Brooklyn Law Review

Volume 78
Issue 2
SYMPOSIUM
Post Zoning: Alternative Forms of Public Land Use Controls

Article 13

2013

The Sky's the Limit: The Border Search Doctrine and Cloud Computing

Nicolette Lotrionte

The Sky's the Limit

THE BORDER SEARCH DOCTRINE AND CLOUD COMPUTING

INTRODUCTION

Imagine you take a spontaneous trip across the border to Canada, just for the night. You leave early the next morning to return to the United States, but on the way back, agents stop you at the border. You show them your passport, you answer their questions, and you do not have a criminal background. Yet, they search your car, look through your bags, and seize your smartphone and wireless tablet. Then, you wait. You may wait a few minutes or several hours. You may even return to the United States without your gadgets, which will be returned to you in several days.[1] While this might all seem unfair, border officials are nevertheless free to seize and search electronics as they please.[2]

Now, what if border agents were to stop and search not *you* but rather a sex offender returning from a trip to Asia, where he loaded his laptop full of files of photographs and videos of nude children?[3] Or what if the person stopped and searched had bookmarked a Google Doc,[4] which contained

---

[1] A simple search online reveals these types of border searches are not uncommon. *See, e.g.*, Katie Johnston, *Laptop Seizures at Customs Cause Thorny Legal Dispute*, BOS. GLOBE (Jan. 8, 2012), http://articles.boston.com/2012-01-08/business/30601167_1_laptops-search-and-seizure-strip-searches (describing the experience of a man who took his laptop to Mexico to get work done and had it seized and held for two months at the Mexico-U.S. border while it was searched); Jane McLean, *Readers Respond: Border Crossing Stories*, ABOUT.COM, http://gocanada.about.com/u/ua/faqscrossingtheborde1/Border-Crossing-Horror-Stories-Share-Your-Border-Crossing-Horror-Stories.02.htm (last visited Sept. 16, 2012) (compiling readers' comments about their experiences at the Canadian-U.S. border, mostly with regard to Canadian border officials).

[2] Specifically, law enforcement at the border is able to search people and property at the border without a warrant, probable cause, or suspicion. *See infra* Part II. Several U.S. Courts of Appeals have expanded this power to data on electronic devices. *See infra* Part II.A.

[3] *See, e.g.*, United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008) (one of many cases where, upon returning from Asia—in Arnold's case, the Philippines—American border officials discovered child pornography during a search of a traveler's computer).

[4] Google Docs is a "Web-based word process[or]" that enables instant sharing and storing of documents, presentations, or spreadsheets, which anyone in the group

information about Improvised Explosive Devices and "jihadist material"?[5] These kinds of searches have become more common in recent years. In fact, government officials searched the electronic devices of more than 6500 people crossing the U.S. border "between October 2008 and June 2010."[6] These devices ranged from laptops to cellular phones and from external hard drives to flash drives.[7] By far, the device that officials searched most frequently was the cellular phone.[8] Moreover, as a result of these searches, law enforcement might use the files they discover as a basis for arresting or excluding these individuals from the United States.[9]

Although the Fourth Amendment protects "against unreasonable search and seizures,"[10] the Department of Homeland Security (DHS) has given U.S. officials broad discretion to conduct warrantless searches at the border.[11] In August 2009, the agencies of Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE) both issued directives that clarified what exactly this generalized power entails.[12] Both directives permit border agents to inspect

---

using the document can edit from any Internet-capable device. *Using Google Docs in the Classroom: Simple as ABC*, GOOGLE.COM, https://docs.google.com/View?docid=dcdn7mjg_72nh25vq (last visited Sept. 16, 2012).

[5] *See Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Const. of the S. Comm. on the Judiciary*, 110th Cong. 2 (2008) [hereinafter *S. Comm. Hearing on Laptop Searches and Overseas Travel*] (statement of Jayson P. Ahern, Deputy Comm'r, U.S. Customs & Border Protection), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg45091/html/CHRG-110shrg45091.htm.

[6] *Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices*, ACLU.ORG (Aug. 25, 2010), http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr [hereinafter ACLU, *Government Data*].

[7] *Id.*

[8] *Id.* During a "nine month period" in 2008, CBP "searched and seized 1,644 electronic devices." Hugo Martin, *No Curbs on Border Searches of Cellphones, Laptops*, SEATTLE TIMES (Feb. 27, 2010), http://seattletimes.nwsource.com/html/travel/2011177028_trbordersearches28.html. Of these devices, "582 were cellphones, 398 were laptop computers and 259 were digital cameras. The rest included MP3 players, flash drives, hard drives, DVDs and other devices." *Id.*

[9] The discovery of "[t]hese materials have led to the refusal [of] admission and the removal of these dangerous people from the United States." *S. Comm. Hearing on Laptop Searches and Overseas Travel*, *supra* note 5.

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

[11] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES (2009) [hereinafter DHS PRIVACY IMPACT ASSESSMENT], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

[12] *See generally* U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009) [hereinafter CBP DIRECTIVE], *available at* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/elec_mbsa.ctt/elec_mbsa.pdf; U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, ICE DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES (2009) [hereinafter

electronic devices, such as laptops and cellular phones, and examine the information on those devices without any "individualized suspicion."[13]

The CBP and ICE derive their authority to conduct these inspections from their respective missions to "interdict" and "investigate violations of federal law at and related to the Nation's borders."[14] DHS has identified electronic storage of data "as the latest method of smuggling . . . material" related to criminal activity into the United States.[15] Thus, a motivating reason for allowing such broad latitude to search people and their property at the border lies in preventing illegal activities, such as "child pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); . . . [and] violations of immigration law," as well as enforcing national security laws, preventing terrorism, and protecting vulnerable infrastructure from potential security threats.[16]

Nevertheless, opponents of border searches argue that electronic devices contain much more information than briefcases or luggage, which have historically been searched at the border.[17] Whereas in the past, a briefcase might have contained work materials, notes, and some personal information, the current availability, portability, and ease of electronic storage means that travelers can carry "exponentially" more private information with them at any given time.[18] As such, opponents argue that the potential invasion of privacy[19] during

---

ICE DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

[13] CBP DIRECTIVE, *supra* note 12, § 5.1.2; ICE DIRECTIVE, *supra* note 12, § 6.1.

[14] DHS PRIVACY IMPACT ASSESSMENT, *supra* note 11, at 2.

[15] *Id.*

[16] *Id.* at 4.

[17] THE CONSTITUTION PROJECT, SUSPICIONLESS BORDER SEARCHES OF ELECTRONIC DEVICES: LEGAL AND PRIVACY CONCERNS WITH THE DEPARTMENT OF HOMELAND SECURITY'S POLICY 1-2 (2011).

[18] DHS PRIVACY IMPACT ASSESSMENT, *supra* note 11, at 2. Nonetheless, as Professor Nathan Alexander Sales pointed out, typical container ships carry between 5000 and 11,000 twenty-foot cargo containers, yet these container ships have always been subjected to suspicionless border searches. Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1111 (2009).

[19] For example, in 2010, the ACLU, New York Civil Liberties Union, and the National Association of Criminal Defense Lawyers filed a lawsuit on behalf of the National Press Photographers Association and Pascal Abidor, a French-American citizen, challenging DHS's electronic border search policy. Abidor was crossing the Canada-America border by train when customs officers searched and confiscated his laptop. His laptop was returned eleven days later, and there was evidence that personal files, such as photographs and chats with his girlfriend, had been searched.

border searches of electronic devices is far greater than during border searches of nonelectronic items.[20] For example, attorneys, doctors, accountants,[21] and journalists might travel across borders with computers and other electronic devices that contain privileged attorney-client, doctor-patient, or confidential-source information.[22] Nevertheless, one might also argue that briefcases of such professionals—which have always been subject to suspicionless border searches[23]—would also contain sensitive materials. Therefore, other commentators contend that "[l]aptop searches are not unique in their ability to reveal sensitive, personal information."[24] They base this rationale on a history of border searches that has revealed sensitive information, such as situations where border officials have opened a sealed letter within a package,[25] looked through photo albums found within a vehicle,[26] and opened a sealed envelope found within a briefcase.[27]

The latest phenomenon in the computing world is the virtualization of computing services—that is, shifting data and services from local servers and hard drives to third-party

---

ACLU in Federal Court Today Challenging Government's Searches of Laptops at Border, ACLU.ORG (July 8, 2011), http://www.aclu.org/technology-and-liberty/aclu-federal-court-today-challenging-governments-searches-laptops-border.

[20] THE CONSTITUTION PROJECT, *supra* note 17, at 1.

[21] Although, in the past, these professionals might have carried privileged or private information in their briefcase, data storage on electronic devices and on the cloud enable individuals to indirectly transport significantly more information. For instance, an article in the American Institute of CPAs' Journal of Accountancy describes CPA firms' transition to electronic storage of data:

> When we were doing the evaluation of the late 1990s, we had massive file rooms to hold all of our tax files and audit workpaper files. If you go into a firm or a business today, we don't have file rooms. The file room is on a computer that is the size of a small toaster. It's amazing—that transition from hard copy to electronic data . . . .

