on defendant's computer. *Id.* Those circumstances are entirely distinguishable from the circumstances here, where the government searches the files on travelers' computers without any warrant and without any suspicion.

regulation”). Here, however, the panel’s decision authorizes general warrantless searches of personal information, and those searches are not subject to court oversight and are not subject to any limiting regulations.

1. Citizens have a reasonable expectation of privacy in 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”).

People naturally presume the privacy of the contents of their computers and other electronic devices. Indeed, this Court recognizes that citizens “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).

People use computers to think, learn, communicate, and associate with others; in so doing, computers record what we think about, what we learn, what we say to others, and with whom we associate. Accordingly, border searches of laptop computers raise fundamental constitutional questions that cannot be facilely

dismissed as affecting only “property” or “closed containers” 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 found 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 (1986) (discussing the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508). Thus, the vital question “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). The border search doctrine has long authorized extensive, highly discretionary searches of physical objects carried by travelers. In the past, 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. Technology, however, now puts massive amounts of confidential communications and privileged information within border officials’ grasp. Thus, “computer searches involve entire virtual worlds of information.” Kerr, at 534. Individuals accordingly value the privacy of their computers even more because they embody so much of their lives.

These unique circumstances require that this Court reevaluate the privacy interests inherent in laptop border searches. *See 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.”). Indeed, the intrusiveness of a search is a significant factor in determining the constitutionality of a border search. *United States v. Flores-Montano*, 541 U.S. at 149, 152, 154-55 (2004); *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 reveal voluminous confidential information about the owner. That the government can and does keep such information makes the problem even more acute. *See Gurley Aff.* ¶ 4. 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.

Kerr, at 569. As a result, computer searches are uniquely invasive. *See id.* In essence, a search of the contents of a laptop computer achieves electronic surveillance of a person’s life.

As the District Court correctly stated:

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

Unlike luggage that travelers pack for a trip, laptop computers are “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, even files that a user has deleted 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 websites 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 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.

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). In particular, the Fourth Amendment was directed at searches 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 “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) (“Since before the creation of our government, [general] searches have been deemed obnoxious to fundamental principles of liberty”) (citation omitted).

In authorizing random suspicionless searches of laptop computers, the panel authorized precisely the kind of general search the Framers rejected, albeit through technologies they never anticipated. 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). Unlike this case, however, customs officials in other cases usually had reasonable suspicion to 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).

6. *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); *Ramsey*, 431 U.S. at 623 (recognizing constitutional concerns raised by border searches of postal mail). Given that laptop computers and

cellphones typically contain email and messages constitutionally indistinguishable from postal mail, the panel decision's conflict with *Ramsey* is clear.

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, the government may not conduct unchecked border searches of laptop computers. The panel's decision to the contrary ignores the personal computer's "vital role."

Indeed, personal computers and other electronic devices are 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, 863 (1997) (the internet "is the most participatory form of mass speech yet developed, entitled to the highest protection from governmental intrusion.") (citations omitted). This protection is

not limited to the contents of citizens' communications; it extends as well to their identity, the identity of their correspondents, and their interests, including the websites they read and the electronic files they download.

7. 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.” 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).

When there is no judicial check, the only avenue of restraint is clear and objective statutory or regulatory standards. For example, *Ramsey* recognized that unconstrained border searches would chill speech but found that border searches of international mailed letters did not chill speech because “the existing system of border searches,” 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 Constitutional issue based on the existing statutory and regulatory protections. *Id.* at 624.

In this situation, by contrast, there is no regulation which constrains the government to act within constitutional bounds, and there is no accountability mechanism to monitor the government's conduct. *See 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"). As such, in the absence of a reasonable suspicion standard, the government will have *carte blanche* to collect information stored on travelers' computers.

IV. CONCLUSION

It is clear from the above discussion that the panel decision failed to appreciate the constitutional concerns raised when border agents randomly search and seize laptop computers from international travelers. The decision likewise failed to acknowledge the logical end of its argument – that under the Fourth Amendment, federal courts may not conduct any oversight of border searches and seizures that do not involve the human body. In so arguing, the decision 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 order rehearing en banc.

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

CERTIFICATE OF COMPLIANCE WITH FRAP 32 AND CIRCUIT RULE 29-2

Pursuant to Circuit Rule 29-2(a), I hereby certify that all parties have consented to the filing of this amicus brief.

Pursuant to Federal Rule of Appellate Procedure 32(a), I hereby certify that the foregoing brief uses 14 point Times New Roman spaced type and the text is proportionally spaced. This brief complies with the type-volume limitations of Circuit Rule 29-2(c)(2) as it is 4,135 words.

Dated: June 10, 2008

A handwritten signature in black ink, appearing to read "Randall Brater", written over a horizontal line.

RANDALL BRATER

Attorney for Amici Curiae

Exhibit 1

No. 06-50581

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

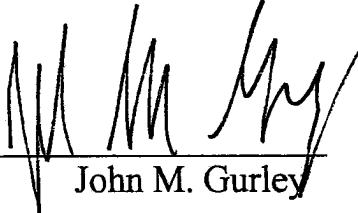
UNITED STATES OF AMERICA) (NO. CR 05-772-DDP)
)
Plaintiff-Appellant,)
)
v.)
)
MICHAEL TIMOTHY ARNOLD)
)
Defendant-Appellee.)
_____)

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.

CERTIFICATE OF SERVICE

I hereby certify that on this 11th day of June 2008, I caused the foregoing Brief for Amici Curiae in Support of Appellee's Petition for Rehearing En Banc to be served by overnight delivery, postage prepaid, upon the following:

Clerk, Appeals Section
United States District Court
312 North Spring Street
Los Angeles, CA 90012

Michael Rafael
Chief Criminal Appeals
312 North Spring Street, 10th Floor
Los Angeles, CA 90012

Marilyn Bednarski
Kaye, McLane & Bednarski, LLP
128 N. Fair Oaks Ave.
Pasadena, CA 91103



TIMOTHY P. KANE