Kim Nilsen, *Moving the Needle*, J. ACCT. (Nov. 2011), http://www.journalofaccountancy.com/Issues/2011/Nov/20114396. Although the computer referred to is not necessarily connected to the cloud, companies are beginning to transition from storing hard copies of files to electronic storage, including electronic storage on third party servers. If a traveler has access to these servers on their wireless devices and a search is conducted, all of these files could potentially be viewed.

[22] For example, border agents impounded the laptop of Bill Hogan, a freelance journalist, upon his return to the United States from Germany. Fortunately, Hogan did not use his laptop for work; however, if he did then he would need to inform sources that the government had their information. Alex Kingsbury, *Seizing Laptops and Cameras Without Cause*, U.S. NEWS (June 24, 2008), http://www.usnews.com/news/national/articles/2008/06/24/seizing-laptops-and-cameras-without-cause.

[23] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[24] Sales, *supra* note 18, at 1115.

[25] United States v. Seljan, 497 F.3d 1035, 1040-41 (9th Cir. 2007), *reh'g en banc granted*, 512 F.3d 1203 (9th Cir. 2008).

[26] United States v. Ickes, 393 F.3d 501, 502-03 (4th Cir. 2005).

[27] United States v. Soto-Teran, 44 F. Supp. 2d 185, 189-92 (E.D.N.Y. 1996).

servers that users can access from anywhere.[28] Software developers, businesses, and private individuals all around the world are beginning to use these virtual servers—known as the *cloud*—and the services they provide.[29] Cloud computing generally embodies "computing services offered by a third party, available for use when needed, that can be scaled dynamically in response to changing needs."[30] Cloud users save and share their information on remote servers, which third parties own and operate and users access through the Internet.[31] Any information or programs that can be stored on a computer's local hard drive can also be stored on these remote servers.[32] Cloud computing was first referenced in 1996 in an MIT paper about the Internet,[33] but it did not launch into existence until 2007 when Amazon began providing cloud-computing services.[34]

Although the majority of consumers are not familiar with cloud computing, research found that 76 percent of respondents of an NPD Group poll used cloud-computing services, knowingly or unknowingly, within the past year.[35] For example, antispam email programs tend to be cloud services.[36] Meanwhile, more than 500,000 individuals used Amazon's

---

[28] ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 4 (2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[29] *See* JOTHY ROSENBERG & ARTHUR MATEOS, THE CLOUD AT YOUR SERVICE 2 (2011). Furthermore, in the proposed 2012 Federal Budget the Obama administration suggested a "Cloud First Policy," which would improve government IT inefficiencies and the delivery of government services by "requiring agencies to evaluate safe, secure cloud computing options before making any new investment." *See* VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 2 (Feb. 8, 2011); OFFICE OF MGMT. & BUDGET, BUDGET OF THE UNITED STATES GOVERNMENT, FISCAL YEAR 2012 (2011).

[30] ROSENBERG & MATEOS, *supra* note 29, at 1.

[31] GELLMAN, *supra* note 28, at 4.

[32] *Id.*

[33] ROSENBERG & MATEOS, *supra* note 29, at 8; *see* Sharon Eisner Gillet & Mitchell Kapor, *The Self-Governing Internet: Coordination by Design*, *in* COORDINATING THE INTERNET (MIT Press 1997), *available at* http://ccs.mit.edu/papers/CCSWP197/CCSWP197.html.

[34] ROSENBERG & MATEOS, *supra* note 29, at 8-9.

[35] Andrew R. Hickey, *Cloud Computing Befuddles Consumers, Despite Use: Study*, CRN.COM (Aug. 9, 2011), http://www.crn.com/news/cloud/231300496/cloud-computing-befuddles-consumers-despite-use-study.htm;jsessionid=gZmvvMv3r7B-f1qFfqyyOA**.ecappj01. The NPD Group found that "only 22 percent of consumers in the U.S. are familiar with the term 'cloud computing'" but "76 percent of U.S. respondents used some form of Internet-based cloud service within the past year." *Id.* The NPD Group is a market research organization that provides "consumer and retail information" to "more than 2000 manufactur[ing], retail, and service companies . . . ." *About NPD*, NPD GROUP, https://www.npd.com/wps/portal/npd/us/aboutnpd/ (last visited Sept. 16, 2012).

[36] BRIAN J.S. CHEE & CURTIS FRANKLIN, JR., CLOUD COMPUTING: TECHNOLOGIES AND STRATEGIES OF THE UBIQUITOUS DATA CENTER 82 (2010).

cloud within the first eighteen months it was open to the public.[37] Companies with computer systems that operate on private servers have also begun to shift their data to cloud servers, which tend to be much less expensive.[38] And individual Internet consumers use cloud services through email, gaming, tax preparation, video and photo sharing, and storing and backing up data.[39] Moreover, companies such as Verizon, AT&T, and Time Warner Cable are beginning to acquire and implement cloud services,[40] which suggests that major companies recognize the large-scale movement of data storage to cloud servers, and that an increasing number of people will become cloud users as customers of such companies.

Although travelers might be uncomfortable with broadening the scope of the border search doctrine to cloud computing, since it will diminish privacy rights at the border, this note argues that the border search doctrine should, in fact, apply to data stored on the cloud.[41] The Supreme Court has not yet addressed border searches of electronic devices. Nevertheless, the Supreme Court has carved out a doctrine that gives the federal government vast power to search the property of individuals who cross the border attempting to enter the United States.[42] The U.S. Courts of Appeals have taken this breadth of authorization and enlarged the scope of the border search doctrine even further.[43] Based on this expansion, this note will demonstrate that it is only logical for courts to extend the border search doctrine to virtual data as well as locally stored electronic data. To do otherwise would undermine the path that courts have already paved and would enable contraband, criminal activity, and national security threats to breach our borders.

---

[37] ROSENBERG & MATEOS, *supra* note 29, at 2.

[38] *Id.* at 6.

[39] Hickey, *supra* note 35.

[40] Andrew R. Hickey, *Cloud Services: Carriers Want Cloud Control*, CRN.COM (July 25, 2011), http://www.crn.com/news/networking/231002498/cloud-services-carriers-want-cloud-control.htm.

[41] What this note means by accessing the cloud at the border is this: certain cloud servers are available with just one click. For example, a Google user might open the Internet browser on his iPhone, BlackBerry, or other electronic device, and Google might be the default page or it might be easily accessible through the browser's bookmarks. Often, users can store passwords so that once on Google's web page, the user might already be logged in to the site. If this is the case, that user has easy access to his email, calendar, photographs, and documents. As a result, a customs officer could access all of this information just as easily, with a single click.

[42] *See* United States v. 12 200-Foot Reels of Super 8mm. Film, 413 U.S. 123, 125-26 (1973) (discussing the Tariff Act of 1930, which gives Congress "plenary power . . . to regulate imports" and to prevent contraband from entering the country).

[43] *See infra* Part II.A.

This note will describe developments in electronic data storage and analyze how the border search doctrine applies to information stored on the cloud. Part I reviews general Fourth Amendment jurisprudence within the United States. In addition, it focuses on the government's access to information that individuals voluntarily convey to third parties. Part II examines an exception to the Fourth Amendment—the border search doctrine. This part looks at the evolution of the border search doctrine, the justification for and consequences of the doctrine, and the federal courts' treatment of computer and electronic-device searches at international borders. Part III explores cloud computing. It defines cloud computing, describes how it works, and discusses its present role in technology. In addition, this part illustrates the complexity that cloud computing adds to border searches, since it could expand such searches to information not already encompassed within Fourth Amendment jurisprudence. Part IV takes a closer look at a third party's access to given information and how this relates to data stored on the cloud—that is, on a third party's server. It will question whether Fourth Amendment protection should extend to data on the cloud. Finally, Part V analyzes how the easy access to data on the cloud plays a role in border searches, even when the data itself is not physically located at the border. The note's conclusion synthesizes cloud computing and the border search doctrine, and it argues that government officials can, in fact, legally access data stored on the cloud during searches conducted at the border.

I. THE FOURTH AMENDMENT AND ITS JURISPRUDENCE

This section discusses the Fourth Amendment's protection and its exceptions. The Fourth Amendment is important in the context of border searches because it typically protects people within the United States from warrantless searches and seizures.[44] The jurisprudence surrounding the Fourth Amendment, however, has resulted in a number of exceptions, including one for searches at the border. This section begins by introducing the Fourth Amendment and the Supreme Court's standard for determining whether a search is unreasonable. This section then distinguishes between situations where there is an expectation of privacy and situations where there is not,

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

and thus between situations where information is protected by the Fourth Amendment and those where it is not, respectively.

The Fourth Amendment protects individuals against unreasonable searches and seizures. When drafting the Amendment, the Framers were particularly concerned about warrants, abuse of power by new officers, and protecting the home.[45] The Fourth Amendment guarantees:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[46]

The reasonableness of a search depends on its nature and the totality of the circumstances surrounding the search or seizure.[47] Where a person has a legitimate expectation of privacy concerning a certain area, the reasonableness of a search of that area depends on "the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted."[48] Moreover, searches executed without a warrant or probable cause of wrongdoing are "per se unreasonable" and prohibited by the Constitution.[49]

The Fourth Amendment primarily protects against warrantless searches and seizures in one's home.[50] This is because individuals expect items and information in their homes to be preserved as private.[51] But Fourth Amendment

---

[45] Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L. J. 979, 1061 (2011).

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

[47] *See* New Jersey v. T.L.O., 469 U.S. 325, 337-42 (1985). For example, there is no expectation of privacy in information given to third parties:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

United States v. Miller, 425 U.S. 435, 443 (1976) (citation omitted).

[48] Bell v. Wolfish, 441 U.S. 520, 559 (1979).

[49] Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)) (internal quotation marks omitted); *see also* Horton v. California, 496 U.S. 128, 133 (1990).

[50] *See* United States v. Thirty-Seven (37) Photographs, 402 U.S. 363, 376 (1971) ("[A] port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search.").

[51] *See Katz*, 389 U.S. at 351.

protection is not limited exclusively to one's home.[52] In *Katz v. United States*, Justice Harlan's concurrence[53] laid out a two-part test for determining whether an individual has a legitimate expectation of privacy, particularly when outside one's home: (1) did the individual "exhibit[] an actual (subjective) expectation of privacy," and (2) is the expectation of privacy "one that society is prepared to recognize as 'reasonable'?"[54] If both questions are answered in the affirmative, then law enforcement may not access, search, or seize the property or information expected to be private, unless they have a warrant. If they take any of these steps without a warrant, they would violate the person's Fourth Amendment rights.[55] Courts may assess the extent to which a search infringes upon an individual's privacy by weighing various factors, including the intention of the Framers of the Fourth Amendment, the way in which the individual uses such location, and "our societal understanding that certain areas deserve the most scrupulous protection from government invasion."[56]

In certain situations there is no expectation of privacy. Indeed, the Supreme Court has repeatedly held that there is "no . . . expectation of privacy in information . . . voluntarily [provided] to third parties."[57] For instance, a person who deposits money in a bank has "no legitimate expectation of privacy" in "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[58] Similarly, there is no expectation of privacy in the phone

---

[52] *See id.* ("[T]he Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an areas accessible to the public, may be constitutionally protected.").

[53] Although this test comes from the concurring opinion of *Katz*, the Supreme Court applies this test when determining the reasonableness of a search and seizure. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy' . . . ." (citations omitted)).

[54] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). In this case the Supreme Court examined whether government-initiated recording of a conversation on a telephone in a public telephone booth was a "search and seizure" within the meaning of the Fourth Amendment. *Id.* at 348-49, 353. The Court held that electronic surveillance of a telephone booth violates the Fourth Amendment because an individual making such a phone call "assume[s] that the words he utters into the mouthpiece will not be broadcast to the world." *Id.* at 352.

[55] *See id.* at 361 (Harlan, J., concurring) ("The point is . . . that the [telephone] booth is . . . a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.").

[56] Oliver v. United States, 466 U.S. 170, 178 (1984).

[57] *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[58] *Miller*, 425 U.S. at 442 (internal citations omitted).

numbers a person dials.[59] In *Smith v. Maryland*,[60] the police, without a warrant, asked a telephone company to install a pen register[61] on the defendant's telephone number.[62] By using the pen register, the telephone company and police monitored the phone numbers that the defendant dialed and determined that he was calling the home of a woman he had robbed.[63] Thereafter, the defendant was indicted for robbery.[64] He moved to suppress the pen register evidence against him on the ground that it was obtained without a warrant.[65] The Supreme Court rejected his argument and held that there is no right to privacy for phone numbers.[66] This is because typical users know that they must turn over numerical information—such as phone numbers—to the phone company and that the phone company has facilities where they record this information for various purposes.[67]

There is an important distinction between *Katz*, where the Court held that the government invaded a legitimate expectation of privacy by listening to a telephone conversation,[68] and *Smith*, where the "pen register[] [did] not acquire the *contents* of [the] communication[]" but only acquired the actual phone number dialed.[69] Indeed, this distinction between the *content* of information and mere identifying information that is voluntarily turned over to third parties—such as phone numbers dialed—dates back to Supreme Court cases from the nineteenth century.[70]

---

[59] *See Smith*, 442 U.S. at 743-44.

[60] *See id.* at 735.

[61] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 736 n.1 (quoting United States v. N.Y. Tel. Co., 434 US. 159, 161 n.1 (1977)).

[62] *Id.* at 737.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.* at 743 ("[I]t is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain a secret.").

[67] *Id.*

[68] Katz v. United States, 389 U.S. 347, 352 (1967).

[69] *Smith*, 442 U.S. at 741 (emphasis in original).

[70] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) ("[T]he government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties."); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their *outward form* and weight, as if they were retained by the parties forwarding them in their own domiciles." (emphasis added)).

In *United States v. Forrester*, the U.S. Court of Appeals for the Ninth Circuit extended this distinction to surveillance of e-mail and IP addresses used for Internet communication.[71] The defendants in *Forrester* were indicted and arraigned for conspiring to manufacture the drug Ecstasy.[72] Their indictment was partially based on evidence the government obtained by monitoring one defendant's Internet and e-mail activity.[73] The court held that the monitoring techniques were analogous to the pen register used in *Smith v. Maryland*.[74] As the court explained,

> [E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.[75]

An important factor considered by the court was that IP addresses and to and from addresses in an Internet user's e-mail do not reveal anything more regarding the underlying contents of communication than phone numbers do.[76] The e-mail and IP addresses do not indicate a message's content or indicate the particular pages of websites viewed.[77] In fact, the court explicitly stated that *Forrester*'s holding extends only to the "particular techniques" used in that case "and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register."[78] As a result, it seems that phone numbers, addresses, e-mail addresses, and IP addresses all fall outside the scope of Fourth Amendment protection, and therefore, government officials may monitor and search this "exterior" information without violating constitutional rights.

II. THE BORDER SEARCH DOCTRINE

There are several exceptions to the Fourth Amendment's warrant requirement for conducting searches. These exceptions include searches of items in plain view,[79]

---

[71] *See Forrester*, 512 F.3d at 509-10.
[72] *Id.* at 505.
[73] *Id.*
[74] *Id.* at 510.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.* at 511.
[79] Horton v. California, 496 U.S. 128, 133 (1990).

searches by consent,[80] searches "incident to a lawful . . . arrest" when "it is reasonable to believe evidence . . . might be found,"[81] searches executed during exigent circumstances or circumstances where law enforcement has probable cause to believe a crime is being committed,[82] and searches at an international border or its functional equivalent.[83] Furthermore, "[t]he permissibility of a particular law enforcement practice is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[84] This section focuses on the Fourth Amendment exception at international borders or their equivalent. It briefly traces the history of this exception and then specifically examines government-issued guidelines and the approaches various courts have employed, including the Fourth Circuit's refusal to exempt "expressive" items from the broad border search power. The second part of this section briefly examines the role that computer security, such as passwords, plays in border searches.

Since the ratification of the Constitution, Congress and the courts have recognized that government interests at international borders weigh more heavily than individual Fourth Amendment interests.[85] The first Congress granted border officials plenary power to conduct warrantless searches.[86] This power rests on the assumption that searches at

---

[80] Florida v. Jimeno, 500 U.S. 248, 250-51 (1991).

[81] Arizona v. Gant, 556 U.S. 332, 343 (2009) (internal quotation marks omitted).

[82] *See* Wengert v. State, 771 A.2d 389, 394 (Md. 2001) (citing several Supreme Court cases that held exigent circumstances are an exception to the Fourth Amendment).

[83] Almeida-Sanchez v. United States, 413 U.S. 266, 272-74 (1973) ("Travellers may be so stopped in crossing an international boundary because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in." (quoting Carroll v. United States, 267 U.S. 132, 153-54 (1925)) (internal quotation marks omitted)). Examples of the functional equivalent to a U.S. border include "an established station near the border, at a point marking the confluence of two or more roads that extend from the border" or "an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City." *Id.*

[84] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)).

[85] *See id.*

[86] 19 U.S.C. § 482 (2012).The statute states:

> Any of the officers or persons authorized to board or search vessels may stop, search, and examine . . . any vehicle, beast, or person, on which or whom he or they shall suspect there is merchandise which is subject to duty, or shall have been introduced into the United States in any manner contrary to law, whether by the person in possession or charge, or by, in, or upon such vehicle or beast, or otherwise, and to search any trunk or envelope, wherever found, in which he

the border are "qualitatively different" from searches within the country. Indeed, border searches help prevent contraband from entering the United States altogether.[87] As a result, "Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ."[88] The government may conduct routine border stops and searches at fixed checkpoints close to the border,[89] on boats in U.S. waters at seaports,[90] and at international airport terminals.[91] Nonetheless, if the search crosses the line between routine and nonroutine—such as searching a person's alimentary canal—CBP and ICE officials must have reasonable suspicion for conducting that search.[92]

CBP and ICE directives have established guidelines for conducting searches at the border.[93] Although the CBP directive provides guidelines for handling sensitive material found on "electronic devices," border agents are nonetheless free to search through the contents of data stored on such devices.[94] As a letter from Congressman Bennie Thompson described the process, "These [searches] include opening individual laptops; reading documents saved on the devices; accessing email accounts and reading through emails that have been sent and received; examining photographs; looking through personal calendars; and going through telephone numbers saved in cellular phones."[95] Nevertheless, the ability to inspect the content of material finds support from the Supreme Court's

---

> may have a reasonable cause to suspect there is merchandise which was imported contrary to law . . . .

Id.

[87] *Montoya de Hernandez*, 473 U.S. at 537, 538.

[88] *Id.* at 539; *see also* United States v. Holtz, 479 F.2d 89, 94 (9th Cir. 1973) (Ely, J., dissenting) (The court upheld the strip search of defendant at the border. Dissent stated that this strip search was the type of inspection to "offend the sensibilities of any decent citizen," and the court should not "depart from its established principles.").

[89] *See, e.g.*, United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).

[90] *See Montoya de Hernandez*, 473 U.S. at 538.

[91] An international airport is the "functional equivalent of a border" where flights arriving from foreign jurisdictions are concerned. Almeida-Sanchez v. United States, 413 U.S 266, 273 (1973).

[92] *See Montoya de Hernandez*, 473 U.S. at 541. The respondent was convicted of unlawful importation of cocaine after inspectors discovered that she had swallowed eighty-eight balloons filled with cocaine. *Id.* at 536.

[93] *See generally* CBP DIRECTIVE, *supra* note 12; ICE DIRECTIVE, *supra* note 12.

[94] CBP DIRECTIVE, *supra* note 12, § 5.2; ICE DIRECTIVE, *supra* note 12, § 8.6.

[95] THE CONSTITUTION PROJECT, *supra* note 17, at 4.

acceptance of border officials opening first-class mail without a warrant and with "less than probable cause."[96]

Although searches should typically be conducted in the presence of the traveler, in certain situations, searches may be conducted outside his or her presence.[97] Indeed, CBP permits its agents to conduct searches that last up to five days before requiring approval, make copies of searched information, and transfer devices or copies of information to other federal agencies if technical assistance is required.[98] ICE allows searches to last as long as thirty days before requiring approval.[99] If a search is conducted away from the immediate vicinity of the border, then that search's legality is determined by considering the totality of the circumstances, which includes the time that has elapsed since the searched item was at the border, the distance from the border, and the manner of the search.[100] Nonetheless, the border search doctrine is still "guided . . . by reason and practicality, not inflexible rules of time and space."[101]

A. The Court's Approach to Border Searches

The Supreme Court has not yet addressed the role of computers and other electronic devices in the border search doctrine.[102] In the past decade, however, federal circuit courts have addressed this issue and held that searches of computers and electronic devices at the border do not require reasonable suspicion.[103] In *United States v. Arnold*,[104] for example, the Ninth

---

[96] *Montoya de Hernandez*, 473 U.S. at 538.

[97] CBP DIRECTIVE, *supra* note 12, § 5.1.4; ICE DIRECTIVE, *supra* note 12, § 8.1.

[98] CBP DIRECTIVE, *supra* note 12, § 5.3.

[99] ICE DIRECTIVE, *supra* note 12, § 8.3.

[100] *See* United States v. Escamilla, 560 F.2d 1229, 1231-32 (5th Cir. 1977); United States v. Nichols, 560 F.2d 1227, 1228 (5th Cir. 1977); United States v. Rodriguez-Alvarado, 510 F.2d 1063, 1064 (9th Cir. 1975).

[101] United States v. Cotterman, 637 F.3d 1068, 1076 (9th Cir. 2011) (citing *Montoya de Hernandez*, 473 U.S. at 537).

[102] *See, e.g.*, United States v. Bunty, 617 F. Supp. 2d 359, 364-65 (E.D. Pa. 2008) ("Although the Supreme Court has not addressed specifically the search of computer equipment at the border, other federal courts have agreed that such searches do not require reasonable suspicion.").

[103] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007); *Bunty*, 617 F. Supp. 2d at 365.

[104] *Arnold*, 533 F.3d at 1005. Arnold arrived at Los Angeles International Airport from a flight from the Philippines and was selected for secondary questioning, where CBP officials asked him to power on his computer. *Id.* CBP officials then opened photograph files on Arnold's laptop, in which they found pictures of nude women. *Id.* A continued search of his photographs led to what officials believed was child

Circuit discussed the types of items the government may legally search at the border.[105] These items include places where a traveler attempts to conceal objects, such as "the contents of a traveler's briefcase and luggage, . . . a traveler's 'purse, wallet, or pockets,'. . . papers found in containers such as pockets, . . . [and] pictures, films and other graphic materials."[106] At the border, the Fourth Amendment does not protect these items—that is, "particularized suspicion" is not required for these items to be searched.[107] Even so, there is a point where searches of these items become unreasonable.[108] But the Supreme Court has left unclear whether and when "a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."[109] Indeed, in *United States v. Vance*,[110] the Ninth Circuit applied a sliding scale and held that "as [a] search becomes more intrusive [to the human body], more suspicion is [required]."[111] But the Supreme Court subsequently clarified that this sliding-scale test does not apply to searches of vehicles at the border.[112]

One court has found that computer searches are more similar to vehicle searches than to the search of a person at the border.[113] Furthermore, the Ninth Circuit has held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border," and accordingly, the sliding-scale test does not apply.[114] Thus, it is much more difficult to determine when a search of an electronic device crosses the line from reasonable

---

pornography. *Id.* Although Arnold argued that a computer is similar to a home, because individuals store personal documents on their laptops, much like they do in their homes, the court rejected this argument and refused to distinguish a "laptop and its electronic contents . . . from . . . travelers' luggage . . . ." *Id.* at 1006, 1009. The court held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Id.* at 1008.

[105] *Id.* at 1007.

[106] *Id.*

[107] *Id.*

[108] *See* United States v. Ramsey, 431 U.S. 606, 618 (1977).

[109] *Id.* at 618 n.13; United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004).

[110] 62 F.3d 1152, 1156 (9th Cir. 1995).

[111] *Id.*

[112] *Flores-Montano*, 541 U.S. at 152.

[113] United States v. McAuley, 563 F. Supp. 2d 672, 677 (W.D. Tex. 2008) ("The Defendant would have this Court impute the same level of privacy and dignity afforded to the sovereignty of a person's being to an inanimate object like a computer. The Court finds this argument without merit. . . . [T]his Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents.").

[114] United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008).

to unreasonable.[115] To add to this difficulty, the Ninth Circuit did not distinguish between a closed container, such as a briefcase, and an electronic device.[116] In fact, the court treated them the same.[117] Various courts, when referring to *Arnold*, have reinforced this treatment by holding that "[a] computer is entitled to no more protection than any other container."[118]

Moreover, the Fourth Circuit refused to carve out a border search exception for computers based on the First Amendment.[119] In *United States v. Ickes*, a customs inspector searched Ickes's van as he entered the United States from Canada.[120] CBP officials searched his vehicle and found his computer, which contained child pornography.[121] Ickes then challenged his conviction for transporting child pornography by arguing that the search of his computer was unconstitutional because "expressive" items are exempt from the border search doctrine.[122] The court, however, rejected this argument.[123] It reasoned that a principal justification for the border search doctrine is to give the United States the ability to protect itself.[124] "Terrorist communications," which can be stored on electronic devices, "are inherently expressive."[125] Therefore, if the court held for the defendant's asserted legal analysis, then the precedent would undermine one of the essential goals of border security—preventing terrorism.[126]

---

[115] *See* United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) ("Customs Officers exercise broad authority to conduct routine searches and seizures for which the Fourth Amendment does not require a warrant, consent, or reasonable suspicion. . . . Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search." (citations omitted)).

[116] *Arnold*, 533 F.3d at 1009 (The defendant "failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed.").

[117] *Id.* at 1009-10.

[118] People v. Endacott, 79 Cal. Rptr. 3d 907, 909 (Cal. App. Dep't Super. Ct. 2008); *see also* United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers.").

[119] United States v. Ickes, 393 F.3d 501, 507 (4th Cir. 2005).

[120] *Id.* at 502.

[121] *Id.* at 503.

[122] *Id.* at 506.

[123] *Id.*

[124] *Id.*

[125] *Id.* (internal quotation marks omitted).

[126] Additionally, a Pennsylvania court has held that government officials may search computer equipment found in luggage without reasonable suspicion. United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008).

The Ninth Circuit has held that "the government must be reasonably certain that the object of a border search has crossed the border [in order] to conduct a valid border search."[127] As a result, in the context of border searches of devices that contain information stored remotely on the cloud, courts must first address a threshold question: does the border search doctrine apply to data stored on servers that are not physically located at the border? In other words, can border officials access virtually stored information, or is a virtual inspection unreasonable?

B. The Role of Computer Security

Although circuit courts have not explicitly addressed the role that passwords play when conducting a border search, it seems possible that password security does little to actually prevent border officials from searching electronic devices. For example, as the U.S. District Court for the Western District of Texas found, "A password on a computer does not automatically convert a routine search into a non-routine search. A password is simply a digital lock."[128] Luggage and briefcases usually have locks, yet they are "subject to 'routine' searches at ports of entry all the time."[129] In *United States v. Bunty*, border agents simply asked the defendant to provide them with the passwords to two laptop computers and informed him that his refusal would lead the government to hire someone else to access the contents of the computers.[130] After the defendant challenged the legality of the search, the district court held that nothing indicated that the search of the computer was any different from a routine computer search at the border.[131]

In *United States v. Cotterman*, the Ninth Circuit reversed the district court and held that border officials in Arizona lawfully searched the contents of Howard Cotterman's computer, even though the border agents detained and transported the computer to a forensic computer laboratory 170 miles away.[132] At first, officials were limited in what they could

---

[127] United States v. Romm, 455 F.3d 990, 996 (9th Cir. 2006) ("We have held the government must be reasonably certain that the object of the border search has crossed the border to conduct a valid border search." (citing United States v. Corral-Villavicencio, 753 F.2d 785, 788-89 (9th Cir. 1985); United States v. Tilton, 534 F.2d 1363, 1366-67 (9th Cir. 1976); United States v. Garcia, 415 F.2d 1141, 1144 (9th Cir. 1969))).

[128] United States v. McAuley, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008).

[129] *Id.* (citing United States v. Flores-Montano, 541 U.S. 149, 154-55 (2004)).

[130] *Bunty*, 617 F. Supp. 2d at 363.

[131] *Id.* at 365.

[132] 637 F.3d 1068, 1070 (9th Cir. 2011).

inspect on the computer because "many of [the] files were password protected."[133] After Cotterman failed to provide the passwords, however, an ICE official "bypass[ed] [the] computer security and open[ed] twenty-three of the password protected files."[134] Without addressing the legality of the particular act of bypassing the password protection, the court held that the search of the computer files was lawful.[135]

These cases support law enforcement's power to search files stored on a traveler's computer and electronic devices at the border without a warrant or reasonable suspicion.[136] Additionally, they suggest that computer searches are lawful even if the devices or files are protected by security features.[137] In the last several years, technological innovations have led more and more people to store data in places other than their hard drives, such as external and third-party servers. If these files are password protected, what does it mean for agents at the border?

III. THE MECHANICS OF THE CLOUD

Cloud computing is "the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections."[138] "Any information [that can be] stored locally on a computer," such as on a hard drive, can also be stored on the cloud.[139] "Cloud computing . . . is physically limitless," since it "can . . . be accessed by users 'on demand' from virtually anywhere with an Internet connection with minimal administrative effort."[140] Google's free e-mail service, Gmail, is an example of cloud computing.[141] This

---

[133] *Id.* at 1071.

[134] *Id.* at 1073.

[135] *Id.* at 1070.

[136] In *Romm*, the Ninth Circuit specifically addressed the "internet cache" on the defendant's computer, and held that customs agents could gain access to this data through the border search doctrine. United States v. Romm, 455 F.3d 990, 993 (9th Cir. 2006). The court defined Internet cache as "a set of files on the user's hard drive" that are "kept by a web browser to avoid having to download the same material repeatedly. Most web browsers keep copies of all the web pages that you view, up to a certain limit, so that the same images can be redisplayed quickly when you go back to them." *Id.* at 993 n.1 (quoting DOUGLAS DOWNING ET AL., DICTIONARY OF COMPUTER AND INTERNET TERMS 149 (Barron's 8th ed. 2003)).

[137] *See e.g.*, United States v. McAuley, 563 F. Supp. 2d 672, 677-78 (W.D. Tex. 2008); United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008); *Cotterman*, 637 F.3d at 1070.

[138] GELLMAN, *supra* note 28, at 4. There is debate about this definition. *Id.* at 4 n.1.

[139] *Id.*

[140] *Tip of the Month: Managing the Risks of Cloud Computing*, MAYER BROWN (Nov. 30, 2010), http://www.mayerbrown.com/publications/article.asp?id=10088&nid=6.

[141] *Id.*

"means that any user's email 'mailbox' may actually be stored in one of several different servers located all over the world and can easily be accessed from anywhere on the Internet."[142]

In order for the cloud to operate, basic technology and infrastructure are required.[143] The "cloud needs servers on a network, and [these servers] need a home."[144] The physical home of these servers is called the data center.[145] Companies like Google, Amazon, and Microsoft "have . . . built up . . . 'mega data centers' [comprising] thousands of servers."[146] These large companies usually build data centers in geographic regions where server use is high and where there is easy access to inexpensive power, like in the Northwest.[147] Cloud consumers may or may not know the actual location of the data center they are using.[148] Additionally, it is possible to simultaneously store data in multiple places at one time.[149]

Cloud services can be used for a number of different reasons by both business organizations and individual users. For example, the *New York Times* needed to convert eleven million archived articles into PDF files in order to make them accessible online.[150] It estimated that this would require "hundreds of servers,"[151] at least four terabytes[152] of storage, and "a months-long delay."[153] So instead of undertaking this project

---

[142] *Id.*

[143] Cloud computing also requires virtualized servers, "an access API," storage, a database, and "elasticity as a way to expand and contract applications." ROSENBERG & MATEOS, *supra* note 29, at 19. The API is the way to access the cloud; it is "what the dashboard and controls are to a car." *Id.* at 27.

[144] *Id.* at 19.

[145] *Id.*

[146] *Id.* at 19-20.

[147] *Id.* at 20.

[148] GELLMAN, *supra* note 28, at 19.

[149] *Id.* at 18. The locations of some data centers, however, are available. *See e.g.*, *Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations/index.html (last visited Jan. 8, 2013) (providing a map with the locations of its data centers around the world). Microsoft and Yahoo! built data centers in Quincy, Washington. ROSENBERG & MATEOS, *supra* note 29, at 22.

[150] CHEE & FRANKLIN, *supra* note 36, at 77.

[151] *Id.*

[152] A terabyte is a unit of computer data space:

> A Terabyte is approximately one trillion bytes, or 1,000 Gigabytes. . . . To put it in some perspective, a Terabyte could hold about 3.6 million 300 Kilobyte images or maybe about 300 hours of good quality video. A Terabyte could hold 1,000 copies of the Encyclopedia Britannica. Ten Terabytes could hold the printed collection of the Library of Congress.

Megabytes, Gigabytes, Terabytes . . . What Are They?, WHAT'S A BYTE?, http://www.whatsabyte.com (last visited Jan. 8, 2013).

[153] CHEE & FRANKLIN, *supra* note 36, at 77.

on its own, the *New York Times* employed a cloud service, Amazon Web Services, which, for $240, was able to process the conversion of eleven million files and store four terabytes of data by the next day.[154] As evidenced by the *New York Times*, companies are beginning to use (or have been using) cloud services like "computing and storage to smooth out usage spikes and avoid upgrading data centers to size capacity for spikes rather than 'normal' usage."[155] On the other hand, individual users most often encounter and use the cloud for data storage.[156] If a person's computer crashes but that user's information is also stored on the cloud, then that person can access the data from a different computer. Unlike with the local hard drive, data is not lost forever.

Google, in particular, has advanced "the technological bounds of cloud computing for more than [a decade]."[157] Google offers a variety of free online applications located in the cloud,[158] which are designed to "divorce" users from desktop operating systems.[159] Through Google, users can "check [their] Gmail, type up a memo on Google docs, manage [their] photos with Picasa, read all [their] favorite sites with Google Reader, and store it all on Google's servers—allowing [the user] to access it from any computer"[160] or Internet-capable device—even a cell phone. Instead of providing a separate cloud storage system, "Google . . . provid[es] storage through [its applications]."[161] Interestingly, Google visitors can go into "incognito" mode while using Google's web browser, Chrome.[162] Incognito mode does not record the sites that Chrome users visit on their hard drives; nevertheless, the sites visited are still recorded on the server.[163] Google does not own the data that business

---

[154] *Id.*

[155] *Id.* at 78.

[156] *Id.* at 80.

[157] *Cloud Computing Benefits: Top Ten Advantages of Google's Cloud*, NEXIO.COM, http://googleapps.nexio.com/index.php?option=com_content&view=article&id=62&Itemid=229&lang=en (last visited Sept. 17, 2012).

[158] Brian Braiker, *The Cloud's Chrome Lining*, NEWSWEEK (Sept. 1, 2008, 8:00 PM), *available at* http://www.thedailybeast.com/newsweek/2008/09/01/the-cloud-s-chrome-lining.html.

[159] CHEE & FRANKLIN, *supra* note 36, at 125.

[160] Braiker, *supra* note 158.

[161] CHEE & FRANKLIN, *supra* note 36, at 81.

[162] Braiker, *supra* note 158.

[163] *Id.* By virtue of the fact that users are employing incognito mode, they must be surfing websites that they expect to remain private. This prompts an interesting question: If border officials do have access to data on the cloud through the border search doctrine, and since the incognito sites are recorded on Google's server, do border officials have access to these incognito websites when they conduct a search?

organizations and individuals store on Google's cloud.[164] Accordingly, Google will not share data, except as noted in its privacy policy. There, Google states that it will share a user's information if, among other reasons:

> [Google has] a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to . . . meet any applicable law, regulation, legal process or enforceable governmental request[,] . . . . enforce applicable Terms of Service, including investigation of potential violations[,] . . . . detect, prevent, or otherwise address fraud, security or technical issues[, or] . . . . protect against harm to the rights, property or safety of Google, [its] users or the public as required or permitted by law.[165]

Furthermore, users may remove data from Google's cloud at will.[166]

Another preeminent cloud service provider, Amazon, offers a variety of cloud web services for both business and personal use.[167] Amazon S3 is a "Simple Storage Service"[168] that is frequently encountered by individual users and is "available for just about every [computer] operating system."[169] Amazon S3 has a simple interface and enables users to store and access "any amount of data, at any time, from anywhere on the web."[170]

According to Amazon Web Services (AWS), "AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection."[171] Users of AWS must provide Amazon with information related to the content of their data on the cloud, in order to ensure compliance, and Amazon "may monitor the external interfaces"

---

[164] *Security First*, GOOGLE, http://www.google.com/apps/intl/en/business/infrastructure_security.html (last visited Sept. 17, 2012).

[165] *Privacy Center*, GOOGLE, http://www.google.com/policies/privacy/ (last modified July 27, 2012).

[166] Dan Rowinski, *How Does Google Protect Your Data in the Cloud?*, READWRITE (July 22, 2011), http://readwrite.com/2011/07/22/how_does_google_protect_your_data_in_the_cloud ("Google promises that data can be taken out of the cloud at any time and promises that it will be completely eradicated within 60 days (though usually much sooner).").

[167] For a detailed description of Amazon Web Services (AWS), see *About AWS*, AMAZON WEB SERVS., http://aws.amazon.com/what-is-aws/ (last visited Sept. 17, 2012). For a detailed description of all of the services that AWS offers, see *Products & Services*, AMAZON WEB SERVS., http://aws.amazon.com/products/ (last visited Sept. 17, 2012).

[168] CHEE & FRANKLIN, *supra* note 36, at 80.

[169] *Id.*

[170] *Id.* (internal quotation marks omitted).

[171] *Amazon Web Services: Overview of Security Processes*, AMAZON WEB SERVS., http://aws.amazon.com/articles/1697 (last updated Sept. 4, 2012).

of that content[172]—language that seems to parallel the monitoring techniques of telephone companies. But Amazon will not monitor the actual content of the data.[173] In fact, its terms of service permit users to encrypt such data so that it remains confidential.[174] With respect to users' privacy, Amazon "release[s] account and other personal information when [it] believe[s] release is appropriate to comply with the law."[175] It seems that information users provide to Amazon, such as when they "search, buy, post, participate in a contest or questionnaire, or communicate with customer service,"[176] is the type of information collected and potentially shared by Amazon with law enforcement.

Cloud computing is a "$150 billion phenomenon,"[177] and it is becoming more ubiquitous.[178] The essential benefit of cloud computing—and data storage in particular—is that information can be accessed from any location. Nationwide retail businesses can back up their inventory data from anywhere,[179] a team working on one document or project can collaborate on it from different locations and on different operating systems,[180] and retail consumers can store credit-card information online and use it to pay for merchandise in a few simple clicks.[181]

If the border search doctrine allows border security agents to access data saved on the cloud, it will enable government officials to reach into an area uncomfortable for

---

[172] *AWS Service Terms*, ¶ 1.3, AMAZON WEB SERVS., http://aws.amazon.com/serviceterms/ (last updated Sept. 4, 2012).

[173] *Id.*

[174] *Id.*

[175] *Privacy Notice*, AMAZON, http://www.amazon.com/gp/help/customer/display.html/ref=hp_468496_share?nodeId=468496&#share (last updated Apr. 6, 2012).

[176] *Id.*

[177] *The King of Cloud: Q&A with Mark Benioff*, TECH. REV. (Oct. 28, 2011), http://www.technologyreview.com/business/38851/?mod=chfeatured.

[178] *Id.* ("In the future, all software will be delivered in the cloud. . . . People will access all the services they need via the Web . . . .").

[179] *Cloud Computing: Definition, Advantages and Why You Should Switch*, GENIE9 OFFICIAL BLOG, http://blog.genie9.com/index.php/2011/03/29/cloud-computing-defenition-advantages-and-why-you-should-switch (last visited Sept. 17, 2012).

[180] CHEE & FRANKLIN, *supra* note 36, at 16.

[181] PayPal, an online service that "allows [users] to send money without sharing financial information" by storing credit card numbers and bank accounts, uses a "cloud-based payments system." *Welcome to the Press Center*, PAYPAL, https://www.paypal-media.com/about (last visited Sept. 17, 2012); *PayPal Boss Thompson Decamps for Yahoo Just as Key POS Strategy Unfolds*, DIGITAL TRANSACTIONS (Jan. 4, 2012), http://digitaltransactions.net/news/story/3383. The reliance on the cloud is one way that PayPal successfully protected its website and users from an Internet attack. Sean Sposito, *PayPal Tries Cloud Cover to Fend Off Further Attacks*, AM. BANKER (Jan. 6, 2011, 3:59 PM), http://www.americanbanker.com/issues/176_5/paypal-cloud-computing-1030928-1.html.

many—for example, private pictures or appointments on a calendar, diary entries, and confidential work information, to name a few. Extending the border search doctrine poses the same risks that the circuit courts disregarded by allowing border officials to search electronic devices.[182] These risks are even greater with the prevalence of smartphones, which are Internet-ready and provide easy access to virtual servers, e-mail, credit-card information, and work-related documents. Officials will be able to access virtual calendars and address books, inventory data, archived business information,[183] photos, chats, and other sensitive information that is not necessarily stored locally on an electronic device. Nonetheless, with few exceptions, the interests of the U.S. government tend to outweigh the privacy rights of individuals at the border, and it may be difficult to establish an appropriate area to draw the line.[184]

IV. DOES *SMITH V. MARYLAND* APPLY TO CLOUD COMPUTING?

An examination of the Supreme Court's holding in *Smith v. Maryland* and its application to cloud computing indicate that data stored on the cloud should be protected by the Fourth Amendment. *Smith v. Maryland* stands for the idea that individuals have "no legitimate expectation of privacy in information [they] voluntarily turn over to third parties."[185] As a result, government efforts to access that information are "not a 'search'" under the Fourth Amendment.[186] In the context of cloud computing, this case is helpful in analyzing whether users have a legitimate expectation of privacy in information they store on the cloud, given that these users similarly turn over information to the third-party service providers who own and operate the servers.

The answer to this question is important to determining the scope of Fourth Amendment protection available to cloud users. If these users have no legitimate expectation of privacy, then data stored on the cloud would not receive Fourth Amendment protection, regardless of whether that information is accessed within the United States or at an international

---

[182] For a discussion of the case law surrounding the border search doctrine and how it applies to electronic devices, see *supra* Part II.

[183] *See supra* note 179.

[184] United States v. Montoya de Hernandez, 473 U.S. 531, 539-40 (1985).

[185] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[186] *Id.* at 746.

border. But if these users have a legitimate expectation of privacy, then the Fourth Amendment should protect such data from being searched without a warrant, unless such search falls under an exception—for example, the border exception.

This note asserts that the facts of *Smith v. Maryland* are distinguishable from the cloud-computing context because, unlike the phone numbers acquired by the pen register, users have a legitimate expectation of privacy in the information they store on the cloud. Indeed, the *Smith* court drew a critical distinction between government interventions that capture the content of a phone conversation, such as the wiretap at issue in *Katz v. United States*,[187] and government investigations that merely access information conveyed to a third party, such as the phone numbers at issue in *Smith*. Pursuant to this distinction, data stored on the cloud would seem closely analogous to the information in *Katz*. As a result, it would be inappropriate to exclude that information from Fourth Amendment protection.

As mentioned above, courts have routinely held that information conveyed to a third party—that is, mere external information—is not information that individuals expect to remain private.[188] Rather, because an individual or business organization furnishes information to a third party, that individual or organization loses its expectation of privacy in the information.[189] As such, government officials can access that information, even in the absence of a warrant, because obtaining it would not constitute a search.[190]

Admittedly, when users store files and data on third-party cloud services, they are furnishing information to third parties. While cloud service providers are very similar to telephone companies and the services they offer, cloud-computing encompasses the disclosure of information that is different in kind from the information provided to telephone companies in *Smith*.

---

[187] *See* Katz v. United States, 389 U.S. 347, 352 (1967) ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

[188] For a discussion of information given to third parties and privacy expectations, see *supra* Part I.

[189] *Katz*, 389 U.S. at 351. ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

[190] *Smith*, 442 U.S. at 745-46.

Telephone and cloud services both provide a means of communication. The cloud provides a means of communication via e-mail communication, as well as a means of accessing one's own data from various locations—essentially communicating with oneself. Telephone service providers keep records of call logs and phone numbers dialed. But these phone service providers do not typically record or eavesdrop on phone conversations.[191] Similarly, it is not necessary for cloud service providers to examine the content of users' data. Service providers may keep records of how much data an individual or organization stores on the cloud and the bandwidth each user consumes, but this is most likely for billing purposes.[192] Cloud service providers may even record the kinds of data users store on the cloud for marketing or development purposes. It appropriately follows that the only information that cloud users voluntarily convey to third parties is the amount of data they are storing and the types of files being stored. Users are not voluntarily conveying the *content* of their information to third parties, and so users never relinquish their expectation of privacy regarding such content. Thus, the content of the information stored on the cloud is much more similar to the content of the phone conversation in *Katz*. Therefore, the Fourth Amendment should still protect the content of users' data from being searched in the absence of a warrant.

Cloud computing is distinguishable from the situation of *United States v. Miller*,[193] where government officials were permitted to access the content of financial information.[194] Unlike cloud service providers, banks play an active role in the content of the information that individuals provide to them. A depositor goes to the bank with the intention of depositing money. The depositor hands over a check to a bank teller or inserts a check into an ATM. That teller or machine reads the content of the check to determine the exact amount being deposited and then deposits that amount into the depositor's bank account. Unlike the mere recording of dialed phone

---

[191] In *Smith*, the police had to request that the phone service use a pen register recording device, which indicates that this is not an ordinary business practice. 442 U.S. at 737.

[192] Most cloud service providers allow users to store a certain amount of data for free and once a user exceeds that free amount the users are billed according to how much storage space they use. Services also charge for the amount of bandwidth used. *See* CHEE & FRANKLIN, *supra* note 36, at 118-19.

[193] For a discussion of *United States v. Miller*, 425 U.S. 435 (1976), see *supra* Part I.

[194] *Miller*, 425 U.S. at 438.

numbers by telephone service providers, it is the job of the bank to account for the *contents* of a user's bank account and to provide the bank user with the fluctuations in his or her stock portfolio. Whereas phone companies keep track of the numbers dialed and e-mail service providers keep track of to and from email addresses,[195] banks do not just focus on who wrote the check and who is depositing it. Instead, they also carefully examine what the check says—including the amount to be transferred—in order to fulfill their obligations to deposit the check, transfer funds, and monitor the depositor's account.

As discussed, cloud users do not voluntarily convey the content of their data to cloud service providers, and so the holding of *Smith v. Maryland* does not apply to virtual information. As a result, the Fourth Amendment protects information stored on the cloud, and government officials may not access that information without a warrant. Nevertheless, the question remains: does this data come under an exception? More specifically, may law enforcement access this data without a warrant if an individual carries an electronic device across an international border? To answer this question, it is necessary to determine whether the border search doctrine applies to this information.

V. BORDER SEARCH DOCTRINE AND INFORMATION ON THE CLOUD

If the third-party exception from Part IV does not apply to data stored on the cloud, then what does it mean for searches at the border? The data is not physically located at the border, but it is easily accessible from a computer, smartphone, tablet, or any other Internet-ready wireless device located at the border. Furthermore, it is possible to require passwords to gain access to cloud programs stored on wireless devices. Do CBP and ICE officials need warrants to access such data, or can they access it without a warrant or reasonable suspicion at the border, as law enforcement agents within the Ninth Circuit's jurisdiction are permitted to do?

It seems logical that the border search doctrine does, in fact, encompass information that is stored on the cloud and accessible through an electronic device. In developing the precedent surrounding the border search doctrine, the Supreme

[195] For a discussion of *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), see *supra* Part I.

Court and the U.S. Courts of Appeals have emphasized that the interests of the U.S. government (in preventing contraband and threats to security from breaching U.S. borders) outweigh interests of individuals who cross the border.[196] If courts, upon hearing a case concerning border officials' search of cloud data, were to rule that accessing such information at the border falls outside the scope of the border search doctrine, then courts would permit U.S. entrants to circumvent DHS policies and U.S. common law. As a result, instead of storing contraband or evidence of illegal activity on local hard drives, savvy entrants would store this material on the cloud, knowing that it could not be accessed by government agents. This would "undermine the compelling reasons that lie at the very heart of the border search doctrine."[197]

A. Data Not Physically at the Border and Passwords

A cloud user's data itself is stored on a server that is not at the border but is instead in a discreet location.[198] A number of cloud service providers house servers in the Northwest;[199] yet, most service agreements do not disclose where servers are located, and the location of smaller cloud service providers may not be available at all.[200] As a result, unlike with data on a local hard drive, the information on the cloud does not physically cross the border with the traveler.

Does this mean, then, that because the data is not physically crossing the border, border officials are unable to search such data under the border search doctrine? This seems unlikely. In *United States v. Romm*, the defendant "never legally crossed the U.S.-Canadian border" because, although he flew to Canada, Canadian border officials refused to admit him into the country.[201] Romm argued that because of this, "he [could] not [be] subject to a warrantless border search."[202] The fact that Romm physically crossed the border, though illegally, prompted the Ninth Circuit to reject this argument.[203] As the court

---

[196] *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985).

[197] United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

[198] See *supra* Part III for a discussion of where certain large cloud companies have built data centers.

[199] *See supra* Part III.

[200] *See* GELLMAN, *supra* note 28, at 18.

[201] United States v. Romm, 455 F.3d 990, 994, 996 (9th Cir. 2006) (emphasis omitted).

[202] *Id.* at 996 (emphasis omitted).

[203] *Id.*

explained, "[T]he issue was whether the *person* searched had physically crossed the border."[204] Therefore, by virtue of the fact that a *traveler* crosses an international border, it is possible that data on any Internet-ready device—which the traveler carries while physically crossing the border—is searchable, regardless of whether the data itself physically crossed the border. It is less clear, however, how other circuit courts would interpret this situation, since none have spoken to this issue.

What if border officials seize a traveler's laptop or mobile device and try to access data that is on the cloud, but that data is password protected or encrypted? Certainly cloud users may protect their information with passwords or encryptions in order to keep the content of their files confidential.[205] Although the Ninth Circuit and several district courts have upheld border searches of computer files where border officials bypassed the password protection, courts have not explicitly addressed the effects of password protection on border searches.[206] Nonetheless, by following the scant authority that exists, it is plausible that passwords fail to generate sufficient protection at the border.

Users can store passwords on their computers, smartphones, and on certain websites in order to free themselves from having to input the password every time they access their cloud servers. If a password is stored in an Internet-ready device, border officials might view this as consent from the device's owner to access that information. With respect to situations where the password is not stored on the device, courts have not yet taken issue with border agents asking for that password or having forensic experts bypass the security system, as in *Cotterman*.[207] If a traveler refuses to comply with requests for a password, the traveler's refusal might result in the device being detained for a longer period of time while the agents determine how to access the information.[208] One way they might access the protected data is by requesting it from cloud service providers—many of which

---

[204] *Id.* (emphasis added).

[205] For example, Amazon's Terms of Service permits encryption of content. *See supra* note 172 and accompanying text.

[206] *See supra* Part II.B.

[207] *See generally* United States v. Cotterman, 637 F.3d 1068 (2011).

[208] *See* United States v. Bunty, 617 F. Supp. 2d 359, 363-64 (E.D. Pa. 2008). Agents allowed Bunty to leave but detained his laptop in order to determine how to access password-protected information. *Id.*

will share a user's information in order to comply with requests from law enforcement.[209]

As a result, it is possible that passwords have little relevance in the border search context. If passwords were truly able to thwart access by border officials, then the ability to password protect cloud data would undermine the justifications of the border search doctrine—namely, preventing contraband and terrorism from penetrating the United States.

B. Data Can Be Accessed at the Border

This note concludes that the border search doctrine does, in fact, apply to data stored on the cloud. The Supreme Court has carved out a doctrine that gives the federal government great power in searching the property of individuals who cross an international border and enter the United States.[210] This doctrine—along with jurisprudence in the circuit courts regarding warrantless searches of electronic devices at the border and the directives of the CBP and ICE—guides the conclusion that warrantless searches of data stored on the cloud are acceptable when executed near the border. If the purposes of the CBP and ICE directives are to prevent the smuggling of contraband into the United States, stop those engaged in criminal conduct, and thwart threats to national security, then certainly data on the cloud should not be excluded from the border search exception. It would be illogical to allow border agents to search local hard drives of travelers' computers without suspicion or consent, and yet preclude those agents from opening files accessible on the same devices but not stored locally. This would enable travelers to bypass CBP and ICE's search procedures, and it would permit them to bring in the very same contraband and execute the very same conduct that the border search doctrine is intended to prevent.

C. Should There Be a Limit?

While this note argues that the government should have access to data stored on the cloud since it serves the purposes of the border search doctrine, this note does not necessarily assert that the extension of the border search doctrine would be

---

[209] *See* discussion of Terms and Conditions of various cloud service providers *supra* Part III.

[210] *See supra* Part II.

beneficial. Expanding the border search doctrine to a realm that is becoming more and more ubiquitous will continue to subvert privacy interests that are only modestly protected even under current law. Therefore, border searches should be limited in a way to protect privacy interests as much as possible. This section outlines the difficulties of an expanded border search doctrine, discusses the self-imposed limits that already exist, and suggests limits for the future.

One problem with digital devices, as one court noted, is that they "are not just repositories of data, but access points, or portals, to other digital devices and data, typically obtained through the internet or stored on a network. All data on the internet is both separate and one."[211] In a case where the government filed an application for a warrant for all passwords and encryption codes for the files on the suspect's computer,[212] the court called the warrant "boundless."[213]

> This is made evident by the fact that the government seeks authorization, among other things, to obtain "all passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data." . . . This poses a multitude of problems . . . . First, once the government has all passwords, it is able to access a defendant's most sensitive information. To the extent the defendant may have medical records on-line, that information is now available to the government. If the defendant's wife, who is not alleged to be involved in any criminal activity, is sending embarrassing, private e-mail messages, that information is now available for use by the government. If the government wants to see what books the defendant is reading, or what movies his wife is viewing, all of this would be fair game under the warrant presented by the government. Moreover, if the defendant has been looking at legal but "dirty" pictures the government will know this as well, even if the defendant had intended to "throw them away."[214]

If border officials are able to obtain access to password-protected or encrypted files stored on the cloud by asking travelers for their security codes or passwords—or by bypassing them—cloud users will face the same challenges described above. Accordingly, the question becomes whether

---

[211] *In re* United States' Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1145 (W.D. Wash. 2011).

[212] The location of the place to be searched was within the United States, not at a border. The government applied for a warrant to search the suspect's apartment, located at "2305 Rucker Avenue # 5, Everett, Washington." *Id.* at 1139. Thus, Fourth Amendment protections applied and a warrant was necessary. At the border, however, obtaining a warrant is not a necessary prerequisite to conducting a search. *See supra* Part II.

[213] *Id.*

[214] *Id.* at 1145 (citation omitted).

there should be a limit to what border officials may access and whether their searches should be limited in scope.

One might argue that self-imposed limits to the border search doctrine already exist. For instance, more than one million people travel across American borders every day, but neither CBP nor ICE has the resources to conduct searches on every individual crossing the border.[215] Instead, DHS has emphasized that searches are typically based on "circumstances . . . which give rise to . . . suspicion"[216]—for example, nervous behavior—"even though courts have repeatedly confirmed that . . . suspicion is not required . . . ."[217]

Moreover, the CBP and ICE directives do require greater protection of sensitive material.[218] If border agents come across material protected by attorney-client privilege or other sensitive information,[219] they must consult the CBP Associate or Assistant Chief Counsel before continuing with the search.[220] CBP counsel will collaborate with the United States Attorney's Office regarding the privileged attorney information.[221] All other sensitive business and commercial information will be treated as confidential, and "[i]nformation . . . determined to be protected by law as privileged or sensitive will only be shared with federal agencies that have mechanisms in place to protect appropriately such information."[222] ICE's policy directive contains similar limitations.[223]

Furthermore, it is safe to bet that border officials cannot access the data of travelers who do not transport computers or other Internet-ready devices over the border, even if border agents are capable of accessing cloud servers through their own devices. Although the holding in *Romm* is based on the fact that the *person* whose effects were searched physically crossed the border,[224] broadening this principle to include situations where that person does not carry an electronic device would exceed the bounds of the court's holding and most likely be unreasonable. Because the traveler is not carrying such devices, there would be no reason for border agents even to suspect that

---

[215] *S. Comm. Hearing on Laptop Searches and Overseas Travel*, *supra* note 5.

[216] *Id.*

[217] *Id.*

[218] CBP DIRECTIVE, *supra* note 12, § 5.2; ICE DIRECTIVE, *supra* note 12, § 8.6.

[219] Sensitive information means medical records and journalistic work-related data. CBP DIRECTIVE, *supra* note 12, § 5.2.

[220] *Id.*

[221] *Id.*

[222] *Id.* § 5.2.4.

[223] ICE DIRECTIVE, *supra* note 12, § 8.5.

[224] United States v. Romm, 455 F.3d 990, 996 (9th Cir. 2006).

the individual stores data on the cloud, unless law enforcement searched cloud servers for data about every person crossing the U.S. border. This seems unlikely, however. Accordingly, border agents would have no basis for searching this information through computers or electronic devices present at the border.

In his article, Professor Sales suggests that law enforcement adopt a policy of "use limits" regarding acquired data.[225] Use limits "seek to promote privacy by limiting what the government may do with the data it does collect, such as restricting the sharing of information."[226] Although a limitation such as this would not necessarily prevent the government from gaining initial access to information that individuals wish to keep private, it would serve as a means of reducing how much information is shared among governmental agencies, copied, and saved for future review. Perhaps the government could require probable cause of possessing contraband in order for border agents to share or copy any material. In addition, DHS should set a solid guideline as to how long a search of a laptop or other electronic device may last, rather than allowing a search to last for a "reasonable period of time,"[227] which in some cases could last hours or days.[228] Sales suggests that longer searches may involve a greater violation of privacy rights because customs or immigration officers might browse "through entirely innocent but sensitive" data while hunting for contraband.[229] Therefore, searches of electronic devices, absent reasonable suspicion of contraband, should be limited to a short period of time, such as one hour or ninety minutes.

CONCLUSION

Several years ago, cloud computing was merely a buzz-word that held little meaning to those who worked outside of the technology realm. Today, however, technology experts predict that the cloud will predominate the desktop by 2020, meaning that most computer users will access software applications and information through the cloud.[230] The problems

---

[225] Sales, *supra* note 18, at 1124.

[226] *Id.* at 1125.

[227] CBP DIRECTIVE, *supra* note 12, § 5.3.1.

[228] *See supra* note 19.

[229] Sales, *supra* note 18, at 1130.

[230] JANNA QUITNEY ANDERSON ET AL., THE FUTURE OF CLOUD COMPUTING (Pew Research Ctr. Publ'ns, June 11, 2010), *available at* http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts.

posed by the intersection between cloud computing and the border search doctrine have not yet been addressed by the government or the courts. However, it is clear that electronic files can be searched at the border.[231] So, in an effort to avoid electronic searches at the border, travelers might turn to the cloud based on an assumption that data on remote servers are immune from the border search doctrine. Sex offenders might upload images or videos to the cloud of child exploitation. Money launderers might unknowingly store pertinent e-mail exchanges on a cloud service. And terrorists might save information about nuclear material or video clips of how to detonate a bomb to their clouds.[232] The proliferation of cloud computing will most definitely result in a need for a clear border-patrol policy to be established.

Absent a clear policy, however, American jurisprudence signifies that law enforcement officials should have the authority to access information on the cloud by invoking the border search exception to the Fourth Amendment. Congress and the courts have always granted border agencies plenary power in searching the people and property that cross international borders.[233] These border agencies serve as the first barrier in preventing contraband and security threats from entering the United States. Privacy rights have consistently been forced to yield to the interests of the American government in accomplishing such prevention, even with regard to electronic data. Precluding border officers from accessing information that travelers store on cloud servers, rather than on local hard drives, would severely undermine our government's ability to ward off smuggled and illegal goods, and it would increase the United States' vulnerability to terrorism. Rather, a policy granting border officials a broad authority to search information stored on the cloud is much more aligned with the Supreme Court and U.S. Courts of Appeals' border search doctrine jurisprudence.

Nicolette Lotrionte[†]

---

[231] *See supra* Part II.

[232] According to the Deputy Commissioner of CBP's statement at a Senate hearing, CBP border agents found "violent jihadist material, information about cyanide and nuclear material, video clips of Improvised Explosive Devices," and more on the computer of a traveler during a border search. *S. Comm. Hearing on Laptop Searches and Overseas Travel*, *supra* note 5.

[233] United States v. Montoya de Hernandez, 473 U.S. 531, 536 (1985).

[†] J.D. Candidate, Brooklyn Law School, 2013; B.A., University of Delaware, 2009. Many thanks to the staff of the *Brooklyn Law Review* for your oversight, assistance, and hard work throughout the writing process. Thank you always to my parents and sisters for your endless encouragement, love, and support.